



DATA PROTECTION REGISTER



Disclaimer

This document contains EUIPO's central register of records of the personal data processing activities established in accordance with Article 31.5 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This central register is made available to the public as provided by Article 31.5 of Regulation (EU) 2018/1725 for reasons of transparency.

This document will be updated regularly in accordance with the implementation of Regulation (EU) 2018/1725 within EUIPO. Our goal is to keep this information accurate and up to date.

Nevertheless, please note that this document is presently under revision due to the requirements of the Regulation (EU) 2018/1725 which imposes changes, in terms of the content and format of the records. Apologies for any inconvenience this may cause.

Reproduction is authorised, except for commercial purposes, provided that the source and non-authentic character are acknowledged and that it is mentioned that the information has been provided free of charge.

Any request concerning the EUIPO's register may be addressed directly to EUIPO's Data Protection Officer (DataProtectionOfficer@euipo.europa.eu).



Short list of notifications of processing operations of personal data

DPR-2017-011	MobileIron Mobile Device Management Tool
DPR-2017-037	Management of personal data in the Pan-European Seal Talent Bank
DPR-2018-001	EUIPO Ex Ante and Internal Quality Checks (trade marks and designs)
DPR-2018-003	Office 365
DPR-2018-004	Management of personal data of EUIPO ALP users
DPR-2018-006	VIP Visitor Access Request
DPR-2018-007	Immediate Feedback Survey
DPR-2018-009	Observatory networks and the related networking activities
DPR-2018-010	Management of Reprography Services in EUIPO
DPR-2018-011	Control of Health and Safety (H&S) documentation
DPR-2018-012	Departmental registers of activity
DPR-2018-013	Social Assistance
DPR-2018-014	Social Financial Aid
DPR-2018-016)	Processing operations of personal data in the general HR Database
DPR-2018-020	Monitoring of Absence from Work due to Sickness or Accident - Medical Control Visit/Examination
DPR-2018-021	Invalidity Committee procedure
DPR-2018-023	Processing of personal data on "Safety to speak up within the EUIPO" - follow up activities related to the Staff Satisfaction Survey 2018.
DPR-2018-024	Food safety trainings of external resources in EUIPO
DPR-2018-025	Preparation and transmission of BoA files to the General Court and the Court of Justice
DPR-2018-026	Issuance of the Laissez Passer (LP) of the European Union (EULP) - Travel document
DPR-2018-027	Management of EUIPOFIT activities
DPR-2018-029	Access management in EUIPO
DPR-2018-030	Mass notification system
DPR-2018-031	Teleworkers' occupational risk assessment
DPR-2018-032	Organisation of the access of EUIPO staff/external resources to Sabadell's and European Commission's premises.
DPR-2018-033	Investigation of H&S accidents/incidents
DPR-2018-034	Occupational Risk Prevention trainings
DPR-2018-035	Processing personal data of EUIPO's staff members for the promotion/ reclassification exercise including promotion /reclassification /unblocking of top grades
DPR-2018-036	Processing personal data within the framework of Calls for Talent
DPR-2018-037	Processing personal data within the framework of Structural Teleworking at EUIPO
DPR-2018-038	Processing of personal data within the framework of Working Time Management, Flexitime and Leave
DPR-2018-039	Individual Medical Files
DPR-2018-040	Processing personal data within the framework of the management and consultation of the personal file
DPR-2018-041	EUIPO Car park management
DPR-2018-042	Processing of personal data within the framework of the Certification Procedure
DPR-2018-043	Remunerations – (payments / recovery of overpayments / retentions)
DPR-2018-044	IBD training map
DPR-2018-045	Monitoring of CSS annual objectives
DPR-2018-046	Compliance with EUIPO's Guidelines on management of external resources'
DPR-2018-048	Mail and parcels distribution
DPR-2018-049	Management of TM & Design paper documentation (TM & Design archive and TM & D Reprography).
DPR-2018-050	Confidential destruction of documents
DPR-2018-051	Record on data procession in the context of the Observatory Studies
DPR-2018-053	Processing personal data within the framework of Internal Mobility procedures at EUIPO
DPR-2018-054	Processing personal data (including externalisation tasks)



DPR-2018-055	Pre-selection, selection and recruitment procedures
DPR-2018-056	Processing of personal data within the framework of the Seat Agreement between EUIPO and the Ministry of Foreign Affairs, European Union and Cooperation (MAEC)
DPR-2018-059	Processing personal data in the follow-up on individual production procedures
DPR-2018-060	Processing personal data in procurement and grant procedures
DPR-2018-061	Reimbursement of expenses related to language stays for dependent children of EUIPO's staff members.
DPR-2018-062	Processing personal data in the context of the Orphan Works database
DPR-2018-066	Machine Translation service for the Office's IP Case Law
DPR-2018-067	Mail management services
DPR-2018-068	Events Platform
DPR-2018-071	Management of User Interactions
DPR-2018-072	Administrative lists/ excel tables regarding task allocation and distribution (in particular Registry Task Distribution List; List of currently pending tasks; List regarding the Quality Reading Team organization)
DPR-2018-074	Processing operations of personal data within the framework of the secondment of National Experts to EUIPO - SNE's
DPR-2018-075	Management of backups of data contained in EUIPO systems
DPR-2018-076	Management of personal data in the Business Continuity Plan
DPR-2018-077	Management of Communication Correspondents Network
DPR-2018-078	PER. Persons Module
DPR-2018-079	Processing personal data within the framework of the Mentoring Programme.
DPR-2018-080	Publication of a list containing personal data referring to specific decisions concerning the administrative status of statutory staff (officials, temporary and contract agents) - Article 25 of the SR and Articles 11 and 81 of the CEOS
DPR-2018-082	Management of faxes
DPR-2018-086	General Media and Broadcaster contact details
DPR-2018-087	Processing of personal data on Missions
DPR-2018-089	Coordination of The Communication Correspondents' Network (CoCoNet)
DPR-2018-090	Processing of personal data in the area of Staff Evaluation
DPR-2018-091	Activities during school holidays for dependent children of EUIPO's statutory staff members - Farm school.
DPR-2018-092	Organisation of meetings and events by Communication Service
DPR-2018-095	EXAMINATION TOOLS
DPR-2018-097	Speakers of training and learning activities organised by the Academy
DPR-2018-098	Academy Network
DPR-2018-100	SIP Card - Regional Public Health Care System - Spain
DPR-2018-101	Recording and photographing
DPR-2018-102	Vaccinations Register - Agreement between the "Consellería de Sanidad - Generalidad Valenciana" and the EUIPO
DPR-2018-103	Knowledge Mapping DTD
DPR-2018-105	Legal Consultations for EUIPO's statutory staff members / seconded national experts (SNE's) and trainees relating to private legal matters - Spanish law.
DPR-2018-106	Processing of personal data within the framework of the Data Protection Office tasks and duties
DPR-2018-112	Management of contact details in Facility management service
DPR-2019-001	Processing personal data on the Prevention and Management of Conflict of Interests - Declaration of Interests for EUIPO staff and members of the Boards of Appeal
DPR-2019-002	Use of a Video- surveillance System in EUIPO
DPR-2019-003	On processing personal data in the internal audit
DPR-2019-004	Magister Lvcentinvs EUTM and RCD Intensive Modules
DPR-2019-005	Statistics on individual production and timeliness, i.e. Board decision tracking table; Rapporteur Statistics; BoA Task Reports
DPR-2019-006	Security Verification of External Resources
DPR-2019-007	Organisation and management of meetings and events by EUIPO
DPR-2019-008	Management of the Inventory of EUIPO's assets
DPR-2019-009	uniFLOW Printing management in EUIPO
DPR-2019-010	Data processing in the context of the application form of the Blockathon Forum
DPR-2019-012	Processing of personal data in the context of the IP Enforcement Forum 2019



DPR-2019-013	Processing personal data within the framework of the renewal of temporary and contract agent's contracts at EUIPO
DPR-2019-016	School and University Visits
DPR-2019-017	Organisation of the access of IBD staff/resources to the installations of other organisations/authorities/companies.
DPR-2019-018	Processing of personal data in the procedure of management of office material requests
DPR-2019-019	Maintenance management in Rosmiman
DPR-2019-020	Statistics, publications and communication of user's data
DPR-2019-021	EUIPO User Area
DPR-2019-022	Acknowledgement of receipt of fines related to traffic infringements
DPR-2019-023	Recruitment of officials by transfers or available reserve lists established by EPSO (paragraph 3.1 of the Framework for the Workforce Management in the Office)
DPR-2019-025	Follow-up of individual production and timeliness
DPR-2019-027	STAKEHOLDER QUALITY ASSURANCE PANEL AUDITORS ("SQAP")
DPR-2019-028	Key User Programme
DPR-2019-032	User Satisfaction Surveys
DPR-2019-034	Language Check Tool (LCT)
DPR-2019-035	Mapping of the experience and competencies of OD inter partes decision makers
DPR-2019-037	Processing personal data within the framework of EUIPO Mobile Telecommunications Services Policy
DPR-2019-038	Management of Incidents and Changes
DPR-2019-039	RCD-Download
DPR-2019-040	EUTM-Download
DPR-2019-041	CESTO
DPR-2019-042	TMC
DPR-2019-043	e-Search Plus
DPR-2019-044	e-Search Case Law
DPR-2019-045	Email Usage
DPR-2019-046	Collection of misleading invoices addressed to the users of the IP systems
DPR-2019-047	Processing personal data for the prevention and management of conflicts of interests - EUIPO Management Board (MB) / Budget Committee (BC) - Members, experts and advisers
DPR-2019-049	OD FTE Table and Smart Display
DPR-2019-050	Processing operations of personal data on EUIPO Directories - Insite "My Portal" / "Who is Who" / "Who to Contact" (Photo publication)
DPR-2019-051	Record of the data processing in the IP Enforcement Portal
DPR-2019-052	RECORD IP Enforcement Portal user list for operations by enforcements authorities
DPR-2019-053	Processing personal data within the framework of the agreement between EUIPO and the European School of Alicante (After School Children's Nursery)
DPR-2019-057	Register of recommended Training DTD
DPR-2019-058	Management of personal data for the EUIPO Trade Mark and Design Education Programme
EUIPO Trade Mark and Design Education Programme	
DPR-2019-059	Space management in EUIPO
DPR-2019-060	User Satisfaction Survey for the Newcomers entering into service at EUIPO
DPR-2019-062	Processing personal data within the framework of the User Satisfaction Survey regarding the Traineeship programme 2017-2018 at EUIPO
DPR-2019-063	Processing personal data within the framework of the User Satisfaction Survey for the Mentoring Programme at EUIPO
DPR-2019-064	Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO
DPR-2019-065	Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO
DPR-2019-066	Workstation Management
DPR-2019-067	User account details from DTD systems stored in the Active Directory Database (WID)
DPR-2019-068	Management of log files on EUIPO telecommunications systems
DPR-2019-069	Management of personal data by Cisco Advanced Malware Protection



DPR-2019-070	Procedure for EUIPO Library Management System (EUIPO Knowledge Hub)
DPR-2019-071	Publications manage by Communication Service
DPR-2019-072	Confidential Surveys conducted through Limesurvey
DPR-2019-073	Privacy statement on processing personal data in registers of activity
DPR-2019-074	Internal Audits in BoA
DPR-2019-076	Processing personal data within the framework of the organisation of internal competitions at the EUIPO and the constitution of related reseve lists
DPR-2019-077	Staff Satisfaction Survey 2020
DPR-2019-078	Survey Peer and 360° Feedback
DPR-2019-080	EPQCs concerning the Vienna Codes classification of EUTMs
DPR-2020-001	Management of mobile telecommunications
DPR-2020-003	Privacy Statement on processing personal data for reporting serious irregularities and wrongdoings "Whistleblowing"
DPR-2020-005	EUIPO eRegister
DPR-2020-007	Amazon Web Services as support for EUIPO IT infrastructure
DPR-2020-008	Microsoft Teams
DPR-2020-009	Virtual events organised through Zoom Video Communications
DPR-2020-010	CD Events Management and Feedback
DPR-2020-011	Delivery of Office equipment, materials and information to EUIPO staff during business continuity scenario
DPR-2020-012	Management of services during business continuity scenario
DPR-2020-013	Processing Personal Data for Legal Entity and Financial Identification
DPR-2020-014	Transfer of email addresses of applicants and representatives filing International Applications to WIPO in the emergency context of COVID-19
DPR-2020-016	OD Calls for Interest
DPR-2020-017	Processing of personal data by IBD in the framework of the Plan for the return to the Office's campus
DPR-2020-018	Manage of personal data in CISCO Umbrella
DPR-2020-019	Pan-European Seal Exchange Programme
DPR-2020-020	Processing of personal data in the context of EUIPO staff accessing the content on the PressReader platform through the EUIPO Knowledge Hub and the PressReader's App
DPR-2020-021	Covid 19 - Plan of return to the Office
DPR-2020-023	Provision of catering services during the process of return to the EUIPO' premises
DPR-2020-024	OD Appeals Notifier
DPR-2020-025	Processing of personal data by Infrastructures and Buildings Department in the Office 365 applications SharePoint and Power Apps
DPR-2020-027	Specific Privacy Statement on pulse survey related to the Staff Satisfaction Survey 2020
DPR-2020-028	Specific Privacy Statement on the processing of personal data in the procedure of follow up on occupational risk prevention incidents
DPR-2020-029	Manage of personal data in the context of eFiling applications
DPR-2020-030	Management of log files related to GI View
DPR-2020-032	EU funded project portals (update of DPR-2017-046)





Reference number	DPR-2017-011
Name of the processing operation	MobileIron Mobile Device Management Tool
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	IECISA ALTIA - DTD Operations external service provider
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing consists on the following activities:</p> <ul style="list-style-type: none">• Management of user requests to be assigned a mobile device.• Management of user requests to modify mobile device plans and/or configuration, when needed.• Maintenance activities required for EUIPO mobile devices.• Activities required in case of a theft of a mobile device.• Activities required when collecting a mobile device from a user. <p>Any user can request a mobile device, and when already assigned, any user can request a change in configuration. These requests are supported by workflow mechanisms implemented in Remedy and managed through the process for Incident and Change Request Management (DPN-2007-051), including a series of validations and/or authorizations by DTD support services or other EUIPO services depending on the nature of the request.</p> <p>Device management is mainly carried out through the MobileIron Mobile Device Management tool, this system is connected to all EUIPO mobile devices and kept synchronized. Depending on the situation, information collected through the Mobile Device Management tool may need to be sent to the service provider for examination.</p> <p>Migrations are carried out manually, and require collaboration with the user assigned. During this process, personal data is made available to the administrator doing the migration, and it is backed up in a local device (MAC computer) for approximately two days to use as a backup in case there were errors during the migration. After this period, information is deleted permanently.</p> <p>Theft and robbery reports are managed through workflow mechanisms implemented in Remedy and follow the process for Incident and Change Request Management, as indicated above. This step, however, requires the user to submit a Police report indicating the details of the person and the robbery, and it may be necessary to pass this information to service providers in order to receive a new device.</p> <p>This Notification is linked to the DPO Notification - DPN-2017-012 EUIPO Mobile Telecommunications Services Policy</p>
Purpose of the processing	It is necessary to collect personal data in order to know the user that was assigned the device, identify the device, and provide maintenance as needed.
Data Subjects	All EUIPO Staff that has been assigned a mobile device (statutory or not)



Description of categories of persons whose data EUIPO processes and list of data categories	<p>During normal assignment and maintenance of the device:</p> <ul style="list-style-type: none">• Name and surname• Mobile telephone number assigned• Login• Approximate location (to within 2 Kms): As currently configured, the geo-localisation won't give the exact location of a mobile, but will identify the country that the mobile is in, in order to do a security validation of the phone, and send an informational message regarding the use of roaming in case the mobile has left the country.• List of applications installed <p>During Data migrations:</p> <ul style="list-style-type: none">• Device username and password• All personal data stored in the device, such as contact book information, photographs, credit card information (if stored on the device by the user), passwords to any application or website (if stored on the device by the user) and in general terms, any personal data maintained by the user on the device. <p>When the user requests a change in roaming due to travel:</p> <ul style="list-style-type: none">• It is necessary to know the country that the user will be traveling to, in order to activate the required roaming plan. <p>During management of theft or robbery of the device</p> <p>Police report of the theft, including all the information available in it: Name, surname, address, contact information, and any details included in the report.</p>
Retention period	<ul style="list-style-type: none">• Information for mobile device management is stored for as long as the user is assigned the device. Once the device has been collected, Information is kept for up to 90 days.• During data migration, information is stored for the duration of the migration process and also kept for approximately two days as a backup in case that there were errors during the migration.• Police reports are kept only for as long as they are needed for reporting the theft of the device, and deleted once no longer needed.• Any information managed through My Service Desk apply the storage limits indicated in DPN-2016-018.
Recipients of the data	<ul style="list-style-type: none">• The service provider and any subcontractor after duly notification to EUIPO and its acceptance.• EUIPO Management (during approval process and in case that investigating mobile usage is required)
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>Information may be sent to the following third parties:</p> <ul style="list-style-type: none">• MOBCO/MobileIron: Service provider for the Mobile Device Management tool. Information may be sent in case of errors or incidents that cannot be resolved by the processor and require the service provider expertise. (Belgium)• Vodafone: Third party requires the Police report in order to manage the theft and replacement of a device. (Spain)



<p>General Description of security measures</p>	<p>The tool is connected to EUIPO's authentication systems in order to verify the person that is trying to access the information. • Tool includes access control measures to grant or deny access based on the profile of the user that is connecting. • FIPS 140-2 certified encryption For the process of data migration: • Information is temporarily stored in a portable device. This information is encrypted and protected by password. • The portable device is also protected by access control mechanisms to grant or deny access to the device. • When not in use, the device is locked in a security safe. The device itself is configured with data encryption and a security pin for access control, in order to ensure that any data stored in the device is properly protected against unauthorized access. This configuration is remotely enforced by the MDM, preventing the user from deactivating it.</p> <p>For this process, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/c972032b-b7de-4e2a-8795-5106f168b2c6</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2017-037 (Updated by DPR-2019-015)
Name of the processing operation	Management of personal data in the Pan-European Seal Talent Bank
Last Updated:	26/07/2019
Controller Organizational entity	Academy
Controller contact details	H
Name and contact details of processor	EUIPO Academy Team IT Administrators and Operators from DTD (IECISA-ALTIA Service Provider). EUIPO Academy Team dealing with Pan European Seal Programme IECISA-ALTIA is a Service provider of DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<ul style="list-style-type: none">• The Pan-European Seal (PES) Talent Bank is a new on-line tool intended to serve as a cooperation platform between offices in the field of intellectual property and other relevant institutions and organisations, both public and private. On this platform, the participating partners will publish traineeship and job opportunities accessible to former PES trainees.• Former PES trainees can create a profile by registering on the website and verifying their profile by uploading a certificate for completion of a traineeship with the EUIPO or the EPO. Upon validation by the Academy Team, registered former PES trainees can expand their profiles by adding information and uploading their CVs, and can submit applications (including supporting documents) for published job/traineeship positions.• The Academy team is designated owner of the system and therefore the one in charge of managing the Talent Bank having full access rights over the content published by all associated partners and users.• The DTD (IT Administrator) has limited involvement in the management of the tool as it is in charge of the technical administration and the backup of data.
Purpose of the processing	The purpose of the PES Talent Bank is to provide a cooperation platform between offices in the field of intellectual property and other relevant European Union institutions and organisations, both public and private, for enhancing the professional and traineeship opportunities for former PES trainees, by providing them with a portal on which available traineeship and job opportunities will be published and PES trainees can submit their applications. In that regard, the purpose of data processing operations is to allow applicants to submit their CVs and make their personal information and professional experience available to the recruitment staff of the offices posting job and traineeship opportunities. In addition, during enrolment, personal data provided by applicants will be used to validate the identity of the applicant and the correctness of the information provided.
Data Subjects	Any person creating an account on the system and submitting their personal data. However, the authorised/validated users of the system will be only former PES trainees who have completed a traineeship at the EUIPO or the EPO and who can provide as an evidence a certificate for completion of such a traineeship. The Academy Team is to validate all created profiles and where the required evidence is missing, the registration will be rejected.
Description of categories of persons whose data EUIPO processes and list of data categories	First name, surname, data of birth, nationality, telephone number, address, photo, email address, year of Pan-European Seal traineeship and institution (EUIPO or EPO), PES University Member, Education level and field of study, applications history, and other information available in users' CVs or other attached documents.



Retention period	<p>Data of validated accounts, namely, accounts of former PES trainees who have completed a traineeship at the EUIPO or the EPO and who can provide as an evidence a certificate for completion of such a traineeship which is to be validated by the Academy, is to be kept for as long as the account is active.</p> <p>Users whose accounts have not been active for a period of 2 years will be deactivated upon the receipt of an email notifying them about this. Two years is a reasonable timeframe considering traineeship programmes normally last one year and selection processes up to six months. Once deactivated, personal data is maintained for the period of three months for the purposes of restoring the account, if the user wishes to do so. After this period, personal data is removed with the exception of the year of Pan-European Seal traineeship, which is kept for statistical purposes but will not be linked to a specific candidate.</p> <p>Accounts that have not been validated during creation or that have been considered invalid are maintained for a period of 3 months for the purposes of allowing the user to provide evidence for the validation of the account. If no evidence is provided during this period, personal data is removed</p>
Recipients of the data	The Recipients of the information are the EUIPO, the EPO and all other approved partners authorized to post available job offers and traineeship opportunities, and their respective recruiting staff.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	The purpose of the PES Talent Bank is to provide a cooperation platform between offices in the field of intellectual property and other relevant institutions and organisations, both public and private, for enhancing the professional and traineeship opportunities for former PES trainees. Transfer of personal data will only take place inside the EU. All such transfers are to be documented by the necessary Memorandum of Understanding with the required contractual clauses in terms of privacy and data protection, etc. depending on the recipient of personal data. Separate documentation is to be drafted and send to the DPO for approval, for each of the transfers depending on the country of the recipient.
General Description of security measures	<p>Several security measures are applied throughout the activities involved in the management of the PES Talent Bank.</p> <ul style="list-style-type: none">• Firstly, the following standard security measures of the EUIPO Information Systems are applied:<ul style="list-style-type: none">- Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed.- Access to the website is restricted by username and password and is subject to prior validation by the EUIPO Academy team.- Authentication and authorization to view and access information based on roles.- Servers are physically protected at the Data Processing Centre.- Network security configured to prevent external threats from accessing the servers.• The EPO and the approved associated partners are responsible for the security of information processed once they undertake a recruitment process. The appropriate documents are to be signed between the EUIPO and the partner to guarantee various elements of personal data processing are to be ensured by the recipient party, e.g. ensure that it complies with, and that its acts or omissions do not cause EUIPO to be in breach of, any applicable laws or regulations related to such processing including but not limited to the Data Protection Regulation ("Applicable Law"); have in place adequate contractual, technical and organisational security measures to ensure that the confidentiality of such processing is in compliance with the Applicable Law; and provide EUIPO on demand with details of the contractual, technical and organisational security measures. Separate documentation is to be drafted and send to the DPO for approval, for each of the transfers depending on the country of the recipient.



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on the processing of personal data in the context of the Pan-European Seal (PES) Talent Bank: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/9aab181f-d65f-4572-ac37-3e6dbf033e74
EDPS Prior consultation	NO



Reference number	DPR-2018-001
Name of the processing operation	EUIPO Ex Ante and Internal Quality Checks (trade marks and designs)
Last Updated:	20/03/2020
Controller Organizational entity	ICLAD
Controller contact details	ICLAD.Secretariat@euipo.europa.eu
Joint Controller organizational entity	Operations
Joint Controller contact details	ODDPC@euipo.europa.eu
Name and contact details of processor	Operations Department (ex ante) International Cooperation and Legal Affairs Department (IQC) DTD for the technical support with the tools
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing consists of checking the quality of decisions, communications and/or tasks carried out by examiners in any area once they are ready for notification to the party/parties of the procedure, or finalised accordingly. These quality checks are performed by designated staff members (experienced examiners, mainly Reference Persons in the respective area of the checks or experts in these fields) who</p> <ul style="list-style-type: none">• review the work products of the examiners once they are ready for notification, or officially issued by the EUIPO and• report the results of their review via a database created for this purpose ("UQCT – Unique Quality Check Tool").
Purpose of the processing	<p>The goal of the Ex Ante and Internal Quality Checks is to improve the global quality of the outputs of the EUIPO, in relation to the Office's service standards. This is achieved by checking (and correcting when needed) the product before or after it is sent to the trade mark or design user depending on whether the check is performed prior to notification or on the finished product, collecting information on areas where improvements are needed. Accordingly, special measures are envisioned (e.g. training actions, change of methodology, the use of good practice examples that can be followed). These results will be analysed only to define the most efficient actions to be used for improving the general quality of the Office's products.</p> <p>The results of the exercise will not be used for assessing the individual performance (its quality or else) of the examiners. The feedback provided to the examiner by the checker would merely be intended to correct errors or suggest improvements, in order to ensure that the product, and future products delivered to the outside user(s) comply with the quality requirements and criteria defined by the EUTMR & RCD Regulations, EUIPO Guidelines and practices of the Office.</p> <p>The analysis of the exact nature of the errors and the repetitive errors and the areas where they occur (all the data presented and used in aggregate and anonymised form by the EUIPO management) is aimed to identify patterns and define correlations such as, for example, examiners with longer experience tend to commit less errors, the main area where errors of the same nature repetitively appear are the opposition decisions, etc. On occasion, it is necessary to make reference, in the form of an annex to the report, to specific trade marks or designs in order to provide examples of the errors for training purposes.</p>
Data Subjects	Examiners in Operations Department



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects are OD examiners.</p> <p>Quality data resulting from Ex Ante and Internal Quality Checks, namely the information related to identifiable natural person (examiner), linked to the quality i.e. correctness, consistency, accuracy and completeness of the products delivered by the said individual. The examiner's name will never be included in the recorded or reported data. But indirectly, through the file number, trade mark or design, and the type of decision, letter or task checked, it would be theoretically possible to identify the examiner involved.</p> <p>However, the necessary technical measures are taken, so that even if the name of the examiner could be identified in each particular case and therefore, the information on examiner's quality could be established for each single product offered by him/her, this information does not give an overall perspective of the examiner's overall quality.</p> <p>This is because the gathering and analysing of the data on all communications - decisions/letters and/or tasks drafted or completed by a certain examiner - is technically not possible (except for specially appointed persons responsible for the reporting) and thus, cannot lead to establishing any conclusions and/or proceeding with any follow-up on the overall individual quality of the products delivered by each of the examiners.</p>
Retention period	<p>Only for the time necessary to achieve the purpose for which they will be processed. The file number of the case concerned will be kept for 15 months, allowing the comparison of cases where mistake(s) were found during the internal quality check (done by an external panel). The data is currently deleted manually, but it is foreseen to automate the deletion as soon as the necessary IT tools are available.</p> <p>The decisions and communications included in the list of 'excellent' cases referred to in point 3 will be removed after 5 years.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process.</p>
Recipients of the data	<p>The recipients having access to the protected information, the file numbers, are only the following persons from ICLAD and OD:</p> <ul style="list-style-type: none">• quality chairs (only for the cases checked by their quality group)• quality checkers (only for their own quality check cases – revised by them)• internal quality check coordinator• reference persons' coordinators (for Ex Ante, only for their specific area)• two data miners (quality officers)• extended addressees (all the employees of the Operations Department – only for their own cases, drafted or co-signed by them). <p>The information concerning the Internal Quality Check (IQC) will only be shared with people necessary for the implementation of such measures on a need to know basis. The data are not used for any other purposes nor disclosed to any other recipient.</p> <p>Only the list of 'excellent' decisions and communications, once they have been notified to the party(ies) of the procedure, may be published internally for Office staff, and in particular for examiners.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to the Ex Ante and Internal Quality Check procedures is stored in a secure IT application according to the security standards of the Office.</p> <p>Appropriate levels of access are granted individually only to the above recipients.</p> <p>The database is password protected under single sign-in system and automatically connected to the user ID. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>All persons dealing with personal data in the context of the ex ante and internal quality check procedure and at the same time, coincidentally with e.g. evaluation procedures concerning the same data subjects, shall sign a confidentiality declaration that is to be kept in the folder of the procedure.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement Ex Ante and Internal Quality Checks:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/1f84d63e-ba34-4a7c-9535-cca25247f735</p>
EDPS Prior consultation	YES



Reference number	DPR-2018-003
Name of the processing operation	Office 365
Last Updated:	07/05/2020
Controller Organizational entity	Digital Transformation
Controller contact details	For internal users: UserFeedback@euipo.europa.eu For external users: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA ALTIA (DTD external service provider) MICROSOFT (the service provider)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Office 365 is a cloud based package of applications (Word, Excel, PowerPoint, Outlook, OneNote, OneDrive) provided to users with the aim to offer more flexibility and improve communications, collaborations, as well as the availability of resources.</p> <p>MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office.</p> <p>The processing of personal data is carried out under the responsibility of the Director of the Digital Transformation Department (DTD), acting as delegated EUIPO data controller. However, DTD acts as processor when the use of the application MS TEAMS is requested by other Department/Service of EUIPO. In this situation, the requesting Department/Service will act as controller.</p> <p>Personal data is processed by DTD's external service provider, such as Microsoft.</p>
Purpose of the processing	<p>The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the above-mentioned services.</p> <p>The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing.</p> <p>Due to the outbreak of the coronavirus COVID-19 virus, the Office has extended the use of Microsoft Office 365, and in particular 'Microsoft Teams' to organise virtual meetings and teleconferences with internal staff and external stakeholders. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing.</p> <p>The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services.</p>
Data Subjects	<p>All EUIPO Staff and external providers with an EUIPO e-mail address.</p> <p>Regarding MS Teams, EUIPO staff members and EUIPO external users included in the MS Team that is used for the exchange of information.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The categories/types of personal data processed are the following:</p> <ul style="list-style-type: none">• Personally identifying Information: username, name, surname, email, work telephone number, current function and preferred language.• Electronic identifying information: IP address, cookies, connection data and access times.• Movies, pictures, video and sound recordings.• Metadata used for the maintenance of the service provided.• Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar) <p>When processing personal data during the organisation of meetings via MS Teams, this personal data is processed in accordance with the Processing of personal data for events, trainings and meetings.</p> <p>Regarding MS Teams, as part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between the Office and stakeholders, such as messages, images, files, voicemails, recordings (if previously agreed), calendar meetings, contacts, metadata used for the maintenance of the service provided.</p>
<p>Retention period</p>	<p>For Office 365, data will be retained for as long as there is a contractual relation with the Office. Once a contract expires, information is retained for 90 days for the purposes of collection from the Office or possible renewal. After this period, information is deleted.</p> <p>The Data Protection Addendum, Microsoft commits to respond to requests for the management of personal data, including data access, modification, deletion, etc. "Microsoft, in a manner consistent with Microsoft's role as a processor will make available to Customer Personal Data of data subjects and the ability to fulfill data subject requests to exercise their rights"</p> <p>Microsoft also commits to redirecting to the Office the requests by any Office data subject directly contacting Microsoft</p> <p>Regarding MS Teams, data will be stored in MS Teams for one year after the exchange activity is completed.</p>



Recipients of the data	<p>For Office 365, in principle the majority of the service operations are automated in order to reduce the need for human access. Microsoft engineers and support staff do not have access to customer data by default, and are only granted access in case it is required for maintenance purposes.</p> <p>That said, information may be stored in the US. In addition, information may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.</p> <p>The following safeguards are implemented:</p> <ul style="list-style-type: none">• In all transfers, Microsoft uses EU Standard contract clauses for the transfer.• In the specific case of transfers to the US, Microsoft is certified to the EU-US Privacy Shield Framework.• Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardize and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft. <p>It is also possible to use the logs in the privacy console to verify when information has been shared with Microsoft staff or subprocessors.</p> <p>Regarding MS Teams, the personal data is disclosed, under the need to know basis, to the following recipients:</p> <ul style="list-style-type: none">• EUIPO staff members and EUIPO external users included in the MS Team that is used for the exchange of information;• DTD, Microsoft and DTD's external service provider involved in the data processing necessary to provide the service. <p>Personal data is processed by DTD's external service provider, such as Microsoft, for the following activities:</p> <ul style="list-style-type: none">• Provisioning end-user support and troubleshooting for Office365 applications and features related to conducting virtual meetings and teleconferences• Track changes to users and groups• Management of content uploaded to MS Teams, including data retention policies• Manage MS Teams settings• Support, operate, and maintain the Online Services. <p>Personal data is stored in the EU according to the application configuration implemented by EUIPO.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?

Information will be stored in Microsoft Datacenters, located in the "European Region": Netherlands, Ireland, Austria, Finland and France. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud.

For Office 365, information may be stored in the US. In addition, information may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.

Regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by EUIPO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.

Nevertheless, if access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented.

- In all transfers to third countries, Microsoft uses EU Standard contract clauses for the transfer with its subprocessors.
- Microsoft requires sub processors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardise and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft.



<p>General Description of security measures</p>	<p>Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud.</p> <p>Microsoft has implemented several controls to ensure the availability of the information. As a minimum, data is replicated between two datacentres within the same region, has redundancy controls and implements backups that are encrypted before being transmitted and stored.</p> <p>Datacentres have physical and logical security monitoring measures, such as:</p> <ul style="list-style-type: none">• Video surveillance of the perimeter• Seismic and environmental monitoring at the buildings• Monitoring of security threats, such as worms, denial of service attacks, unauthorized access, or any type of unlawful activity. <p>Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres. This includes security controls against accidental or unlawful destruction, loss, unauthorized access, use, modification or disclosure. These internal controls are audited on a yearly basis, if required, audit information can be provided under a Non-Disclosure Agreement (NDA).</p> <p>Information is encrypted while at rest and in transit.</p> <p>As mentioned above, information may be stored in the US, or may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.</p> <p>The following safeguards are implemented:</p> <ul style="list-style-type: none">• In all transfers, Microsoft uses EU Standard contract clauses for the transfer.• In the specific case of transfers to the US, Microsoft is certified to the EU-US Privacy Shield Framework.• Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardize and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft. <p>It is also possible to use the logs in the privacy console to verify when information has been shared with Microsoft staff or subprocessors.</p> <p>For more information, please check the Security and Privacy Risk Assessment: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/c4b23e3e-061e-40d0-9914-b298bc0a2158</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement: http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/4277d2cb-6489-4876-a60f-1a135a601c1f/FINAL%20Privacy%20Statement%20Office%20365.pdf</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-004
Name of the processing operation	Management of personal data of EUIPO ALP users
Last Updated:	27/03/2019
Controller Organizational entity	Academy
Controller contact details	For internal staff academy@euiipo.europa.eu For externals: DPOexternalusers@euiipo.europa.eu
Name and contact details of processor	EUIPO Digital Transformation Department as internal processor in the role of application manager. Deloitte as external processor, providing services to Human Resources Department (consultancy services related to the EUIPO ALP). ECISA-ALTIA and SOPRA as external processors, providing services to Digital Transformation Department (EUIPO ALP administration and queries). Linguarama Iberica S.A. as external processor, providing services to Academy Department exclusively for language courses. EUIPO Infrastructure and Buildings Department as internal processor : ibddpc@euiipo.europa.eu Pomilio Blumm as external processor, providing services to IBD as described in DPR-2019-007: dmo@pomilio.com
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The EUIPO ALP is a learning management system based on Moodle, which produces online learning sites for students to improve their knowledge about different subjects through active collaboration, communication and resource sharing. The necessary profile information is generated during the registration process and EUIPO ALP account creation. The account allows the user to enrol in different courses and his or her profile data is used to track individual progress. The user can edit his or her profile data and request that the controller delete it.
Purpose of the processing	Purpose of the processing operation of course participants: - to plan and organise and promote training activities for EUIPO ALP users; - to create a training history log for EUIPO staff, which will be available in the HR Portal; - to issue certificates of participation for the different training courses; - to collect feedback from participants so that the controller can promote and deliver better and more effective training, according to participants' needs and knowledge as well as the skills necessary for their job; - to keep logs that include user activity (access time, actions, etc.), which could be used to resolve user incidents.
Data Subjects	- EUIPO users, i.e. users with an EUIPO corporate account: staff, seconded national experts, trainees and external service providers. - General users. - Pan European Seal users.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following mandatory personal data is collected to create the user account:</p> <ul style="list-style-type: none">- Profile information: Username, Password, First name, Surname, Email address, City/Town, Country, Nationality, Date of birth. <p>The following non-mandatory personal data could be collected if the user so wishes:</p> <ul style="list-style-type: none">- Other profile information: Time zone, Description box, User Picture (file to upload), First name
Retention period	<p>For general users and Pan European Seal users (users who do not have an EUIPO corporate account), data is kept for as long as the user has an active account. The EUIPO will delete the account following a 10-year period of inactivity, or upon request of the user to cancel the account.</p> <p>For EUIPO users (users with an EUIPO corporate account), the account will remain active as long as there is a contractual relationship with the EUIPO. All data will be deleted 2 months after the contract is finished.</p>
Recipients of the data	EUIPO staff: information on completed courses is available from the HR Portal in compliance with DPR-2018-016. . This information is visible to Human Resources Department and to EUIPO staff's line managers.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>Data is stored in the content management system (EUIPO ALP) on a database server (MySQL) in accordance with the security standards of the Office.</p> <ul style="list-style-type: none">- Information is stored in security hardened servers with access control measures and protected by a username and password. Anonymous access will not be allowed.- Authentication and authorisation to view and access information is based on roles.- Access to EUIPO ALP for roles with permission to view personal data is restricted by username and password and subject to prior validation by Academy Department.- Servers are physically protected at the Data Protection Centre.- Networking security is configured to prevent external threats from accessing the servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/S...</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/11caa204-ea88-4c28-b40f-79ec33a5b8c5</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-006
Name of the processing operation	VIP Visitor Access Request
Last Updated:	21/05/2019
Controller Organizational entity	Communication
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain. Contact: Head of Communication Service: PersonalDataCS@euipo.europa.eu
Name and contact details of processor	Protocol team / Security Services (Communication Service / IBD Security Services)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In order to facilitate VIP visitor access to the EUIPO premises (which entails mainly not passing through security control when entering with private or EUIPO official vehicle to the 'Campus') the protocol team receives personal data via the following two different methods:</p> <p>1) request via Remedy (the VIP visitor access request) in which case Security services process the personal data as described in the Notification DPN-2018-029 on the procedure of access management in EUIPO.</p> <p>2) VIP Visitor access organised directly by the protocol team; the VIP/VIP's secretariat will be requested to send in advance: identification number; licence plates of car when not an EUIPO official vehicle; names and identification numbers of accompanying persons drivers and security guards.</p> <p>The information will be requested and received by email or phone call and stored temporarily in sharedox and/or outlook.</p> <p>After the completion of the event that requires the attendance of the VIP, this information will be deleted from the storage place, i.e. ShareDOX or Outlook.</p>
Purpose of the processing	The personal data is collected so that the identity of the VIP visitor and accompanying individuals can be confirmed and checked, and access can be granted to EUIPO premises in a secure way.
Data Subjects	VIP external visitors/stakeholders/drivers/bodyguards
Description of categories of persons whose data EUIPO processes and list of data categories	Identification data: name, surname, job title, employer/institution, identity number (NIE, NIF, identity card, passport), vehicle type and licence plates.
Retention period	The data will be stored in Outlook and Sharedox until the visit of the VIP is completed.
Recipients of the data	N/A
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>Information stored in Sharedox is protected by the standard security measures of the EUIPO Information Systems:</p> <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed.• Access to the system is subject to justified approval based on position and roles.• Authentication and authorization based on roles. The content accessible and the operations available differ depending on roles.• Servers are physically protected at the Data Processing Centre.• Network security configured to prevent external threats from accessing the servers. <p>The processing of this information will be both manual and automated.</p> <p>All personal data related to the list of contacts internally stored follows the secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>FINAL VERSION_VIP Visitor Access_Data Protection_Privacy Statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/48bfee7b-feed-4821-aa6f-07bd2efa56c4</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-007
Name of the processing operation	Immediate Feedback Survey
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euiipo.europa.eu
Joint Controller organizational entity	Operations
Joint Controller contact details	Director of the Operations Department, EUIPO ODDPC@euiipo.europa.eu OD is the joint-controller to the extent related to the processing of personal data concerning OD examiners only.
Name and contact details of processor	1. BERENT Deutschland GmbH as the external service provider ("Berent") Contact details: BERENT Deutschland GmbH Carl-Ludwig-Strasse 16 D-37213 Witzenhausen Germany Tel: +49 5542 9119-01 E-mail: info@berent.com 2. Severiano Servicio Móvil S.A. ("Severiano")
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The EUIPO offers users immediate feedback surveys and other feedback options through the EUIPO website (such as the feedback functionality in Help & FAQs and at the end of the e-filing procedure) or through any other communication channel such as the phone, fax or video conference tools through MS Teams. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. These feedback solutions allow the EUIPO to measure the user satisfaction with the Office tools, services or products and/or to gather feedback in order to improve office tools, services or products. You may be requested to complete the survey through the Limesurvey tool. The answers are collected and analysed to explore cause-effect relationships related to satisfaction or experience of users. Participation in any feedback process is voluntary</p> <p>The EUIPO processes the answers of the respondents along with other identification data automatically extracted from the EUIPO systems and/or contact details provided by the respondents themselves. However, personal data are not used for the analysis of the survey results. They will only be processed to contact the users when a follow-up is needed.</p> <p>External service providers (Berent, Severiano - First Line and Deloitte) can be appointed to conduct these surveys and produce statistical reports under the instructions of EUIPO.</p> <p>The immediate feedback surveys on classification deficiency letters issued by OD examiners are conducted with the use of the Limesurvey Tool.</p> <p>Place where data is stored:</p> <p>The data is stored in the EUIPO Portal Database, Limesurvey tool and in the document management system of the Office (ShareDOX). The servers are located in the EU (Spain); and in the service provider survey systems (i.e. CATI (computer assisted telephone interviewing), CAWI (computer assisted web interviewing), Deloitte, platforms run by Berent - the "Survey System". The data will be hosted in a datacentre in Berlin, Germany, and accessed from the BERENT HQ in Kassel, Germany.</p>
Purpose of the processing	<p>The purpose is to gather feedback from users and/or provide users with a personalised follow-up with the aim of increasing their satisfaction in relation to the EUIPO tools, services or products. The purpose is not to evaluate or assess the performance or work of EUIPO internal staff.</p>
Data Subjects	<p>The data subjects are:</p> <ul style="list-style-type: none">- The users participating who after using the EUIPO services, tools or products participate in the surveys; and- The trade mark examiners of the EUIPO OD department who prepare classification deficiency letters. The data collected can only indirectly identify the data subjects.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The data subjects are:</p> <ul style="list-style-type: none">- The users participating who after using the EUIPO services, tools or products participate in the surveys; and- The trade mark examiners of the EUIPO OD department who prepare classification deficiency letters. The data collected can only indirectly identify the data subjects. <p>The data collected are:</p> <ul style="list-style-type: none">• Responses and comments to the questions and forms; Data on users automatically collected by the EUIPO Portal while answering the questions (e.g. language, date and time);• Data on users already existing in the Office systems, including personal data such as record ID, PER ID, country, username, application id, application, name, company name, email, telephone number, type user, subtype user and language, complaint id (if related to complaints), complaint summary, complaint nature, process, track, tool, round, all related files and filings.;• Contact details provided by the user himself in the form: name, email address, phone number.• Track ID related to classification deficiency letters• Name and surname of the examiner <p>• Through MS Teams, additional data may be collected as follows:</p> <ul style="list-style-type: none">- Personally identifying Information: username, name, surname, email, work telephone number, current function and preferred language.- Electronic identifying information: IP address, cookies, connection data and access times.- Movies, pictures, video and sound recordings.- Metadata used for the maintenance of the service provided.- Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar) <p>For further information, consult the MS Teams privacy statement.</p>
<p>Retention period</p>	<p>Personal data are kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>In particular:</p> <ul style="list-style-type: none">• The data contained in the excel tables on ShareDOX: 2 years from when the survey took place since users may be contacted for follow-up (in case a user has made a suggestion for example the time limit to contact him back on the final status of the suggestion is 2 years). The excel tables will be anonymised after the established retention period;• Reports on ShareDOX: indefinite since the reports are presented in aggregated way without personal data;• EWS and Limesurvey: 2 years for the same abovementioned reasons.• Data will be stored in MS Teams for one year after the exchange activity is completed.



<p>Recipients of the data</p>	<ul style="list-style-type: none"> • Staff from CD (Customer Feedback, Customer Care (First Line, Second Line, Complaints), QPROs) and DTD involved in the follow-up process. • Staff from DTD in charge of the maintenance of the IT systems. • Staff from OD (Director, Deputy Director and Head of Service 1) • The external service providers staff involved in performing the survey will collect the results of the survey and analyse the raw data in order to perform statistics and figures in collaboration with Customer Feedback Team. • The 'super administrators' and 'administrators' of the Lime Survey tool. <p>Internal processor:</p> <p>Name, position: Head of Service of the Customer Management Service Organizational entity: Customer Management Service – CMS</p>
<p>Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?</p>	<p>NO</p>
<p>Are there any transfers of personal data to third countries or international organisations?</p>	<p>NO</p>
<p>General Description of security measures</p>	<p>All personal data related to immediate feedback or other forms of feedback surveys is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none"> • Role-based access control to the systems and network • Logical security hardening of systems, equipment and network • Physical protection via secure Data Centre • Confidentiality and data protection clauses are signed-off by the service provider participating in the survey exercises. Please see a copy of these clauses as an annex 3 hereto. • The service provider complies with the guidelines described in ISO 20252:2012, and the ESOMAR, MRS and BVM codes. BERENT's Managers are members of these aforementioned research associations and, as such, are obliged to conduct all business in accordance with the rules and regulations of these codes. • Please see in annex 4 and 5 a description of Berent security measures under the documents "EUIPO-Data protection web-server" and "Berent security measures". • Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) • For the Limesurvey tool, please see annex 6 for more information on security measures. <p>MS Teams has been configured to preserve the confidentiality of the information you exchange by implementing encryption during all communications and in storage, and anonymous access is not authorized. For more information on MS Teams, please check the specific privacy statement posted on EUIPO website</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy statement for external users: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/c94fa228-7316-44d2-a72c-3ddb748d639d</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-009
Name of the processing operation	Observatory networks and the related networking activities
Last Updated:	28/04/2020
Controller Organizational entity	Observatory
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	Observatory staff and consultants and EUIPO event organisers
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Networking is in the nature of the European Observatory on Infringement of IPRs. Regulation (EU) No 386/2012 defines the Observatory as a network of experts from the public and the private sectors and described the tasks of that network in its Communication entitled 'Enhancing the enforcement of IPRs in the internal market'. That Communication stated that the Observatory should serve as the central resource for gathering, monitoring and reporting information and data related to all infringements of intellectual property rights. It should be used as a platform for cooperation between representatives from national authorities and stakeholders to exchange ideas and expertise on best practices and make recommendations to policymakers for joint enforcement strategies.</p> <p>The Observatory being a network has created a number of other networks for its numerous activities. The list of the current networks can be found in ShareDOX under the following link http://sharedox.prod.oami.eu/share/page/repository#filter=path%7C%2FOffice_Docs%2FM%2520INT%2520RELATIO NS%2FM21%2520Observatory%2FCentral%2FStakeholders&page=1</p>
Purpose of the processing	<p>The Observatory shares contact information with the different members of its networks, asking for their contribution and feedback on initiatives and inviting them to the numerous networking events. In the Observatory Restricted Access Area (RAA), access is given to documentation pertaining to different networks, since one of the aims is to put people in contact and foster collaboration. Also, for this purpose the Observatory will make use of MS Teams a collaborative tool and Zoom Video Communications .</p> <p>For MS Teams refer to specific privacy statement. For Zoom Video Communications refer to specific privacy statement.</p> <p>To ensure the coordination between the different networks, the Observatory also issues annual Country Reports for the public stakeholders (representatives of the Member States in the Observatory). These reports allow the public representatives to have</p> <ul style="list-style-type: none">• a general overview of the different areas, in which the Member States interact with the Observatory;• the contacts the Observatory has in the different Member States;• the Observatory events and meetings that representatives from the Member State have attended;• know in advance what the Observatory is going to ask for and what kind of help is needed from them to collect data in their country. <p>In addition, and in order to maintain the members of the different networks updated on the ongoing activities, the Observatory sends out a newsletter (by GetResponse) on a quarterly basis.</p>
Data Subjects	The contact persons of the stakeholders of the Observatory, experts, enforcers and any individual taking part in one of the various networks of the Observatory



Description of categories of persons whose data EUIPO processes and list of data categories	The contact persons of the stakeholders of the Observatory, experts, enforcers and any individual taking part in one of the various networks of the Observatory.
Retention period	The documents containing the information of the members of the different networks are living documents that are constantly updated when there are changes. Whenever a person does not longer form part of a network, the data is automatically deleted from the lists.
Recipients of the data	<p>The information concerning the members of the different networks will only be shared with people necessary for the implementation of such measures on a need to know basis. This also extends to our providers hired for consultancy tasks and events organization.</p> <p>With regards to other staff groups of the EUIPO, they have read only access where necessary for the work related to the network and events (hence, ICLAD staff for the EU Delegations Network, CS staff for the public awareness networks, Cabinet staff for updating the ED, CD staff for supporting the promotion of the Observatory tools and DTD and on the need to know basis some external providers).</p> <p>Personal data is not used for any other purposes or disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to [process name] is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing personal data in the context of the EU Observatory networking activities:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/4ad2ff33-2e72-47ac-be2e-2055095cff91</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-010
Name of the processing operation	Management of Reprography Services in EUIPO
Last Updated:	27/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Reprography Coordinator, Common Services, IBD EUIPO External processor: External Reprography provider Grupo EULEN
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In general, EUIPO staff and external resources request Reprography services through the use of the My service desk, product Reprography Requests.</p> <p>The requests are received and attended by the Reprography external provider which maintains an Excel table of all requests for the purpose of accountability and accurate invoicing (as not all requests come from My service desk). Additionally, in accordance with the paperless policy of the office and Objective 1.3, Line of Action 1 of the Strategic Plan 2020, the reprography services have foreseen to launch a campaign with the purpose of raising users' awareness and stimulating the responsible and sustainable use of paper. The campaign consists of informing the users of their individual consumption of paper through a user individual consumption report that will be sent to each user on a monthly basis through the use of Remedy 09 tool.</p>
Purpose of the processing	<p>The purposes of the processing operation in the Excel table are as follows:</p> <ul style="list-style-type: none">• Quality control of the provider;• Accurate invoicing and sound financial management;• User-friendly management of the requests and traceability of the information;• Creation of statistics on the use of the reprography services. <p>The purpose of the processing operation in the User consumption report is to calculate the individual consumption of paper when using the reprography services of the Office and stimulate the reduction of both overall and individual consumption.</p>
Data Subjects	EUIPO internal staff and (statutory or not)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data processed in the Excel table maintained by the external provider of reprography services is as follows: Name, surname, REQ number, department, service, date of request, details of the request.</p> <p>The personal data processed in the user individual consumption report is as follows:</p> <ul style="list-style-type: none">• Name, surname;• Remedy Request number;• Paper size requested and corresponding number of pages;• Total Individual Consumption/ Month (all converted to A4);• Service average/Month.



Retention period	<p>The excel table with all Reprography requests is stored in a specific folder Y:</p> <p>The user individual consumption report is generated through the use of Remedy09 tool and is sent to the individuals by mail.</p>
Recipients of the data	<p>Access to the Excel table maintained by the external provider of reprography services have the following user groups:</p> <ul style="list-style-type: none">• Staff of the external provider in order to perform the service;• Reprography team of EUIPO (internal) for quality and financial control purposes. <p>Access to the user individual consumption reports have the following user groups:</p> <ul style="list-style-type: none">• The affected staff member, for information and for awareness raising purposes.• IBD coordinator of the service during the start-up stage.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p> <p>The staff of the Reprography services provider dealing with personal signs a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement Reprography services:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/bb7fd9e1-18af-4607-ba51-db07902a0135</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-011 (update DPN-2017-002)
Name of the processing operation	Control of Health and Safety (H&S) documentation
Last Updated:	10/12/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal: H&S internal team in IBD, EUIPO External: Health & Safety (H&S) services provider - 'PREVING Consultores S.L.U.' (https://www.preving.com/) and its subcontractor (Sistel which is official distributor of Google Cloud Platform licences). Coordinator of the Business activities (for the external resources working in construction projects only)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The process aims at gathering, storing and screening of Health and safety (H&S) related documentation from external providers (both contractors and sub-contractors) who carry out activities in EUIPO premises, in order to align EUIPO procedures with legal requirements stemming from the Council Directive on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC) and Spanish transposition measures - Real Decreto 171/2004.</p> <p>The H&S controls of all external resources except from the resources working in construction projects are done in a dedicated tool- the security verification portal where all the documentation is stored. The portal is integrated with the access management system that permits the automatic authorisation/non-authorisation/suspension of access on the basis of the result of the control of the H&S documentation.</p> <p>The H&S documents of external resources working in construction projects are stored in the document management system used by the EUIPO- Sharedox.</p>
Purpose of the processing	<p>The control of Health and safety (H&S) documentation by the HS& services provider of EUIPO, during which personal data is processed, is one of the prerequisite for the authorisation of access of external resources and service providers to EUIPO premises. Another purpose of the processing operation is to ensure that EUIPO provides an appropriate level of occupational Health and safety measures thus complying with the applicable legislation in the sphere of occupational risk prevention as follows:</p> <ul style="list-style-type: none">• Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC);• ADM-18-72 regarding the H&S Committee at EUIPO (Acerca del comité de salud y seguridad laboral);• Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales;• ADM-12-05 Concerning occupational risk prevention in the Office;• Artículo 9 del real decreto 1627/1997 sobre disposiciones mínimas de seguridad y salud en obras de construcción (applicable for construction projects only)
Data Subjects	It is compulsory for all external resources and service providers of EUIPO that enter the Office premises to go through the health & safety documentation checks/controls before the access is granted.



Description of categories of persons whose data EUIPO processes and list of data categories

The categories/types of personal data processed are the following:



Retention period	The applied retention policy for health & safety documents lays down 5 years from the end of the service of the person as period of retention for all documents. Personal data in the tool is stored for the period of the contract with the tool provider.
Recipients of the data	<p>Different users have access to data:</p> <ul style="list-style-type: none">• EUIPO internal administrators (Head of CSS; Health and Safety Officer) have access to all information for control purposes;• H&S services provider - 'PREVING Consultores S.L.U.' has access to the information in order to perform the control of the documentation;• Coordinator of the Business activities (for the external resources working in construction projects only). <p>Each company has access to the data of its employees in the Portal. In case of subcontracting, the contractor has access to the data of the subcontractor's employees and in some cases may be responsible for the submission of their data.</p> <p>Access to the data can be given to providers of Google for the purposes of Customer support, response, diagnosis and resolution services, incident tracking, responding to customer queries, and technical support.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>The data of the external resources (excluding the data of the external resources working in construction projects) is sent to the Security verification tool provider who stores it at Google Cloud Platform, Zone europe-west1-b (Ghlin, Hainaut, Belgium) European Economic Area (EEA). The data storage provider is certified in ISO 27001 and applies all necessary physical and IT security measures to protect the data. EUIPO has validated these security measures in the Security risk assessment linked below.</p> <p>It must also be noted that GCP does not have direct access to the information, however, even if not accessible by Google, it could still be transferred outside of the EU as part of the services provided by the subprocessors. Google employs subprocessors from the US, Europe, Asia and India for the purposes of Customer support, response, diagnosis and resolution services, incident tracking, responding to customer queries, and technical support. The full list of subprocessors is located here: https://cloud.google.com/terms/subprocessors. For transfers of data outside of the EU, and in particular for transfers to subprocessors, Google implements model contract clauses. The standard model is located here: https://cloud.google.com/terms/eu-model-contract-clause. Google is also registered in the Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active.</p> <p>In case of transfer of personal data, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.</p>



General Description of security measures	<p>The security measure applied are as follows:</p> <ul style="list-style-type: none">• The access to the data in the Portal will be secured through the use of security policy of passwords and users who will have different roles and levels of permissions. As user names are linked with an email address, then users can be a pool of people sharing an account, or single users. Different user profiles will be created, depending of the access to the data.• Access Control system implemented and roles defined to ensure that information can be accessed only by those required to access it.• Data stored at Google Cloud Platform, Zone europe-west1-b (Ghlin, Hainaut, Belgium) European Economic Area (EEA), certified in ISO 27001.• Physical Access control system compliant with CSA CCM v3.0, SSAE-16 / ISAE 3402, SOC 2 Type II.• Full protection at Core Switches with systems IPS and NGFW. Servers with ESET File Security antivirus, with centralized management and automated updates and scanners.• Encrypted communication channels (TLS v1.2 and VPNs) for secure communication of data.• Information is backed up to ensure integrity and availability of the data.• The Service provider carries out monitoring of the systems and periodic penetration tests to ensure that any vulnerability is promptly identified and fixed.• The service provider has an incident management protocole that includes communication of data breaches to EUIPO. More information can be found in the Security Requirements and the Security risk assessment provided by EUIPO. - <p>The security measures of the Document management system Sharedox where the documentation of the external resources working in construction projects is stored are according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement control of H&S documentation: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/aa247304-9675-4db1-a9d3-f8d183248520
EDPS Prior consultation	NO



Reference number	DPR-2018-012
Name of the processing operation	Departmental registers of activity
Last Updated:	20/06/2019
Controller Organizational entity	EUIPO
Controller contact details	For queries, the DPC of the Department owner of the register should be contacted. https://insite.prod.oami.eu/dpo/who-to-contact#DPCNetwork
Name and contact details of processor	IECISA-ALTIA – DTD Operations service provider Other service providers from the Department may be involved in the management of the registers.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	As part of operational activities of the Office, Departments sometimes keep registers of activity. These registers normally include the information of a task and the persons involved in the task (responsible and affected users), therefore requiring to store the personal data of those involved in the activities of the register. Examples of these registers of activity are: <ul style="list-style-type: none">• Action logs.• Exception logs.• Internal Department incident logs.• Internal Department risk logs.
Purpose of the processing	Personal data is collected in these registers to ensure it is possible to follow-up with those involved in the activities collected in the register. It must be noted that registers of activity are not used for measuring individual performance.
Data Subjects	EUIPO Staff, and service providers of EUIPO
Description of categories of persons whose data EUIPO processes and list of data categories	The following information is normally collected in a register of activity: <ul style="list-style-type: none">• name and surname;• organisational assignment (department, area and/or service);• link to the activity (responsible, affected user, or similar).• Request number, if associated with a ticketing system, such as Remedy/MyServiceDesk• Additional personal data, such as the email or location, may be collected, depending on the nature of the register of activity.
Retention period	Information is kept for the period that the activity in the register is being completed. Once the activity is complete, information is kept for up to three years (the standard ISO audit cycle), as evidence for audit purposes.
Recipients of the data	In general terms, personal data included in a register of activity is not shared with any recipients. That said, it is possible that information collected in a register of activity is made available to either Internal or External auditors, as evidence.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Information that is stored in Sharedox, Y: drive and other Office tools is protected by the security measures implemented for EUIPO systems:</p> <ul style="list-style-type: none">• Systems require username and password to access.• Authentication and authorization based on roles.• Systems are installed in security hardened servers with access control measures and protected by username and password. No anonymous access allowed.• Server is physically protected at the Data Processing centre.• Network security configured to prevent external threats from accessing the servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6b5f91cb-883c-4f81-b7ec-9b54eddb1302</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-013
Name of the processing operation	Social Assistance
Last Updated:	28/06/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of the Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Human Resources Department of EUIPO is offering a social mediation service to its staff members and their families.</p> <p>The consultation and assessment service of the welfare officer covers both professional (communication, stress, conflicts, burn-out, etc.) and private matters (adaptation, specific problems, etc.). The welfare officer also carries out individual and collective activities in prevention, assistance and, where the need arises, social accompaniment (social “follow-up”).</p> <p>The consultation with the welfare officer is entirely voluntary. Consultations may be made on matters relating to family, money, psychological issues, administrative issues, adjusting to the environment and cultural issues, health, conflict management, relationships and miscellaneous matters.</p> <p>Most consultations are carried out verbally, either via a phone conversation or via a face to face interview with the welfare officer. The welfare officer does not keep any “social file” and uses emails to extract aggregate data from them for the purpose of reporting about her work to her supervisors. Emails are also used for purposes of follow up of cases and extraction of statistic data which is anonymised.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of the processing of data is to enable EUIPO's to offer a social mediation service to its staff members and their families. According to the need of the staff member making a request for this service, data are processed with the purpose of carrying out an analysis of the person's situation in order to give the appropriate practical assistance and psycho-social aid. The main aim of this service is to assist in reconciling professional and private life and to secure the most favourable personal conditions for each individual to develop their potential.</p> <p>The welfare officer carries out her duties in accordance with Article 1 of the Staff Regulations and with the code of deontology of the International Federation of Social Workers http://ifsw.org/</p> <p>The welfare officer reserves the right to process personal data without the consent of the person concerned, on the grounds of “protecting the vital interests of the data subject” (Article 5.1.(e) of Regulation (EU) 2018/1725) only when it is strictly necessary.</p>
Data Subjects	EUIPO's officials, temporary and contract staff members Seconded National Experts and Trainees



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>Personal data processed:</p> <ul style="list-style-type: none">- Identification of the data subject (full name, personal number, address, family composition /spouse/ partner/ children/ other family members). It concerns EUIPO's staff members in activity and retired staff members;- Data concerning the person's family situation;- Salary and family allowances (if relevant to the nature of the request);- Possible different medical opinions (Medical Service or JSIS, doctor, etc.) and social data along with the proposed assistance;- Compiling, analysis and management of individual cases in the framework of practical help in order to support staff in a difficult situation. <p>When doing the request for assistance, the staff member provides most information referring to his/her personal data. However, the welfare officer may consult data of the person concerned stored in HRD database, on a need to know basis and strictly necessary to analyse the case.</p>
<p>Retention period</p>	<p>Personal data are stored in the email box of the welfare officer for a period of 2 years to allow for eventual follow-up and extraction of statistical data. This period is extended to 5 years if a follow-up of your case is necessary.</p> <p>Nevertheless, the data subject may opt out of the above mentioned retention periods by explicitly requesting it to the social worker.</p> <p>Data are kept beyond 5 years in case of complaint and further judicial procedure. In that case, all documents are kept until the end of the judicial procedure.</p> <p>Data are deleted as soon as no longer required in the case at hand.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Most of the processing operations are done orally (phone conversations, bilateral interviews). The welfare officer alone has access to the data subject's personal data and keeps in emails the details of requests for assistance. Such data may be disclosed to the person concerned and/or to any related family member depending on the cases . No other persons have access to personal data, except if necessary and on a strict need to know basis, for example:</p> <ul style="list-style-type: none">- References made to specialists (e.g. doctors, psychologists, lawyers, specialized social services), upon prior approval of both the data subject and the specialist;- Details of medical nature transmitted directly by the data subject (or at his/her request by the welfare officer to the Medical Service doctor and/or JSIS Ispra doctor for medical advice (e.g.: hospitalization/ serious illness/ or any other situation depending on the request);- The social services of other institutions/agencies in case of joint handling of a case;- Data may be transmitted to the relevant national social services for staff no longer employed by EUIPO / or if national assistance is required;- Data may also be transmitted to the data subject's hierarchy (e.g.: Head of Service/ Director/ Appointing Authority /or authorized delegated person) if the personal situation of the data subject has an impact on the work environment/ organization) and requires solutions at work (e.g.: medical absences / conflict at work with the authorization of the person concerned); <p>Personal data of the data subjects, as well as details of emails kept by the welfare officer are not disclosed to any recipient without the data subject's prior unambiguous, free and informed consent. The transmission of such data is done on a need to know basis and is strictly limited to only what is necessary.</p> <p>In exceptional cases data transfers may be necessary to protect the vital interests of the data subjects under Article 5.1. (e) of Regulation 2018/1725.</p> <p>In case of need to transmit certain administrative details of the case, on a temporary basis to other recipients on a strict need to know basis (e.g.: Legal Service) , the transmission of data is done in compliance with Articles 9 and 46-50 of the Regulation (EU) 2018/1725.</p> <p>The data are not used for any other purposes nor disclosed to any other recipients.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>Only a limited number of authorized persons working in these procedures have access to data on a strict need to know basis for assistance to the staff member concerned.</p> <p>Emails: details of data related to requests for assistance are only kept by the welfare officer in emails and held securely so as to safeguard the confidentiality and privacy of the data therein. The email system is password protected under single sign-on system and automatically connected to the user ID. The standard security measures of EUIPO's MS-Exchanges is applied. Access to the social worker's computer is password protected.</p> <p>Paper files: no paper files are kept by the welfare officer, neither by the Human Resources Department. Medical documents related to requests for social assistance are only kept by the Medical Service according to the security rules of storage for such documents.</p> <p>All data are kept according to the standard EUIPO's security measures for confidential documents.</p> <p>Hard copies of documents, if any, are stored in locked cupboards with keys available only to the welfare officer. Should there be a need for transfer of documents containing personal data, the welfare officer would mark all documents "confidential" in their respective headers, on routing sheets, or on envelopes.</p> <p>In accordance with Article 4. 1. (b) of Regulation (EU) 2018/1725, such data will not be processed for any other purposes or used in support of measures or decisions regarding any particular individual.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on processing operations for Social Assistance: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/40729335-318f-4b9a-8760-600e8bac1401</p>
<p>EDPS Prior consultation</p>	<p>YES</p>



Reference number	DPR-2018-014
Name of the processing operation	Social Financial Aid
Last Updated:	28/06/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO is offering a social financial aid service to its staff members and their families. EUIPO grants two types of social financial aids:</p> <ul style="list-style-type: none">- Salary advance : may be granted only as an exceptional measure and only to staff members in particularly difficult situations- Complementary financial aid for disability : may be granted to officials and temporary staff in active employment if the person concerned by the disability is at least 30% physically disabled and/or at least 20% mentally disabled according to the evaluation of the EUIPO's medical officer based on the scale laid down by the Inter-institutional Medical Board. <p>When analysing the case, the welfare officer will take into account all relevant health, social and family situation of the staff member concerned.</p> <p>Most consultations are carried out verbally, either via a phone conversation or via a face to face interview with the social worker. The welfare officer does not keep any "social file" and uses emails to extract aggregate data from them for the purpose of reporting about her work to her supervisors. Emails are also used by the welfare officer for purposes of follow up of cases and extraction of statistic data which is anonymised.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of the processing of data is to enable EUIPO's to offer a social financial aid to its staff members and their families. According to the need of the staff making a request for this service, data are processed with the purpose of carrying out an analysis of the person's situation for the granting of social financial aid.</p> <p>The welfare officer carries out her duties in accordance with Article 1 of the Staff Regulations and with the code of deontology of the International Federation of Social Workers http://ifsw.org/ .</p> <p>The welfare officer reserves the right to process personal data without the consent of the person concerned, on the grounds of "protecting the vital interests of the data subject" (Article 5.1.(e) of Regulation (EU) 2018/1725) only when it is strictly necessary.</p>
Data Subjects	EUIPO's officials, temporary and contract staff members.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>Personal data processed:</p> <ul style="list-style-type: none">- Identification of the data subject (full name, personal number, address, family composition/ spouse/ partner/ children / other family members) . It concerns EUIPO's staff members in activity;- Personal data of the person's family situation;- Family and education allowances (if relevant to the nature of the request) ;- Possible different medical opinions (Medical Service or JSIS, doctor, etc.) and social data along with the proposed assistance;- Financial data of the person concerned and his/her family members to the extend of what is strictly necessary and on a need to know basis (e.g.: payslips and any other document necessary to analyse the situation);- Invoices;- Bank account number;- Disability certificate stating the degree of the disability (Medical data are submitted to the Medical Service in a closed confidential envelope);- Justifications/ opinions and detailed assessment of the person's situation in order to take a decision for granting/ or not granting a financial aid;- Compiling, analysis and management of individual cases in the framework of practical help in order to support staff in a difficult situation;- Social financial file with details and necessary documents justifying the payment of the social aid. (These documents are only kept by the social worker).
<p>Retention period</p>	<p>Personal data concerning the granting of financial aid are stored for a period of 7 years for reasons of budgetary discharge in conformity with the Financial Regulations.</p> <p>Data are kept beyond 7 years in case of complaint and further judicial procedure. In that case, all documents are kept until the end of the judicial procedure.</p> <p>Data are immediately deleted as soon as no longer required in the case at hand.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Most of the processing operations are done orally (phone conversations, bilateral interviews). The welfare officer alone has access to the data subject's personal data and keeps in emails the details of requests for assistance. Such data may be disclosed to the person concerned and/or to any related family member depending on the cases . No other persons have access to personal data, except if necessary and on a strict need to know basis, for example:</p> <ul style="list-style-type: none">- References made to specialists (e.g. doctors, psychologists, lawyers, specialized social services), upon prior approval of both the data subject and the specialist;- Details of medical nature transmitted directly by the data subject (or at his/her request by the welfare officer to the Medical Service doctor and/or JSIS Ispra doctor for medical advice (e.g.: hospitalization/ serious illness/ or any other situation depending on the request);- In case of aid for disability, an ad hoc committee consisting of the EUIPO's medical officer, the welfare officer and the Authorizing Officer. Where appropriate, two experts appointed by the Director Executive of EUIPO, according to the nature of the disability, are consulted;- The social services of other institutions/agencies in case of joint handling of a case;- The data subject's hierarchy (e.g.: Head of Service/ Director/ Appointing Authority/ Authorizing Officer and/or authorized delegated persons) for decision taking and approval of payments;- A limited number of authorized staff of the Finance Department/ HRD and PMO working with financial files (only to the extent necessary to process payments/remunerations);- External staff (IT administrators) could also have access to the electronic data Emails/ and Excel tables for payments of remunerations/advances), if necessary for technical reasons. <p>Personal data of the data subjects, as well as details of emails kept by the welfare officer are not disclosed to any recipient without prior unambiguous, free an informed consent of the person concerned. The transmission of such data is done on a need to know basis and is strictly limited to only what is necessary.</p> <p>In exceptional cases data transfers may be necessary to protect the vital interests of the data subjects under Article 5.1. (e) of the Regulation (EU) 2018/1725.</p> <p>Transmission of data is done in compliance with Articles 9 and 46-50 of the Regulation (EU) 2018/1725.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>Only a limited number of authorized persons working in these procedures have access to data on a strict need to know basis for assistance to the staff member concerned.</p> <p>Emails: Details of data related to requests for assistance are only kept by the welfare officer in emails and held securely so as to safeguard the confidentiality and privacy of the data therein. The email system is password protected under single sign-on system and automatically connected to the user ID. The standard security measures of EUIPO's MS-Exchanges is applied. Access to the social worker's computer is password protected.</p> <p>Paper files: data concerning social financial aid is kept in secured locked cupboards in Human Resources Department by the welfare worker. Medical documents related to requests for financial aid are only stored by the Medical Service according to the security rules of storage for such documents.</p> <p>Excell tables concerning the payment of advances of salary/ remunerations are stored in HRD by a limited number of authorized EUIPO's and PMO staff working in salaries .</p> <p>The individual social financial file and hard copies of documents, if any, are stored in locked cupboards with keys available only to the welfare officer. Should there be a need for transfer of documents containing personal data, the welfare officer would mark all documents "confidential" in their respective headers, on routing sheets, or on envelopes.</p> <p>All data are kept according to the standard EUIPO's security measures for confidential documents.</p> <p>In accordance with Article 4.1. (b) of Regulation (EU) 2018/1725, such data will not be processed for any other purposes or used in support of measures or decisions regarding any particular individual.</p> <p>All the application forms used and the decision regarding the granting of salary advance will contain data protection provisions .</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on processing operations for Social Financial Aid: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/e512cdfc-362c-4130-b92e-195c7a7a4035</p>
<p>EDPS Prior consultation</p>	<p>YES</p>



Reference number	DPR-2018-016)
Name of the processing operation	Processing operations of personal data in the general HR Database
Last Updated:	13/12/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	HRD - Line managers - Head of Staffing, Development and Recognition Service - Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Personal data of EUIPO's staff is actually processed in HR database "Allegro" / SAP SuccessFactors/ Alfresco / ShareDox , Excel /Access/ Outlook. The HRD is working on changes of database from HR "Allegro" to "SAP SuccessFactors" in the cloud. The HR database "Allegro" will be deactivate after the transfer of all its modules to "SAP SuccessFactors" in the cloud.



Purpose of the processing	<p>Personal data is processed solely for administrative purposes and for an efficient management of the staff's rights and obligations in accordance with the rules of the Staff Regulations (SR), the Conditions of Employment of Other Servants of the European Union (CEOS) and the administrative decisions related hereto.</p> <p>The purpose of the processing operation is:</p> <ul style="list-style-type: none">- to manage internal staff (establishment plan / internal mobility) and external staff (seconded national experts/ trainees/ consultancy and agency staff);- to manage the budget planning/ budget cycle/ workforce planning and monitoring of Title 1 of the budget (SAP-BPC);- to manage recruitment (career/ staff skills, expertise, talents / internal mobility/ team leader's profile to share knowledge within a professional network;- to manage the individual's rights and obligations (entitlements, salary, allowances - Annex VII of SR);- to manage the renewal of temporary and contract agent's contracts;- to manage termination of service/ employment and pensions (Annex VIII of SR);- to manage data of staff travelling on mission/ working conditions, working time, absences and teleworking;- to manage data of staff members participating at the "20 years Medal Ceremony" (EUIPO staff having 20 years of service at EU institutions/ agencies and retired staff;- to manage access to the Joint Sickness Insurance Scheme (JSIS) online from outside the EUIPO network (name, surname, birth date, personal number, mobile phone identification, email address). The information is required by the European Commission Authentication System (ECAS) for the maintenance of personal data of EUIPO staff;- to update personal data in HR database "Allegro" and HR database "SAP SuccessFactors" in the cloud according to the annual confidential declaration and the declaration on conflict of interests / to update contact information (staff addresses, personal and work telephone numbers, emails, contact persons, staff member's relatives). Giving the personal mobile phone number is entirely voluntary. However, it is important that EUIPO's Security Services (Infrastructure and Buildings Department) could send text messages to staff member's phone in case of emergency;- to confirm to the Security Service (IBD) that the person for whom the staff member has requested an access card to EUIPO is his/her spouse or legally recognised partner. In case of change of situation, the Security Service will be informed by the HRD in order to deactivate the access card of the person concerned. <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Data Subjects	<p>Statutory staff members: bound by the SR and CEOS (officials, temporary agents, contract agents, special advisers) and whenever relevant for the processing of individual rights, data related to the relatives of the staff members concerned.</p> <p>Non-statutory staff: seconded national experts, (SNE's) trainees, agency staff (interims) and staff from external contractors/sub-contractors (consultancy) delivering services to EUIPO.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The following data are processed only on need to know basis and by authorized staff of HRD:</p> <ol style="list-style-type: none">1. Staff members: full name, photo, personnel number, gender, marital status, date/place of birth, nationality, address, email, telephone, private mobile phone, contact persons/relatives, CV, education, languages, expertise/talent, position applied for, type of contract and post, contract duration, grade/step, task allocation, administrative status, assignment, appraisal assessment, promotion, training in/outside EUIPO, conditions of work, working time and absences, salary, type of allowances, data necessary for the termination of service/employment in particular for the calculation of pensions and allowances, type of family record, spouse/family income (necessary for the determination of an eventual right to allowances), persons treated as dependent children/ conflict of interests and annual confidential declaration/ data of removal, travel expenses/place of origin, bank account, data related to missions and all relevant data supplied by the staff member necessary to manage his/her individual file. Team Leader's profile published in Insite includes the name, photo and expertise of data subjects .2. Agency staff (interims) and Trainees: full name, photo, personal number, nationality, identity card/passport, date of birth, gender, assignment, time management, contract /traineeships details, CV and traineeship reports.3. External provider's staff: full name, CV (photo voluntary), nationality, date of birth, gender, assignment, start/ end date of services delivered at EUIPO, reference number and employer (email);4. Staff members participating at the 20 years "Medal Ceremony": full name, number of years of service, dates of entry/ end of service. <p>The photo taken by the Security Service (IBD) to new recruited staff will be uploaded to the staff member's service card. Under consent of the data subject, his/her photo will appear on the Office search directories: MyPortal (HRD "SAP SuccessFactors") / "Who is Who" (CS - Insite) / and "Who to Contact" (CS - Insite). Data subjects have the possibility to withdraw consent to the publication of their photo by selecting the correspondent option in myPortal link. For questions staff members can send an email to hrddpc@euipo.europa.eu. The photograph will be withdrawn in the maximum period of 15 days.</p>
<p>Retention period</p>	<p>Any document/ data important for the staff member's career is stored in the personal file and kept during 8 years after the extinction of all rights of the person concerned and of any dependents, and at least 120 years after the birth data of the person concerned.</p> <p>For data that can be destroyed in a shorter period of time, the EUIPO retention period and schedule for files will be applied (including data related to services delivered by external contractor's staff: consultancy and agency staff).</p> <p>Data related to the management of skills, expertise, talents which are stored in "SAP SuccessFactors in the cloud" will be kept during the duration of the employment activity of the data subject at EUIPO.</p> <p>Data uploaded from HR "SAP SuccessFactors" to the "Mass Notification System" (personal mobile and work phone number) will be maintained for as long as a user has a contractual commitment to the Office.</p> <p>Data uploaded from HR "SAP SuccessFactors" to ICLAD-Event database" will be kept as indicated in the Privacy Statement published by ICLAD in Insite/ICLAD/Data protection.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data

Access is given to HRD statutory staff processing data / Academy staff (for trainings) / ICLAD-Event Database administrator (events concerning statutory staff, SNE's and trainees).

HRD statutory staff may have support of interim staff or trainees to carry out their functions. A declaration of commitment and confidentiality prior to starting working must be signed.

EUIPO managers, as defined by the current organization chart, have access to the CV of all staff (languages, education, training, professional experience, technical skills and expertise, personal interests and competencies). The line managers may access the following information regarding their subordinates: working time, conditions of work, absences, career, contracts, assignment, appraisal and any other data necessary for the management of their staff. The line manager's assistants and staff working in the department's central team in charge of resources issues may also be authorised to access the same personal data as their line managers. Data of external staff (consultancy) is accessible to EUIPO managers of the departments for which the external consultants deliver services, as well as to the staff authorised by them.

Within the framework of data processing to manage inventory/ maintenance and working spaces, the following data will be disclosed from HR database "SAP SuccessFactors" to "Rosmiman tool" (IBD): full name / department / workplace location/ email address/ internal phone number / internal and external staff status / employee number.

IBD (events organisation) and CS (ceremony videos) will receive from HRD the list of data subjects (full names) who confirmed their participation at the "20 years Medal Ceremony".

For organizational purposes EUIPO's staff members have access to the planning of absences of their colleagues working in the same Department/ Service . This information is strictly limited to the name/ surname/ dates of requested absences not yet approved /and dates of absences approved. There is no access to the reasons of absence.

The staff of Customer Services Department (Information Center) have access to data with regard to staff member's availability in order to attend incoming calls and generally improve EUIPO user's satisfaction. The access to data is limited to the absence's planning of HR database, which has been integrated in the CRM system, without any information referring to the reason of absences.

The Academy has access to the following data kept in "HR database Allegro" : training requests, full name and service of data subjects, languages, historic and certificates of training.

The PMO / Finance Area for salary payments and other services within the framework of the SLA-PMO_EUIPO. The Litigation Service and Court of Justice in case of complaints. The OLAF within the framework of their enquiries. Under request, access may be given to the Internal Audit Service/Court of Auditors and to other institutions (officials transfer).

Other recipients:

- Data of management skills/ expertise/ talents/erecruitment candidates (job applications) / ecandidatures (traineeships) and seconded national experts

are processed in "SAP SuccessFactors" in the cloud (storage in Germany and Holland). The photo attached by data subjects to their CV will be stored in the same recipient.

- Data of salaries/ workforce planning/ budget monitoring and task allocation on Excel / Access are processed in "SAP BPC" (EUIPO servers). The final

e-payslips are processed in OpenText tool;

- Alfresco/Sharedox: data of the personal file of EUIPO's staff members is transferred to OpenText (on premises) that is linked to "SAP

SuccessFactors" in the cloud;

- Agency staff (interims) and data of staff of consultancy service providers are processed in "SAP SuccessFactors" in



the cloud. CV's of external

consultancy staff are stored in "Sharedox - FD" and accessible to HRD for data processing according to Guidelines on management of external resources;

- Missions will be processed in "Concur" cloud system (storage in France);

- HR database "Allegro" and its modules are stored in My SQL database. HR "SAP" database is stored in Oracle server;

- The following data is uploaded to the Office Directories - Insite "My Portal"/ "Who is Who" and "Who to Contact": name, surname, email address, phone

number and the data subject's photo (under the data subject's consent) ;

- The following data is uploaded from HR "SAP SuccessFactors" to "ICLAD-Event database":

name/surname/email/department of statutory staff, SNE's and

trainees;

- Outlook.

EUIPO contractors and subcontractors might have access to data for maintenance and development of the applications supporting "HR Allegro" and "SAP SuccessFactors" under request and supervision of EUIPO.

SNE's and Agency staff employers will have access to a portal in "SAP SuccessFactors" containing the offers on SNE's secondment and "interim staff" posted by EUIPO. The employers can upload the candidatures of their employees to the portal and submit them to EUIPO for selection according to the offers of employment available at EUIPO. Data required: candidate's full name/country of origin/ email/ telephone and CV's (pdf) in order to add them to the process of selection done by EUIPO.

The traineeship report and references on the work done by trainees at EUIPO can be sent by them to third persons (e.g.: candidature for a job).

Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.

Access to JSIS online: For the access to JSIS online from outside EUIPO network, staff members have to communicate their personal mobile phone number to HRD. These data will be disclosed to the Digital Transformation Department (DTD) which is registering all staff access information to ECAS in a centralised way. Data required by ECAS: EUIPO login, personal number, birth date, email address, full name and mobile phone. The ECAS is managed by the European Commission DG DIGIT / Identity & Access Management (IAM) Service Desk.

Mass Notification System : The Security Services (IBD) will use this system to disseminate (by telephone text messages) security related information to EUIPO's staff (internal / external) in case of emergency/ crisis situation. For internal staff, the personal mobile and work phone numbers will be uploaded from HR "SAP SuccessFactors" to the "Mass Notification System". For external staff, IBD will collect these data from the service provider's tool.

The data are not used for any other purposes nor disclosed to any other recipient.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member; line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein. Reports to third parties, external to the EUIPO, may contain collective or more detailed data on an anonymous basis.</p> <p>Personal data shall be anonymised when the data subject's identification is not necessary (migration of data).</p> <p>Staff members would be asked to consent to the release of individual data other than the normal organisational information and reporting (e.g.: organizational chart).</p> <p>Cloud systems "SAP SuccessFactors and "Concur" have 24/7 security monitoring and alerting, security incident and threat response procedures, and automated security measures to prevent unauthorised access.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" and "Concur" are also certified in ISO 27001.</p> <p>A declaration of confidentiality is signed by the persons having access to the HR database.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data in the HR database is published in Insite/ HRD/Data : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f09879dd-8e22-4bee-a069-1242a4152909
EDPS Prior consultation	NO



Reference number	DPR-2018-020
Name of the processing operation	Monitoring of Absence from Work due to Sickness or Accident - Medical Control Visit/Examination
Last Updated:	27/09/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service HRD IDCQ Hospitales y Sanidad, S.L.U.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data related to the monitoring of absence from work due to sickness or accident and medical control visit / examination.</p> <p>It concerns officials, temporary agents, contract agents, seconded national experts and trainees.</p> <p>EUIPO is assisted by an external Medical Service for the monitoring of absences from work due to sickness/accident, as well as for medical control visits/examinations.</p> <p>Medical checks are carried out by examining doctors to validate absence for sickness and accident and to check the link between diagnosis and prognosis. The Medical Service may contact the patient's doctor who issued the certificate in order to clarify some details when the diagnosis is not clear.</p> <p>The staff member concerned shall notify the Office of his incapacity as soon as possible and at the same time state his/her current address.</p> <p>Staff members may at any time be required to undergo a medical examination arranged by the office to determine whether they are able to carry out their duties and to check whether the absence is justified.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>



Purpose of the processing	<p>The processing of individual medical data is necessary to assure that the absence from work due to sickness or accident is justified and that its duration is proportional to the nature of the illness / accident.</p> <p>The processing of data is done in compliance with:</p> <ul style="list-style-type: none">- Articles 10 to 16 and Article 25.1.(h) of Regulation (EU)2018/1725;- Articles 59 to 60 of SR, Articles 16 and 91 of the CEOS;- Decision N° ADM 18-32, dated 06/08/2018, on the definition of the responsibilities of the EUIPO's Medical Service;- Commission Decision N°92-2004, dated 06/07/2004, introducing implementing provisions on absences as result of sickness or accident and applied at EUIPO by analogy;- Decision N°ADM10-10Rev of 12/09/2011, Decision N°MB 16-13 of 31/05/2016 and Decision N°MB-18-14, dated 05/06/2018;- The Conclusion of the Heads of Administration N°221/04, dated 19/02/2004 on the access of officials to their medical files ;- The Organic Law 15/1999 (Spain) and "Ley 41/2002 - autonomia del paciente (Spain)" .
Data Subjects	<p>Statutory staff members: officials, temporary agents and contract agents.</p> <p>Non-Statutory staff: seconded national experts and trainees</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <p>Surname, forename, gender, date of birth, personal number, personal address, email address, telephone numbers, Service / Department of assignment, medical certificates and its date of reception by the Medical Service, partial or total limitation of work (e.g. 100%, 50%..), name and speciality of doctors, periods of absence.</p> <p>The following additional data can be processed depending on the specificity of the cases: medical records related to sick leaves / accident (reports, analysis, and diagnosis); date of medical examinations / treatment / specialist visit; details of whether or not the person concerned attended the medical control / examination; conclusion of current treatment: justified / unjustified absence, ability and date to return to work; job related problem (if applicable); details of the invalidity procedure (if applicable).</p> <p>The medical certificate sent by the staff member to the Control Area of the Medical Service, must comply with the formal requirements:</p> <ul style="list-style-type: none">• must be legible;• must state clearly that the staff member is unfit to work;• must include the patient's family name and first name;• must indicate where the patient is staying and• must indicate the foreseeable duration of the incapacity for work, specifying the start and end dates. <p>If the formal requirements are missing in the medical certificate, the medical officer will contact the staff member and/or the treating doctor who issued the certificate (by telephone, email, etc.), so that it can be corrected.</p>



Retention period

Data relating to sick leaves are kept by the Medical Service in the individual medical file of the person concerned.

Files of the control doctor concerning medical visits/examinations of staff members are kept as long as the person concerned is in activity at EUIPO, after which time they are archived with the individual medical file of the person concerned.

The retention period can be extended up to 30 years, after the date of end of service of the person concerned .

Non-medical related documents: email reminders, planning of medical appointments, etc. are not kept in the medical records and are automatically deleted once it has served its informative purpose at every medical review.

External medical service:

On the last day of the contract with the external Medical Service (or at any time upon EUIPO requests), EUIPO shall receive from the contractor the hard copy including all relevant administrative and medical information treated during the contract.

Due to legal obligations, the external provider stores personal data according to the Spanish Law .

In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.



Recipients of the data	<p>Medical Service: only the doctors, the nurse and the assistant have access to the medical file.</p> <p>The external Medical Service can only access to EUIPO's staff health data under the supervision of the Office, in particular concerning the processing of data, the categories of data to be processed, the disclosure of data and how data subjects could use their rights according to Regulation (EU) 2018/1725.</p> <p>Data on sick leave / accident may also be communicated to another institution or agency when the staff member is transferred. Transfer of data is done after the consent of the data subject and only to persons authorized to have access to health data.</p> <p>Administrative details of the file (such as name, email address, telephone number, periods of absence) may be transferred to a restricted number of authorised staff of HRD working on absences.</p> <p>In addition, certain administrative details may be disclosed on a temporary basis to the Director of HRD, the Head of Service of Entitlements and Staff Welfare Service, the Social Assistant, the Appointing Authority (AA), the Authority Authorized to Conclude Contracts (AACC), the Legal Service and the Court of Justice in case of complaints.</p> <p>The Reporting Officers and their delegates are also informed about the absences of their staff, but only on the dates of sick leave of their staff.</p> <p>IT technicians (internal or external staff) may have access to the Medical database "Access" for maintenance and software renewal. They do not have access to the medical data.</p> <p>The data disclosure or transfer is done in compliance with the relevant current legislation and established case law. No personal data is transmitted to parties which are outside the recipients and the legal framework mentioned.</p> <p>Authorised staff dealing with administrative documents in connection with health data is requested to sign a declaration of confidentiality equivalent to a health professional.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>Medical files on paper are stored by the Medical Service in secured archives that are accessible only to the doctors, the nurse and the assistant.</p> <p>Some medical data related to monitoring of absences from work due to sickness or accident are stored in electronic format in "Access database" (EUIPO's Server).</p> <p>"Access database" is password protected under sign-on system and automatically connected to the user ID and general password.</p> <p>The access to medical files is granted only to the Medical Service. Medical files are kept according to the security measures of EUIPO Information Systems under confidential documents.</p> <p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorisation process. Mechanisms of access tracking and monitoring of use of systems are established. Authorized users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on Monitoring absences from work due to sickness or accident – Medical Control Visit / Examination: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6766021d-79fd-4cd0-b84c-f7664dc026fb
EDPS Prior consultation	NO



Reference number	DPR-2018-021
Name of the processing operation	Invalidity Committee procedure
Last Updated:	30/08/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service – HRD IDCQ – Hospitales y Sanidad , S.L.U.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>Processing individual medical data within the framework of the Invalidation Committee procedure .</p> <p>The application to launch an invalidation procedure may be made at the request of the person concerned or at the request of the Administration based on a recommendation of the Medical Service. In the latter case, the person's sick leaves must have totaled at least 12 months in any period of three years.</p> <p>The decision whether to launch an invalidation procedure is taken by the Appointing Authority (AA) or the Authority Authorized to Conclude Contracts (AACC) .</p> <p>The medical grounds are never forwarded. Anything which relates to medical information remains protected by medical confidentiality. Only the doctors involved may access to this information.</p> <p>The Invalidation Committee consists of three doctors:</p> <ul style="list-style-type: none">- the first is appointed by EUIPO;- the second is appointed by the person concerned;- the third is appointed by agreement between the first two doctors. <p>Should the person concerned fail to appoint a doctor, the President of the Court of Justice of the European Union shall appoint one.</p> <p>The Invalidation Committee has the task:</p> <ul style="list-style-type: none">- to determine whether or not the person concerned is fit to work;- to determine the causes of unfitness to work;- to indicate how frequently revisions should be carried out. <p>The proceedings of the Invalidation Committee are secret and are covered by medical confidentiality.</p> <p>The Invalidation Committee shall decide either that the person concerned fulfils / or does not fulfill the conditions for recognition of invalidation under the SR /CEOS.</p> <p>On the conclusion of its proceedings, the Invalidation Committee delivers an opinion to the AA or AACC, but does not mention medical grounds for its decision. Medical grounds are placed in the medical file of the staff member concerned .</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The Human Resources Department (HRD) is responsible for conducting procedures relating to invalidation in accordance with Article 59(4) of the Staff Regulations (SR), Articles 16 and 91 of the Conditions of Employment of Other Agents (CEOS).</p> <p>The purpose of the processing operation is to obtain from the Invalidation Committee a conclusion as to whether the official, temporary staff member or contract staff member concerned should be granted invalidation or should resume professional activities.</p> <p>The processing of personal data is subject to Article 10, 15 and 16 of Regulation (EU) 2018/1725 .</p>
Data Subjects	Statutory staff: officials, temporary agents and contract agents



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <ul style="list-style-type: none">- Information from the medical personal file: surname, forename, gender, date of birth, personal number, grade, date of take up employment, Service / Department of assignment, personal address, email address, telephone numbers, medical certificates and its date of reception by the Medical Service, partial or total limitation of work (e.g. 100%, 50%..), name and speciality of doctors, periods of absence.- The following additional data can be processed depending on the specificity of the cases: medical records related to sick leave / accident (reports, analysis, and diagnosis); date of medical examinations / treatment / specialist visit; details of whether or not the person concerned attended the medical control / examination; conclusion of current treatment, justified /unjustified absence, ability and date to return to work; job related problem (if applicable).- The date of the application to launch an invalidity procedure, who launched the application (the person concerned or the Administration), the total number of days of sick leave over the three-year period preceding, procedural letters sent to the doctors, administrative correspondence, details of the invalidity procedure, report, medical and administrative conclusions.
Retention period	<p>Medical data and considerations which led to the conclusions of the Invalidity Committee are recorded in a medical report which is filed in the medical file of the person concerned.</p> <p>The retention period of the invalidity files can be extended up to 30 years, after the date of end of service of the person concerned, under the same procedure as for medical files .</p> <p>Non-medical related documents: email reminders, planning of medical appointments, etc. are not kept in the medical records and are automatically deleted once it has served its informative purpose at every medical review.</p> <p>External medical service:</p> <p>On the last day of the contract with the external Medical Service (or at any time upon EUIPO requests), EUIPO shall receive from the contractor the hard copy including all relevant administrative and medical information treated during the contract.</p> <p>Due to legal obligations, the external provider keeps the data according to the Spanish Law .</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The Medical Service (MS), the AA/ AACC and the members of the Invalidation Committee.</p> <p>External doctors (if need) and other institutions (if transfer of the data subject). Transfer of the medical data/ file is done after the consent of the data subject).</p> <p>The external Medical Service can only access to EUIPO's staff personal health data under the supervision of the Office, in particular concerning the processing of data, the categories of data to be processed, the disclosure of data and how data subjects could use their rights according to Regulation (EU) 2018/1725.</p> <p>Certain administrative details of the file may be disclosed to a restricted number of authorised staff of Human Resources Department working on Invalidation files, the authorised staff of PMO and FD (salary / pensions).</p> <p>The same administrative data may be disclosed on a temporary basis to the Director of Human Resources Department, the Head of Service of Entitlements and Staff Welfare Service, the Social Assistant, the Legal Service and the Court of Justice in case of requests, complaints, litigations, or any other administrative procedure . Upon request, administrative details may also be disclosed to the Internal Audit and the Court of Auditors.</p> <p>Data may also be communicated to another institution or agency when a staff member is transferred .</p> <p>IT technicians (internal or external staff) may have access to the Medical database "Preven" and "Access" for maintenance and software renewal. They do not have access to the medical data.</p> <p>The data disclosure or transfer is done in compliance with the relevant current data protection legislation and established case law. No personal data is transmitted to parties which are outside the recipients and the legal framework mentioned.</p> <p>Authorised staff dealing with administrative documents in connection with health data is requested to sign a declaration of confidentiality equivalent to a health professional.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>Medical data kept on paper by the Medical Service is stored in secured archives that are only accessible to the Medical Service.</p> <p>The database used on the premises of EUIPO by the Medical Service ("Preven" and "Access") are both password protected under sign-on system and automatically connected to the user ID and general password. The access to medical data is done only by the Medical Service. Medical data are kept according to the security measures of EUIPO Information Systems under confidential documents.</p> <p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorisation process. Mechanisms of access tracking and monitoring of use of systems are established. Authorized users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>EUIPO service-provider/contractor ("IDCQ Hospitales y Sanidad S.L.U.") use their own security systems for data processing.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement relating to the Invalidity Committee procedure in EUIPO: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/4ccfe8dc-b8dd-4758-893d-eb123c56e5a5
EDPS Prior consultation	NO



Reference number	DPR-2018-023
Name of the processing operation	Processing of personal data on "Safety to speak up within the EUIPO" - follow up activities related to the Staff Satisfaction Survey 2018.
Last Updated:	04/07/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Independent external provider Willis Towers Watson (WTW)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>Following the feedback given by EUIPO's staff on the Staff Satisfaction Survey 2018 and in the context of continuous organisational improvement, the Office would like to follow-up on the results obtained concerning the "safety to speak up in EUIPO".</p> <p>In particular, the 2018 Staff Satisfaction Survey results have shown, inter alia, that there are staff concerns about whether it is safe to speak up within the EUIPO. Under the category of Supportive Culture, the question "I believe it is safe to speak up in EUIPO" has been rated as one of the lowest scoring questions and significantly below the EU Norm. Consequently the Office wishes to further explore this topic in order to identify and understand the underlying causes so as to be able to address the issue appropriately.</p> <p>To this aim, the same independent external provider, Willis Towers Watson (WTW) which carried out the Staff Satisfaction Survey 2018 has been requested by EUIPO to conduct a follow-up activity composed of a pulse survey and focus groups.</p> <p>In this context, WTW will identify a representative sample of staff members (around 160) to whom a short "Questionnaire" (7 questions) will be sent individually by email to collect feedback on this topic followed by the organisation of 12 focus groups with the same representative sample of staff members to discuss the topic. The representative sample will aim to cover different departments, hierarchical levels, working conditions (teleworkers/non teleworkers), working relationships, function groups, grades, length of service, and age and gender. The sample will be decided by WTW based on the list of EUIPO statutory staff and Seconded National Experts (SNEs) provided by the Human Resources Department. The names of staff composing the representative sample will be made known to the Office in particular to the staff of the Human Resources Department working on this activity in order to provide support with the logistics as necessary and to the respective line managers for operational reasons. The focus group meetings will be organised and attended by WTW professionals only. Individual responses and information shared during the focus group sessions will be kept confidential and not shared with EUIPO.</p> <p>Each participant will receive information (briefing pack) by email sent by WTW including an individual link to access the survey. The participation to the pulse survey and the focus groups is entirely voluntary. For those who do not wish to participate in the survey and subsequently the focus groups, they will not suffer any negative consequence and detriment. Only WTW will know the names of those who have declined their participation and such information will not be shared with EUIPO.</p> <p>The conditions of confidentiality are stated in the contract signed between the Office and the provider and will be strictly respected by both EUIPO and WTW.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of processing data is to identify the causes of staff concerns about "Safety to speak up within the EUIPO" and to find solutions for improvement.</p> <p>For these reasons, Willis Towers Watson (WTW) will process data within the follow-up activity composed of a pulse survey and focus groups.</p>
Data Subjects	<p>Statutory staff: Officials, temporary agents and contract agents.</p> <p>Non-statutory staff: Seconded National Experts</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>For the purpose of the selection of the representative sample, the following information related to all EUIPO statutory staff and SNE's will sent to the provider by the Office:</p> <ul style="list-style-type: none">• Department, service;• Hierarchical level (Team Leader, Staff);• Teleworker regular (yes or no);• Working relationship (official, temporary agent, contract agent or SNE);• Length of service (less than 5 years, 5 to 10 years, more than 10 years);• Age (under 35 years of age, 35 to 45 years of age, 46 to 55 years of age, 56 years or older);• Gender;• Function group; Administrator (including Contract Agent function group 4) or Assistant (including Contract Agent function groups 1 to 3); and• Electronic address. <p>For the participants in the follow-up exercise, in addition to the above the following personal data will be processed:</p> <ul style="list-style-type: none">• Their opinions expressed in the initial phase via responding to the survey and during the focus groups sessions.
<p>Retention period</p>	<p>The personal data will be kept only for the time necessary to achieve the purpose for which they will be processed, consequently will remain in the database until the results have been completely analysed and the final report with the aggregated results has been delivered. Any Personally Identifiable Information (PII) is deleted from WTW systems no later than 6 months after the event closes.</p> <p>The aggregated anonymous data on groups (excluding individual - level data) will be kept until the next survey is carried out, for the purpose of research analysis and reporting, and specifically, to make a comparison.</p> <p>Only the aggregated final report and analysis of results (consolidated data) will be stored in EUIPO document management system (in HRD confidential folder) for 10 years according to the Office's security measures.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
<p>Recipients of the data</p>	<p>The processed and aggregated results of the survey and the focus groups (anonymous) will be accessible to all EUIPO staff in the form of a final report summarising the overall findings and results.</p> <p>An additional and more detailed report (with aggregated anonymous results of the survey) will be accessible to the following persons: Director of the HRD, the Head of Staffing, Development and Recognition Service (HRD), the EUIPO management and a limited number of staff of the HRD and other Departments working in the survey.</p> <p>The information concerning the detailed results will only be shared with people necessary for the implementation of such measures on a need to know basis. The data are not used for any other purposes nor disclosed to any other recipient.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Processing of personal data are carried out by a service provider Willis Towers Watson (WTW) and the Human Resources Department, acting as the data controller for this processing will monitor and verify the implementation of the required organisational and technical security measures necessary to ensure compliance with the Regulation (EU) 2018/1725.</p> <p>Pre-populated personal data and pseudonymised answers are stored on the WTW servers according to their security measures and processes access being provided only to the core project team and technical support on a “need to know” basis.</p> <p>Only the final report and analysis of results will be stored on EUIPO servers and in ShareDOX (confidential HRD folder), according to the security measures of the EUIPO Information Systems.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein. The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	PS on “Safety to speak up within the EUIPO” follow-up activities related to the Staff Satisfaction Survey 2018: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f56a7109-91dc-4509-802e-62f857dd9a1d
EDPS Prior consultation	NO



Reference number	DPR-2018-024
Name of the processing operation	Food safety trainings of external resources in EUIPO
Last Updated:	27/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processor: Head of Common services, IBD External processor: 'PREVING Consultores S.L.U.'
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	According to the Guidelines for the management of external resources: External resources shall only participate in training sessions for knowledge that they cannot obtain outside the Office, such as the Office's business applications, working procedures, safety and security rules. With this regard, EUIPO catering services provider's staff occasionally receives trainings on specific F&S procedures established by EUIPO. The trainings have the objective to inform them how to use specific facilities/installations in the office or how to implement specific control procedure (control of products, installations, providers, etc.) in order to prevent food safety incidents /correct performance / promote good practices.
Purpose of the processing	The purpose of the processing operation is to ensure that all catering services provider's staff is informed about specific F&S procedures established by EUIPO (control of products, installations, providers, etc.) thus reducing the possibility that food safety incidents occur/reoccur.
Data Subjects	Catering services provider's staff (external resources)
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data processed is in the attendance sheet signed by each participant in the F&S trainings and consists of name, surname and signature.
Retention period	The data is stored for the period for which the provider of catering services has a contract with the office .
Recipients of the data	The F&S officer from 'PREVING Consultores S.L.U.', H&S responsible and Head of Catering services in EUIPO have access to the data.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement on the procedure for the organisation of F&S trainings: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/92d7c93e-2de1-437f-a921-b7dc6280941c
EDPS Prior consultation	NO



Reference number	DPR-2018-025
Name of the processing operation	Preparation and transmission of BoA files to the General Court and the Court of Justice
Last Updated:	25/03/2019
Controller Organizational entity	Boards of Appeal
Controller contact details	Head of the Knowledge, Information & Support Service (KIS) of the Boards of Appeal, Boards of Appeal (BoA) European Union Intellectual Property Office (EUIPO), Avenida de Europa 4, ES-03008 Alicante, Spain BoA-KIS-Information@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>According to Recital 30 Regulation (EU) 2017/1001 (EUTMR) and Art. 72 EUTMR, BoA decisions are subject to appeal before the General Court (GC) and the Court of Justice (CJ). The GC and the CJ have jurisdiction to annul or alter the contested BoA decision. In order to allow for judicial review, BoA has to transfer the file of the contested decision to the Courts.</p> <p>When an appeal has been filed against a BoA decision, the KIS service of BoA is responsible for preparing the complete BoA file for the GC and the CJ and make it available to the Courts. The file (in PDF-format) is placed on an FTP server where the Courts can pick it up and the Office's litigation unit (ICLAD) is informed via e-mail each time a file is made available. For a more detailed description of the process see QSD-0200-Work instruction Prepare File for Litigation (Annex 1) and IG – Preparation of BoA-Files for the CG & CJ (Annex 2).</p>
Purpose of the processing	Comply with the legal obligation to provide the GC and CJ with the files of BOA decisions under appeal before the Courts; allow for an effective judicial review.
Data Subjects	Parties, their representatives, third parties (e.g. witnesses or experts) and EUIPO staff members involved in the specific case under appeal
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data of the parties, their representatives and third parties (e.g. witnesses or experts) as well as of EUIPO staff involved in the case under appeal; the personal data included in the file consists of: - names and contact details - job positions - very rarely: health related personal data in case of a request for re-establishment of rights (restitutio in integrum) - very rarely: date of marriage and information on religious orientation in case where a marriage certificate is submitted to prove change of name
Retention period	The electronic files are deleted from Sharedox after the court decision has become legally binding and the case is closed.
Recipients of the data	The processor (DMO of BoA) and its back-up; the responsible persons at the GC and CJ
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to this processing operation is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">- role-based access control to the systems and network;- logical security hardening of systems, equipment and network;- physical protection via secure Data Centre. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC).</p> <p>Access control systems with adjustable permissions are implemented to control the access that a user or group has to the files or folders containing the production data.</p> <p>The server where the files are stored for retrieval by the Courts are protected.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Data protection statement on processing personal data in the preparation and transmission of BoA files to the Courts: https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/DPS-on-processing-personal-data-in-the-preparation-and-transmission-of-files-to-the-GC-and-CJ_en.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-026
Name of the processing operation	Issuance of the Laissez Passer (LP) of the European Union (EULP) - Travel document
Last Updated:	26/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Joint Controller organizational entity	Other
Joint Controller contact details	General Human Resources and Security, Unit HR - A.3 - HR Information Systems and Reporting Sector HR.A.3.002 - Reporting Systems and User Services
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

The Council Regulation 1417/2013 of 17 December 2013 lays down a new form of LP (travel document) issued by the European Union and replacing the Regulation (ECSC, EEC, Euratom) N° 1826/69. It requires to the Commission to act as coordinator notably for processing purposes and to ensure compliance with Regulation (EU) 2018/1725.

Regulation N°1417/2013 indicates that the new LP should comply with the security standards and technical specifications applicable to the national travel documents issued by Member States pursuant EU legislation and keeping compliant with the specifications of the International Civil Aviation Organisation (ICAO).

This includes that common security standards and interoperable biometric identifiers should be integrated into the LP in addition to the biographical data. It is for each Institution /Agency to capture and provide the biographical data of the applicants/special applicants and to transfer them to the Commission LP Central Service.

The Commission is Controller of the process from the moment it receives those biographical data (via the application and delivery form) up to the moment it puts an end to the retention of such data, except for the steps performed by EUIPO at its demand, notably in case of remote delivery.

The EU LP is a travel document granted to a list of officials and other servants of the Union and, since the adoption of Regulation 1417/2013, to certain new categories of special applicants namely family members of Members of an institution, family members of officials and of other servants of the Union who fulfil the conditions laid down in Article 23 of SR and Articles 11 and 81 of the CEOS, the officials and other servants of the Union who do not fulfil the conditions laid down in the above referred Articles as well as their family members, the Seconded National Experts and their family members, the junior professionals in Delegation (JPD) and their family.

The Council Regulation 1417/2013 has foreseen a precise sequencing of roles throughout the issuance process:

- A first phase of enrolment (capture of personal data both biographical and biometrical (facial image and fingerprints) which is covered by the provision of Article 2, paragraph 1: "For the purpose of this Regulation each institution may conclude agreements with other institutions with a view of creating synergies and alleviating the costs".

In this context it has been agreed that the Commission would act on behalf of all other institutions/agencies.

EUIPO signed a SLA with the Commission for the issue of the LP for EUIPO staff.

The Commission would run two locations of the enrolment stations, one in Brussels and one in Luxembourg and support the running of the European Central Bank (ECB) centre in Frankfurt.

- For the two other steps of the issuance process, production of the LP and its personalisation, Regulation N° 1417/2013 establishes that the Commission shall designate an entity to be responsible "taking due account of the sensitive nature of the documents to be produced" and in accordance with the provisions applicable to the award of contracts. Finally, once personalised, the LP are sent back to the Commission which check their quality and readability and ensures the delivery of each of them hand by hand or through remote delivery to the final holder.

Biographical personal data:

- EUIPO will be in charge of the pre-enrolment phase which consists in the capture of the biographical data of the EUIPO LP applicants necessary to establish the LP. The list of the biographical data collected is presented in Annex I of Council Regulation N°1417/2013.

- EUIPO will send those data to the Commission for it to process them (integrate them into the system that will eventually encrypt them).

- The Commission processes the biographical data of the applicants received from EUIPO.

Biometrical personal data:

- The Commission captures (in Brussels and in Luxembourg LP Central Service) the biometrical data of the applicants, except for those captured by the ECB centre, where it is operated by the ECB but as a part of an overall unique system.

- The Commission processes the biometrical data of the applicants once received encrypted and via secure link. In a certain number of cases, the enrolment will take place using a mobile station able to be transported abroad, to be used by EU Agencies in Europe or by EU Delegations in the world. This will be limited to the minimum. The biometrical data will be then exported on a secure USB key and brought back to the Commission LP Central Service for further processing.



- The Commission verifies the correctness and quality of the personal data collected, prepares the data in files ready to be used in the personalisation of the LP and proceeds to their encryption.
- The Commission sends the encrypted biometrical and biographical data of the EUIPO applicants to the external contractor for further processing (personalisation of a blank booklet / LP with those data).
- The Commission receives the personalised LP and checks the correctness of the document. This includes a check of the correctness of the personal data included on the vision page as well as in the clip (facial image and finger prints).
- The Commission stores the personalised LP during the necessary period before delivery (normally few days but considering a maximum of 3 months).
- In case of hand-to-hand delivery, the Commission during the delivery redoes together with the applicant a check of the correctness of the data included whether visible or not (stored in the LP chip) with the exception of the fingerprints no longer accessible.
- In case of remote delivery (taking place outside the Commission LP Central Service in Brussels or in Luxembourg) this operation is done only on the visible data by the Institution / Agency of origin. The remote delivery is considered an exception to the system. It includes the possibility that this remote delivery be operated outside the European borders, in the office of EU delegations situated in third countries. Remote delivery might become nevertheless the normal way for the Agencies, bodies and joint undertakings not located in Brussels or in Luxembourg.
- The Commission exchanges information on the progress of the application via the exchange/transmission/reception of the application form which contains the biographical data collected and information related in some cases to the members of the family of the applicants.
- The Commission is likely to be responsible for keeping the paper version of the finalised application form once the process of delivery has ended.
- The Commission will liaise with the different Institutions /Agencies in charge of managing the lost and stolen LP to that end it will communicate non personal data unless a specific need appears or in case of urgency. This may include that the data subject is not informed or has not his consent collected beforehand. This may occur in case his/her own security is at stake.

Automated/ Manual Operations:

The application form used to sustain the whole process of LP issuance is filled in manually within EUIPO and transmitted electronically (encrypted and digitally signed) and on paper to the LP service run by the Commission (by valise/DHR). The subject data are copied from that application form during enrolment. Biometric data are captured during enrolment with the physical presence of the data subject.



Purpose of the processing	<p>The purpose of the processing of personal data is to allow the issuance of EU Laissez Passer to EUIPO staff and/or non-staff (special applicants as defined by the Council Regulation N°1417/2013 responding to international recommendations and the European legislation.</p> <p>Legal basis: Protocol N° 7 on Privileges and Immunities annexed to the Treaty / Article 23 of the SR and Articles 11 and 81 of the CEOS.</p>
Data Subjects	<p>EUIPO statutory staff and / or certain categories of special applicants according to Regulation N° 1417/2013 and by decision of the EUIPO AIPN on who could request an EU LP.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Biographical personal data:</p> <p>Staff identity including surname, name, nationality, date of birth, gender, place of birth, function, job titles, staff type, position, statutory link, posting/address, family position including the information (surname, name, date of birth, nationality, gender, address, link with the original holder) for each family member applying for a LP in connection with an application for / or the holding of a LP by the original holder.</p> <p>Detailed data included in each personalised LP may differ following the specific requirements inherent to each demand, in particular the position in the diplomatic list of mentions.</p> <p>Biometrical personal data:</p> <p>Facial image (photo), fingerprints and signature of the holder. No fingerprints for children under 12 years old.</p>



Retention period

The need of storage has been considered under two different approaches:

1. The need to store the personal data used is inherent to the process in place. Between the moment the application is made by the applicant to EUIPO up to the moment he receives the personalised validated LP from the delivery service of the Commission there is a need to store the data collected in a database. This storage avoids a discontinuity into the process in case a problem or a doubt arises. It takes place in the LP service run by the Commission for the steps under its responsibility. It covers both biographical and biometric data.

2. The need to store those personal data for a longer period is linked to the life-cycle management of the EU LP. It must remain proportional to the purpose served. For that reason:

- Fingerprints and digital signature are stored only for the time necessary to the effective and successfully delivery of the LP. They are deleted at that time (a few days depending on the day the future holder takes to come and collect the personalised document with a maximum of 3 months). The LP is destroyed if not delivered.

Nevertheless, they remain stored in the chip contained into the LP under the responsibility of the holder including for their submission to the controls operated at the borders.

Independently of the purpose of the LP process, each Institution/Agency stores the personal biographical personal data of its applicants and special applicants according to their own rules.

EUIPO will keep a scanned copy of the application form for the period of validity of the LP. The original form of EUIPO applicants will be kept by the Commission EU LP central service.

Within the first year a scanned version of the paper version is done and electronically stored in a database managed by the Commission LP central service for the remaining period of validity of the LP.

At the end of 6 years, both the paper version and the scanned version of the application form are destroyed. The Commission will repeat this process for each new application.

Biographical personal data:

For EUIPO own staff: personal data existing and extracted from Allegro HR, SAP SuccessFactors, Open Text tool or Sharedox (i.e. name, nationality, birth date, administrative position, title, etc.) have the same retention period as already existing for such data and collected for other purposes (i.e: data stored in the personal file during 8 years after the extinction of all rights of the person concerned and of any dependents, and at least 120 years after the birth data of the person concerned).

The Commission will retain these data for a period of time limited to the duration of validity of the issued EU LP.

Personal biographical data are deleted upon expiration of a maximum of 6 years validity period running as from the date of issuance of the LP.

For special applicants (members of the family or ad-hoc holders): the retention period is limited to the duration of validity of the issued EU LP (maximum 6 years). Personal biographical data, if not kept under other processes are deleted upon expiration of a maximum of 6 years validity period running as from the date of issuance of the LP.

At the end of those retention periods, biographical data are erased.

Biometrical personal data:

The retention should be limited to the need for all holders (normal and /or special applicants as well as ad hoc holders):

For facial image, fingerprints and digital signature at the level of the contractor: the retention period is limited to the time needed to issue the EU LP after successful validation and fulfilment of the acceptance process (normally a few days and up to a maximum of 3 months).

For fingerprints and digital signature at the level of the Commission:

The retention period is limited to the time needed to issue the EU LP after successful validation and fulfilment of the acceptance process (a few days and up to a maximum of 3 months).

For facial image at the level of the Commission: the retention period is limited to the time needed to issue the EU LP



(maximum 6 years).

At the expiration of the validity of the EU LP, it must be returned to the Commission to be cancelled and/or partially or totally destroyed. After this process, in case it is cancelled but not totally destroyed, it may be kept by the holder. In this later case, the data (both biographical and biometrical) continue to be accessible on the invalid LP under the sole responsibility of the holder. Access to biometrics would nevertheless continue to depend on the use of specific technical devices not commercially easily accessible.

For the registration of the Video surveillance: the retention period would be aligned on the one foreseen in the Belgian legislation.

In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.



Recipients of the data	<p>Who has access to data:</p> <p>EUIPO: The Head of Service and authorized staff of the Entitlements & Staff Welfare Service - HRD, the Director of HRD and staff authorized by the Director and EUIPO IT administrators (internal and/or external staff); The Commission LP central service in Brussels and in Luxembourg and authorized staff in Frankfurt; The national authorities responsible for the border control; The authorities in charge of security at the border including airports, maritime or fluvial ports; The national authority responsible for the management and lost and/or stolen document, including those of non EU countries; The Appointing Authority (AA) and the Authority Authorized to Conclude Contracts (AACC); The disciplinary bodies in the institution, notably IDOC; OLAF; The auditors, Interpol, SIS II, Sirene; Europol, Cefpol; The central alert system 24/7 within the remit of its competencies and on a need to know basis;</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures

The management of the personal data within the issuance process will be submitted to specific secure rules taking into account the ICAO recommendations and the EU legislation for EU national passports and other travel documents including EU LP.

In certain cases, the enrolment will be done in a mobile station. In this case, the use of mobile station for enrolment will allow to re-create the same conditions for the capture of the biometrics data as in the fixed enrolment stations with the difference that the staff in charge of the use of the mobile station will be also in charge of encrypting the collected data on a secure USB key and to carry it back to the Commission LP central service in Brussels for further treatment (next step: enrolment). The data will be down-loaded in the system and erased from the USB keys upon downloading.

Acting as central service for the issuance of the EU LP, the Commission processes the personal data of EUIPO's staff in compliance with Regulation (EU) 2018/1725 and applies the

Commission's information systems security policy.

EUIPO IT security measures apply to the personal data processed in EUIPO, notably by:

- Recording which personal data has been communicated, at what time and to whom: Registration of transmissions/collection/handling of personal data to a party is lodged in a central database, as part of the standard process of EU LP issuance. The logging information includes data, time and identifier of user who authorized the transmission. Depending on the phase of the process, this logging information allows to know to whom it is communicated.
- Ensuring that it will subsequently be possible to check which personal data have been processed, at what time and by whom.
- Ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution/body: The issuance process of the EU LP is providing a central service to all EU institutions and Agencies. The terms of collaboration and service provided are defined in a service level agreement composed of a common section applicable to all parties and a specific section where Institutions and Agencies can specify particular handling or arrangements. The handling of personal data is in the common section of the service level agreement.

The transmission of personal data between EUIPO and the Commission is done through the encrypted email box EUIPO-EULP-HRLP-ALC. The Commission EU LP Central Service is responsible for keeping the paper version of the finalised application once the process of delivery has ended. The transmission of originals will be done by Valise/DHL. Recipients have access to personal information only on a need to know basis. The respect of the segregation of tasks among the staff in charge of the different phases of the issuance as well as the requirement of a dual access for each critical step entailing the processing of the encrypted data guaranteed that data under process are well protected against undue access. A permanent trailing of the files, auditing of the processes, reporting of activities and events and registration of the life cycle management applied to each file also ensure that the process keeps in line with the internal control standards for effective management.

Recipients only access to the personal data they need to know never exceeding the scope of their specific missions. Currently access to fingerprints is strictly ring-fenced to the internal verifier of the integrity, correctness and correct interoperability of the personalised Laissez Passer before delivery. Such verification at the border remains an exception.

Data processed by EUIPO are stored in secure IT applications (ShareDox, Encrypted Outlook, HR "Allegro" database and "SAP SuccessFactors" in the cloud) according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorised recipients. For "SAP SuccessFactors" data is stored in the cloud in servers in SAP Germany and SAP Holland data centers.

EUIPO HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein. Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.

The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.





For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Issuance of the Laissez Passer of the European Union (EU LP): http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3db3c47a-0629-4023-956c-b04dd8948583
EDPS Prior consultation	NO



Reference number	DPR-2018-027 (update of DPN-2017-032)
Name of the processing operation	Management of EUIPOFIT activities
Last Updated:	09/08/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Hospitality team leader External processor: EUIPOFIT service provider (EULEN) European Union Intellectual Property Office
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPOFIT is a concept focused on integrating work-life balance among EUIPO personnel. The aim is to enhance well-being at the workplace and to improve the general health of EUIPO staff through the promotion of:</p> <ol style="list-style-type: none">1) sport and leisure facilities such as: GYM, relaxation rooms, leisure rooms and outdoor installations;2) sport activities such as basic activities classes and loan of bicycles;3) sport events and tournaments. <p>There are several data bases that contain personal data of EUIPOFIT users:</p> <ul style="list-style-type: none">• EUIPOFIT registration form that all EUIPOFIT users have to fulfil and sign in order to inscribe themselves as EUIPOFIT members and accept the rules of use of the EUIPOFIT installations;• Classes attendance form where all basic activities classes´ attendees register themselves;• Bicycle Loan Acceptance form where all EUIPOFIT users that want to loan a bicycle inscribe themselves and accept the rules of use of the bicycles;• Declaration of consent (only for external resources) . By signing this declaration, the users voluntary give their consent for the processing of personal data as described in the Privacy statement provided to them. This declaration should only be filled in by external resources (not statutory staff of the EUIPO) because the legal basis for processing their data is Article 5.1. (d) of Regulation (EU) 2018/1725 ('the data subject has unambiguously given his or her consent'). EUIPO internal staff should not fill in this declaration because the legal basis for processing their data is compliance with EU Financial regulations as per Article 5.1. (a) of Regulation (EU) 2018/1725. <p>All EUIPOFIT users have to register themselves as EUIPOFIT members fulfilling the EUIPOFIT registration form. All EUIPOFIT members can attend the basic activities classes or can loan a bicycle fulfilling the corresponding forms. EUIPO defrays the costs of access to the gym, basic activities classes and loan bicycles for all statutory members and their partners.</p>
Purpose of the processing	<p>The personal data in this process is collected and stored for several purposes as follows:</p> <ul style="list-style-type: none">• accountability and financial control on the monthly reports and payment claims received from the EUIPOFIT service provider;• elaboration of statistics and reports on the use of EUIPOFIT,• monitoring of users´ interests and preferences regarding EUIPOFIT services (sport facilities, activities and events) thus ensuring the users´ satisfaction.
Data Subjects	EUIPOFIT members (users)



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data collected in the EUIPOFIT registration form is as follows: name, surname, personal number, company/organization, signature</p> <p>The personal data collected in the Classes attendance form is as follows: name, surname.</p> <p>The personal data collected in the Bicycle Loan Acceptance form is as follows: name, surname and signature.</p> <p>The personal data collected for the purpose of organisation of sport events and tournaments is processed as described in the notification for the management of meetings and events.</p> <p>The personal data collected in the Declaration of consent consists of name, surname and signature of the user.</p>
Retention period	The data is stored for the maximum period of 5 years from the date of the discharge for the financial year to which the data relates.
Recipients of the data	Hospitality team responsible for EUIPOFIT management and EUIPOFIT service provider EULEN.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The documents on paper are locked in secure cupboards to which only authorised people have access.</p> <p>Some personal data may be stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>As from 30/09/2017, the staff of the Service Provider has signed a Confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement EUIPOFIT :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/48644657-c085-4c49-b0d1-3ebad9265f0b</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-029
Name of the processing operation	Access management in EUIPO
Last Updated:	20/05/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Head of security services, EUIPO Security team in the Infrastructures and Buildings Department and EUIPO staff responsible for the restricted areas. External processors: Security services provider Securitas and its subcontractor Nsecure.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The management of accesses in EUIPO is organised on the basis of the use of:</p> <ul style="list-style-type: none">• Access cards for the management and monitoring of the access to the five zones of EUIPO, according to Decision No ADM 17-26 of 31 March 2017 regarding access to the database of the access control system;• Palm reader for the management of access to highly restricted zones;• Keys for the management of the access to concrete zone/meeting room/office/space;• Specific authorisation for the access of minors (persons under legal age of maturity). <p>The access to the 5 zones of EUIPO (public, semi-public, office, restricted and highly restricted) is done on the basis of the use of access cards. There are several types of access cards: internal staff/ external contractor/ visitor/ service provider/ partner/ retired/ MBBC member and observer/ school & events access card.</p> <p>Security services receive request for access to the office premises through Remedy09 tool (except from accesses for minors and events), register the information in the access control system AEOS and issue/distribute an access card according to the access rights authorised to the person.</p> <p>The following information is printed on the access card: name, surname, personal number, photo and type of card (service provider, external contractor, etc.). All people entering the office installations, except for visitors, events participants and service providers, sign an acknowledgement of receipt of the access cards (T0033 – Acknowledgement of receipt access cards) that explains the use of the card and the processing of personal data related to this use.</p> <p>In order to ensure the management of access to restricted zones, two types of lists are maintained:</p> <ul style="list-style-type: none">• a list of staff members responsible for the management of access to a restricted zone;• lists of people authorised to access a concrete restricted zone. <p>The access to the highly restricted zone is based on the use of the access card and a Palm reader that ensures that the highest security measures are applied.</p> <p>The access to concrete office/location/meeting room is based on the use of keys. Keys can be used as well for accessing the restricted and highly restricted zones but only in emergency situation. All keys are stored in key cabinets and the authorisation to access them is requested through Remedy09 tool (Remedy products Security key request and Key request). The authorised people use their access cards to open the key cabinet and access their keys.</p> <p>The access of minors is authorised upon signing of liability exemption form by the adult that accompanies them. A list of all minors authorised to enter the EUIPO premises and all scanned exemption forms are stored in Sharedox.</p> <p>The access of visitor is requested through the Remedy09 tool. Upon his/her arrival, the visitor signs Risks Information Receipt that contains a data protection disclaimer.</p> <p>Detailed information regarding the processing of personal data in the access management procedure can be found by all data subjects in the Privacy statement visibly placed at the main entrance of EUIPO premises.</p>
Purpose of the processing	<p>The data is processed only with the following purposes:</p> <ul style="list-style-type: none">• Avoid unauthorised people to enter the Office's installations;• Manage the access of authorised people to the five different zones depending on their access rights (visitors, service provider, event, external services, staff's family, etc.);• Close monitoring and control of the access to the restricted and highly restricted areas that represent highest security risk for the organisation;• Ensuring the security and safety of EUIPO staff, premises and patrimony.
Data Subjects	<p>All the people that have an authorisation to enter the EUIPO premises (staff, SNE, MBBC members and observers, trainees, external contractors, service providers, visitors, event attendees, students, retired employees, partners, etc.).</p>



Description of categories of persons whose data EUIPO processes and list of data categories

Data subjects are all people that are authorised to enter the office premises (on a regular basis or as visitors).

1. The personal data collected in the process of the management of the access to the five zones of EUIPO through the use of access cards is as follows:

- Personal data in AEOS: name, surname, personnel number, photo, ID/Passport number and type of card authorised; access level (according to the zone for which the access has been authorised); access related information (time and date of access and access control points where the card has been registered); number of the card and number of the chip of the card; Following finding 6 (recommendation) of the Audit 53 "ISO 27001 Controls – Third Parties": data of the company and the company manager for external services (name of the company, the name of the manager/coordinator and the e-mail) and other data of the person such as email, location and office phone number, department, service.
- Personal data in the list of people authorised to access the restricted and highly restricted zones: personal number, name, surname, restricted area and access card's expiry date
- Personal data in the list of people responsible for a concrete zone: name, surname and corresponding restricted zone for each responsible of a restricted zone.
- Personal data in the Acknowledgement of receipt of the access card (T0033 – Acknowledgement of receipt access cards): name, surname, personal number, type of card of the person, signature and date of delivery.

2. The personal data collected in the process of management of the access through the use of keys is as follows:

- name and surname of the person;
- personal number;
- date of receipt and date of return of the key (In the excel tables in Sharedox)
- access log information (date and hour of access to the key cabinet that are stored only in the keys software).

3. The personal data collected in the process of management of the access to highly restricted zones through the use of Palm reader is as follows:



Retention period

In the process of management of the access to the five zones of EUIPO through the use of access cards the data is stored in the access control system AEOS. Data related to the access logs (date, hour, place of access) in the access control system AEOS is kept for three months according to Art. 2 of ADM-17-26 of 31 March 2017. The rest of the data necessary for the management of the accesses (name, surname, personal number, photo, type of card authorised, access level, email, location and office phone number, department, service, etc.) is stored for 3 months from the date the person has stopped working for the Office. The personal data in AEOS regarding retired staff will be retained for the maximum period of 25 years. In the event that Security services receive information that the person has died/does not any more wish to have an access card for the Office premises, the data will be deleted from the system. The personal data in AEOS regarding official partners of a staff member/retired person will be stored till the staff member has contractual relations with the Office or till HRD/staff member/retired staff informs IBD that the person is not any more considered as an official partner/will not visit the Office premises anymore.

Personal data in AEOS can be stored for a longer period than the one established above only in case the data is necessary for the purpose of an investigation and is erased once the investigation finishes. In any case, the Data Protection Officer will be prior consulted in case such a prolonged retention period is necessary and duly informed upon closure of the case and deletion of data.

Nevertheless, apart from AEOS access management system, part of the data related to the access to the 5 zones is stored as follows:

- Data in the lists of people authorised to access restricted and zones is stored in an Excel table in Sharedox for the maximum period of one year from the date the person has stopped being authorised to enter these areas in order to ensure compliance with audit requirements;
- Data in the list of people responsible for a restricted zone is stored in an Excel table in Sharedox for the purpose of management and control of the access to the restricted areas. This data is stored in Sharedox for the time for which the person performs his/her duties as restricted area responsible (owner);
- Data in the Acknowledgement of receipt of the access card (T0033 – Acknowledgement of receipt access cards) is stored on paper for as long as the person is under contractual obligation;

In the process of management of the access to concrete zone/office/locations/meeting rooms through the use of keys the data is stored in the Deiseter Electronic software and the in Excel tables in Sharedox for the maximum period of 3 months from the date the person has stopped being authorised to use the keys.

In the process of management of the access to highly restricted zones through the use of Palm reader the data is stored in the ULTRA MANAGER 2 software (Recogtech) for the maximum period of 3 months from the date the person has stopped being authorised to use the palm reader.

In the process of management of accesses of minors through the use of Liability exemption form signed by the responsible adult, the data is stored as follows:

- 1) Liability exemption form on paper;
- 2) Excel table with all minors that have been already authorised the access in Sharedox (only for minors accompanied by adult working in EUIPO) .

In case the responsible adult for the minor is a EUIPO staff member or external resource, the data is stored till the minor reaches adulthood or the responsible adult works in EUIPO premises. In case the responsible adult for the minor is a visitor, the data is stored for the maximum period of 2 months.

The data (name, surname, signature) related to the management of visitors' access is stored in AEOS for 3 months and on paper in the document Risks Information Receipt for visitors for the period of 1 month after the day of visit.



Recipients of the data	<p>In the process of management of the accesses through the use of access cards, Security Services team (the officer responsible for physical security and his/her alternate officer) and the external security company (security auxiliaries) have access to all the data. Apart from them, the external security company (technicians and security guards) have access to the data stored in AEOS.</p> <p>According to Art. 2 of ADM-17-26 of 31 March 2017, the officer responsible for physical security and his/her alternate officer may grant limited access to the 'access control database' to individuals of the Office who for reasons related to the performance of their job duties of control of access to restricted areas of the Office may need to consult the database.</p> <p>In the process of management of the accesses through the use of Keys, both Security Services team (the officer responsible for physical security and his/her alternate officer) and the external security company (production technicians) have access to the data in Deiseter Electronic software. The internal security team and the external security services provider have access to the data regarding the management of keys in Sharedox.</p> <p>In the process of management of the accesses through Palm reader software, both Security Services team (the officer responsible for physical security and his/her alternate officer) and the external security company (production technicians) have access to the data in the ULTRA MANAGER 2 software.</p> <p>In the process of management of accesses of minors, Security Services team (the officer responsible for physical security and his/her alternate officer) and the external security company (security guards and auxiliaries) have access to the data in through the use of Liability exemption form signed by the responsible adult. Access to the data in the Excel table regarding minors have the internal security team and the security auxiliaries.</p> <p>H&S team and the security guards have access to the Risks Information Receipt for the visitors.</p> <p>DTD is recipient for the purpose of the use of printers: The information that DTD receives is Personal number and ID card number in accordance with DPN-2017-045 uniFLOW Printing Management - Update.</p> <p>HRD is recipient: HRD receives the personal number and the photo of the card user and stores it in the Success factor data base in accordance with DPN-2018-016.</p> <p>Communication service (CS) is recipient: If the user gives his consent, the photo is transferred to CS and is published on Insite.</p> <p>The responsible people for each restricted areas receive information regarding the access logs attempts in the corresponding restricted area in compliance with Article 3 of Decision No ADM 17-regarding access to the database of the access control system.</p> <p>Personal data can be disclosed to security services of Sabadell for the purpose of organisation of the access to the Sabadell's premises in case you are authorised to access EUIPO installations there as described in the Privacy statement for the Specific Privacy Statement on the processing of personal data in the procedure of managing of accesses to Sabadell's premises.</p> <p>Access card holders can purchase products from the vending machines in the Office. For this purpose, Serunion (catering services provider) receives from Security services the number of the chip of the access card for the purpose of management of purchases/delivery of products done through the vending machines.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to the access management procedure is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>The information on paper is locked in cupboards or in rooms. Their access is restricted only to the authorised people as described in section Who have access to the data.</p> <p>The external provider´s staff signs a confidentiality declaration in order to guarantee the compliance with the confidentiality clause in its contract.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement for EUIPO staff and external resources working in EUIPO. Privacy statement for visitors. :</p> <p>http://sharedox.prod.oami.eu/share/page/repository#filter=path%7C%2FOffice_Docs%2FK%2520INST%2520AFFAIRS%2FK03%2520DP%2FK0305%2520DP%2520Domains%2FDPC-IBD%2F3%2520-%2520NOTIFICATIONS%2FNotifications%2520IBD%2FNotifications%2520IBD%2FAccess%2520management%2520in%2520EUIPO%7C&page=1</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-030
Name of the processing operation	Mass notification system
Last Updated:	27/01/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Head of Common service, IBD Security services in Common services Human Resources Department External processors: Orange Espagne S.A.U. (hereinafter to be referred to as "Orange")
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The mass notification application of Orange 'Comunica SMS' will be used by the Security services in IBD for dissemination of security related information to EUIPO internal staff and external contractors in case of emergency/crisis situations. The system will collect the data (personal and work mobile telephone numbers) of internal staff from the Success Factor data base and of external contractors from the Vetting portal for security verification of external staff. The telephone numbers of external staff will be uploaded by their companies (service providers) in the Vetting portal.
Purpose of the processing	The personal data is collected and processed in order to ensure that EUIPO staff and external resources that access regularly the office installations are duly and timely informed about any emergency/crisis situation or any fact that the security services consider of importance for their security and safety and that could potentially impact their work/life/wellbeing.
Data Subjects	EUIPO internal staff and external resources
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data that will be processed are the mobile telephone numbers (work and personal) of EUIPO internal staff and external resources.
Retention period	Personal data will be stored for as long as the person has contractual obligation to the Office.
Recipients of the data	The following parties will have access to the data: <ul style="list-style-type: none">• Security services in Infrastructures and Buildings Department for who will disseminate the messages;• H&S services provider (only for external contractors) who administrates the Vetting portal and verifies the information provided by the companies;• Orange and its authorised contractors have access to the data. The companies (provider os EUIPO) have access only to the data of their own employees (the company inserts the telephone numbers of their own employees in the Vetting portal);



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>The data is transferred to the secure servers of the mass notification tool provider. All necessary IT and physical security measures are applied in order to protect the data.</p> <p>Orange can involve subprocessors which, based on the information available in the corporate privacy policy, may be located in India, Israel, Morocco, Tunisia and the US.</p> <p>As per the corporate privacy policy, Orange has implemented the following safeguards when transferring customer personal data outside of Europe:</p> <ul style="list-style-type: none">• For Orange Business Services entities, binding corporate rules and EU Commission standard contractual clauses.• For external suppliers, Orange ensures that at least one of the following is implemented:<ul style="list-style-type: none">o Specific contracts approved by the European Commission which give Customer Personal Data the same protection it has in the European Uniono If the service provider is in the US, the transfer is done under the Privacy Shield.
General Description of security measures	<p>The application is stored on secure servers. The service provider of the application has ISO 27001 certification.</p> <p>More details on the security measures can be found in the document Privacy and Security Risk Assessment linked below.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statements for the use of the mass notification system:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/442bbecc-284b-4880-955e-ed37f410465d</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-031
Name of the processing operation	Teleworkers' occupational risk assessment
Last Updated:	27/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: H&S officer Action Plans Manager IBD, EUIPO External processor: Health & Safety (H&S) services provider - 'PREVING Consultores S.L.U.'
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>According to the decision Admin-04-30 from 2005, the EUIPO complies with the provisions of Law 31/95 for occupational risk prevention. These provisions state that the office should assess the health and safety risks related to the work place and work environment of its staff and inform the workers regarding the applicable preventions measures. According to Administrative decision ADM-04-10 of the President of the EUIPO of 29th of March 2012 concerning teleworking, teleworkers in EUIPO shall have the same working conditions as staff working at the premises of the Office.</p> <p>The Human Resources Department with the technical cooperation of Digital Transformation Department (DTD) and Infrastructures and Buildings Department (IBD), H&S team, are responsible for the implementation of this decision and the overall functioning of teleworking. H&S external provider in IBD receives through Remedy the requests for assessment of the H&S risks of the work places of new teleworkers or of teleworkers that have changed their telework place (address). H&S external provider in IBD visits the work place of the teleworker and assesses the H&S risks. The action plan manager ensures that there is a working extinguisher at the teleworker's work place. This procedure includes processing of personal data in several documents:</p> <ul style="list-style-type: none">• Data collection sheet;• H&S risks assessment sheet;• List of teleworkers (2 Excel sheets).
Purpose of the processing	The personal data is processed for the purpose of ensuring the compliance with the applicable legislation (Law 31/95 for occupational risks prevention and to Administrative decision ADM-04-10). Moreover, the personal data is processed in order to ensure that all prevention measures are taken in order to avoid any potential incidents/accidents related to the working environment of EUIPO staff, thus ensuring its safety.
Data Subjects	EUIPO staff to whom regular teleworking (equal or higher than 50% of teleworking time) is allowed/assigned according to Administrative decision ADM-04-10.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data processed in the Data collection sheet is as follows: name, surname and address of the teleworker; signature of the responsible for the H&S risks assessment.</p> <p>The personal data processed in the H&S risks assessment sheet is as follows: name, surname and address of the teleworker.</p> <p>There are 2 List of teleworkers as follows:</p> <p>1st Excel sheet used by H&S team: name, surname, address, description how to reach the address, telephone number of the teleworker.</p> <p>2nd Excel sheet used by Action plans manager: name, surname, email.</p>



Retention period	<p>The retention period for the documents used by H&S team is 5 years after the person leaves the office. The applied retention policy for health & safety documents lays down 5 years as period of retention for all documents except for the document proving the medical capability of the worker for the tasks to be performed, or resignation to the medical examination when possible that will be retained for 10 years in the general case and for 30 years in the case of occupational noise exposure.</p> <p>The retention period for the Excel sheet used by the Action Plans Manager is 18 months.</p>
Recipients of the data	<p>H&S internal team and the external provider Preving have access in order to perform the occupational risk assessment.</p> <p>Facility management team has access to the data (Action plans manager and FM operations team have access to the table related to the extinguishers for control purposes; Maintenance team has access to the data for the purpose of resolution of incidents).</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>Personal data on paper is stored in locked cupboards.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>General Privacy statement Teleworking:</p> <p>http://sharedox.prod.oami.eu/share/proxy/alfresco/slingshot/node/content/workspace/SpacesStore/4ce19ecc-4f5a-4c5d-a354-5512be6efbd7/Teleworking.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-032
Name of the processing operation	Organisation of the access of EUIPO staff/external resources to Sabadell's and European Commission's premises.
Last Updated:	23/09/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Head of Common services, IBD Human Resources Department (only for the management of the access to the European Commission premises) External processors: External security services provider Securitas, subprovider Nsecure. Security services Sabadell (applicable in the process of organisation of the access in Sabadell). Security services in the European Commission (applicable in the process of organisation of the access in EC). European Union Intellectual Property Office (EUIPO)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In order to perform their duties and responsibilities some of EUIPO staff and external resources has to access on a regular basis Sabadell building's premises where the Data Processing Centre and some warehouses of EUIPO are located;</p> <p>Other EUIPO staff has to access the European Commission's premises in order to perform its duties (missions, meetings, etc.).</p> <p>Security services in IBD facilitate the organisation of the access to these premises by collecting the necessary data and sending it to the Security services of Sabadell bank and the Commission so that they can authorise the access and issue the badges.</p> <p>In the process of organisation of the access to Sabadell's premises, the access cards are requested only for the staff/resources who have to enter on a regular basis in the Data Processing Centre or the warehouses of EUIPO located in the Sabadell's premises near the EUIPO buildings.</p> <p>In the process of organisation of the access of EUIPO staff to the European Commission (EC), the request for the badge comes directly from the person who needs to access on a regular basis the Commission's premises. Security services in IBD send to the requester the template provided by the Commission for authorisation of access pass named Application for an access pass to the European Commission buildings. Once the requester has fulfilled the template, IBD checks with HR whether the information provided by the requester is correct and, in case of confirmation, sends it to the Commission.</p> <p>In order to ensure that the badges will be timely and duly renewed or returned to the issuing authorities (Sabadell or Commission), Security services in IBD maintain Excel tables with information regarding the people who have been authorised the access to Sabadell bank's and the Commission's premises.</p> <p>Moreover, in order to organise the payment for the badges in the current year and to plan the budget for badges' renewal for next year, HRD regularly consults the Excel table with the people who have been authorised to access the Commission's premises.</p>
Purpose of the processing	The personal data is collected and processed for the purpose of: - organisation of the access of EUIPO staff/external resources to Sabadell's premises; - organisation of the access of EUIPO staff to European Commission's premises and for and budget control and planning.



Data Subjects	<p>The data subjects in the process of organisation of the access to Sabadell building are all EUIPO staff and external resources authorised to access on a regular basis the EUIPO CPD or warehouses in the Sabadell building.</p> <p>The data subjects in the process of organisation of the access to the premises of the European Commission are all EUIPO internal staff that has submitted a request to Security services for access badge for the Commission premises and has received authorization by the HRD.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Categories of persons whose data EUIPO processes: staff or external resources authorised to regularly enter the Sabadell's premises or the European Commission's premises.</p> <p>The personal data processed for the purpose of organisation of the access of EUIPO staff/external resources to Sabadell's premises is as follows: name, surname, ID number, company/Department, badge expiry date.</p> <p>The personal data processed for the purpose of organisation of the access to the European Commission's buildings is as follows: name, surname, personal number, birth date, nationality, status, contract type, badge type (programmable/non-programmable), signature, card delivery date and card expiry date, access to the parking (yes/no) and cost of the card.</p>
Retention period	<p>The information is stored till the person is authorised to access the concrete premises (till the expiry date of the card in case that renewal has not been requested). In case the person, who has been granted with access to the premises of the Commission/Sabadell, leaves the office before the expiry date of the card, the card is collected and returned to the issuing authority and the personal information is deleted from all records.</p>
Recipients of the data	<p>Security services in IBD and external security provider access the data in order to organise the authorisation of access.</p> <p>HRD access the data of the staff authorised to access the European Commission's premises. Moreover, in order to organise the payment for the badges in the current year and to plan the budget for badges' renewal for next year, HRD regularly consults the Excel table with the people who have been authorized to access the Commission's premises.</p> <p>Security services in the Sabadell building are recipient in the process of organisation of the access of EUIPO staff/external resources to the Sabadell building.</p> <p>Security services in the European Commission are recipient in the process of organization of the access of EUIPO staff to the Commission's buildings.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>Data is transferred to the security services of Sabadell when a person is authorised to access the CPD of EUIPO placed in the Sabadell Building. All necessary security measures are taken to protect the data.</p>
General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) <p>The Security service provider (security auxiliaries) have signed confidentiality declaration.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statements for the procedure of organisation of the access to the EC and to Sabadell's premises: http://sharedox.prod.oami.eu/share/page/repository?file=EC_Privacy%20Statement_EC%20.docx#filter=path%7C%2FOffice_Docs%2FK%20INST%20AFFAIRS%2FK03%20DP%2FK0305%20DP%20Domains%2FDPC-IBD%2F3%20-%20NOTIFICATIONS%2FNotifications%20IBD%2FNotifications%20IBD%2FBadges%20Commission%20and%20Sabadell
EDPS Prior consultation	NO



Reference number	DPR-2018-033
Name of the processing operation	Investigation of H&S accidents/incidents
Last Updated:	22/07/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processor: H&S officer in IBD H&S team in IBD External processor: Health & Safety (H&S) services provider - 'PREVING Consultores S.L.U.'
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	According to the decision Admin-04-30 from 2005, the EUIPO complies with the provisions of Law 31/95 for occupational risk prevention. These provisions state that in case of incidents/accidents that could have/ have resulted in injury/lesion for the worker, the office has the obligation to perform an investigation in order to clear the causes for this incident/accident.
Purpose of the processing	The personal data is processed for the purpose of ensuring the compliance with the applicable legislation (Law 31/95 for occupational risks prevention). Moreover, the personal data is processed in order to ensure that all prevention measures are taken in order to avoid any incidents/accidents, thus ensuring the safety of EUIPO staff.
Data Subjects	EUIPO staff and external resources that have had an accident/incident in the office premises that have or could have resulted in injury/lesion.
Description of categories of persons whose data EUIPO processes and list of data categories	Identification data of the person who has had an incident/accident: name, surname, department, length of the service. Health data of the person who has had an incident/accident: accident qualification, type of lesion/injury, date and time of the accident, form of occurrence (falling, hitting, etc.), accident forecast (minor, major, etc.), affected part of the body, injury description.
Retention period	The time limit for storage is 10 years after the person leaves the office. The applied retention policy for health & safety documents lays down 10 years as period of retention for all documents proving the medical capability of the worker for the tasks to be performed.
Recipients of the data	H&S internal team and external provider Preving for the purpose of conducting the interviews and elaboration of the reports.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) The data on paper is stored in locked cupboards. The external service provider's staff signs a declaration of confidentiality.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement H&S incidents and accidents investigation: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/60bec7d5-909f-4d49-b049-e0e6d0548edc
EDPS Prior consultation	NO



Reference number	DPR-2018-034
Name of the processing operation	Occupational Risk Prevention trainings
Last Updated:	27/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: H&S officer H&S team in IBD External processor: Health & Safety (H&S) services provider - 'PREVING Consultores S.L.U.'
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>According to the decision Admin-04-30 from 2005, the EUIPO complies with the provisions of Law 31/95 for occupational risk prevention. With this respect, the office provides training and informs EUIPO internal staff about the occupational risks in their work environment and the prevention measures that they can take regarding these risks and in situations of emergency. Upon arrival all EUIPO internal staff is obliged to complete an occupational health and safety course at EUIPO Learning portal and receives an induction training from the Responsible for Risk Prevention (HRD sends the list of internal staff to H&S team).</p> <p>Moreover, taking into consideration the observation from the External Audit from April 2017 the office shall raise the awareness on basic H&S principles and rules of the external provider staff that carries out hazardous activities or those with significant likelihood of breaching such rules (currently, catering, security and maintenance and event management external staff).</p> <p>According to the EUIPO's self-protection plan, the office disposes as well of emergency intervention teams (EPIE's, EAE's, JE) that assist EUIPO staff and help people with special needs in case of emergency situation. The emergency intervention teams receive special trainings and are responsible for informing all EUIPO staff upon their arrival for the emergency routes that correspond to their location.</p>
Purpose of the processing	The personal data is processed for the purpose of ensuring the compliance with the applicable legislation (Law 31/95 for occupational risks prevention). Moreover, the personal data is stored in order to ensure that each person working in EUIPO has been informed about the occupational risks in his/her work environment, thus ensuring the safety of EUIPO staff.
Data Subjects	EUIPO internal staff and external resources.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Personal data related to the Internal staff:</p> <ul style="list-style-type: none">- Information receipts: name, surname, personal number and signature;- Certificate H&S: name and surname;- H&S control table: name, surname, department, email;- List of internal staff sent by HRD: Name and surname;- Acknowledgement of receipt of emergency information given by the EPIEs to internal staff: name, surname, signature. <p>Personal data related to the External resources:</p> <ul style="list-style-type: none">- List of externals that have received induction training on risk prevention: name, surname, date, company, signature;- Certificate for risk prevention training: name, surname;- List of externals that have received induction training on accessibility: name, surname, date, company, signature;- Questionnaire on accessibility: name and surname;- Certificate for accessibility training: name, surname.- Acknowledgement of receipt of emergency information given by the EPIEs to external staff: name, surname, signature. <p>Personal data related to the EPIEs network:</p> <ul style="list-style-type: none">- Annual Meeting sheet: name, surname, signature;- EPIE appointments: name, surname, personal number, signature;- EAE appointments: name, surname, personal number, signature, and company if external;- Acknowledgement of receipt of equipment: name, surname, personal number, signature;- General list of EPIE's – EAE's – JE's: name, surname, telephone number (if available);- List of absences/leaves/vacations: name, surname, office location;- Lists of EPIE's – EAE's – JE's who have passed the mandatory trainings: name and surname;<ul style="list-style-type: none">o H&S control list: name and surname;o List of people who have passed the First aid and Fire prevention course given by Academy: name, surname, personal number, telephone number and signature.
Retention period	All documents in Sharedox (according the the Classification plan) and on paper are stored for 5 years after the person leaves the office. The applied retention policy for health & safety documents lays down 5 years as period of retention for all documents except for the document proving the medical capability of the worker for the tasks to be performed, or resignation to the medical examination when possible that will be retained for 10 years in the general case and for 30 years in the case of occupational noise exposure.
Recipients of the data	H&S internal team and the external provider Preving have access for the purpose of organization and follow-up on the trainings.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to [process name] is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p> <p>All personal data stored on paper is locked in filing cupboard.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement Occupational risk prevention trainings:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/247e0f9b-ed50-47db-98a4-98936234dd5f</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-035
Name of the processing operation	Processing personal data of EUIPO's staff members for the promotion/ reclassification exercise including promotion /reclassification /unblocking of top grades
Last Updated:	15/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing data of staff members (officials, temporary and contract staff) within the framework of the annual promotion/ reclassification exercise, as well as the promotion/ reclassification/ unblocking of top grades for officials and temporary agents.</p> <p>According to the SR and CEOS higher grades in AD and AST careers will be accessible only to a limited number of officials and temporary agents occupying a post associated to a high level of responsibility:</p> <ul style="list-style-type: none">- "Head of Unit or equivalent" (manager) or "Adviser or equivalent" (senior expert) for an AD;- "Senior Assistant for an AST. <p>The careers of the jobholders in the following situations are blocked until appointment associated to a higher level of responsibility through an internal selection procedure as follows:</p> <ul style="list-style-type: none">- AST 9 "Assistant in transition" to be promoted to AST 10 "Senior Assistant";- AST 10 "Senior Assistant in transition" unblocked to AST 10 "Senior Assistant";- AD 12 "Administrator" to be promoted to AD 13 "Adviser or equivalent";- AD 13 "Administrator in transition" to be promoted to AD 13 "Adviser or equivalent". <p>A number of promotion/ reclassification/ unblocking possibilities will be decided each year on the basis of a monitoring of the number of promoted staff, the comparison with the references presented in Annex I.B of the SR, the needs of the Office and the budgetary possibilities.</p> <p>The promotion/ reclassification system applicable to EUIPO staff is the result of the examination of the comparative merits of staff members of the same function group, grade and statutory link, eligible for promotion/ reclassification/ unblocking, based in particular on the number of points accumulated, the appraisal reports since the last promotion, the use of languages in the execution of their duties and the level of responsibility exercised by them.</p> <p>The promotion/ reclassification exercise is launched every year by the Human Resources Department (HRD) through a Communication to staff (published on EUIPO's Intranet) once the appraisal exercise is completed. The promotion/ reclassification/ unblocking exercise of top grades is launched through the publication of vacancy notices in accordance with EUIPO's Job and Competency Mapping.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purpose of the processing operation is to conduct the annual promotion/reclassification exercise for officials, temporary and contract staff, as well as the promotion/reclassification/unblocking of top grades for officials and temporary agents in compliance with Article 45 of the Staff Regulations (SR), Articles 54 and 87(3) of the Conditions of Employment of Other Servants (CEOS), and Management Board Decisions MB-16-18 for officials, MB-16-19 for temporary agents and MB-16-20 for contract agents.
Data Subjects	Statutory staff members: officials, temporary agents and contract agents.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The data processed are the following:</p> <ul style="list-style-type: none">- full name, personal number, contract duration, job title, career stream, function group, grade, seniority date in grade, statutory link, job assignments (current and past), working conditions including teleworking if applied, the number of days of leave on personal ground/unpaid leave taken during the promotion exercise reference period;- the written justification provided by EUIPO Directors a) when proposing promotion points at a different level than what is foreseen with regard to the overall performance assessment, b) when proposing to promote a staff member and c) when proposing not to promote a staff member who has reached the threshold of points;- the accumulated capital of points since the last promotion/reclassification, the promotion/reclassification threshold, the number of promotion/reclassification points proposed/awarded in the current exercise including specific merit points, total number of promotion/reclassification points (sum of accumulated points and points awarded in the current exercise), the number of promotion/reclassification in the past promotions/reclassification exercises;- the appraisal reports since the last promotion/or since the recruitment, the use of languages and the level of responsibilities exercised. If an appraisal report has not been finalized as a result of a delay for which the jobholder cannot be held responsible and the jobholder is present during the promotion exercise, any other relevant information;- a list of staff members proposed by the Appointing Authority for promotion/reclassification and, the written justification provided by the Appointing Authority in case of particularly exceptional merits;- the possibilities of promotion/reclassification/unblocking in each function group and grade for each statutory link.
<p>Retention period</p>	<p>All the individual documents, the number of points and the final promotion decision are stored in the personal file (Allegro/Alfresco) in accordance with Article 26 of the Staff Regulations and kept during the same period of retention as for the personal files and kept during the same period of retention as for the personal files .</p> <p>The promotion file with Excel tables contains all background information regarding promotion data for the staff members concerned, for example, information such as minutes taken by the secretariat and signed by the Staff Committee delegation/Joint Promotion and Reclassification Committee, lists and the decision of the Appointing Authority. The promotion file is kept for 10 years.</p> <p>The lists of staff eligible proposed for promotion/reclassification/unblocking and the lists of staff promoted are disclosed in EUIPO's Insite and archived for a period not longer than 5 years.</p> <p>Statistics are drawn up each year in an anonymous form following the promotion exercise.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Data are accessible to:</p> <ul style="list-style-type: none">- the authorized staff of HRD responsible for the appraisals and promotion processes and procedures;- the Deputy Executive Director, the President of the Boards of Appeal, the Director of the Departments and the staff members authorized by them to work on the promotion files (e.g.: assistants/secretariat);- in case of complaint and further judicial procedure, data may be disclosed to the HRD staff responsible for complaints, the Legal Service and/or to the EU Court of Justice.- the Staff Committee;- the Joint Promotion and Reclassification Committee (JPRC); the Joint Committee (JC);- the specific Management and Advisory Committee on promotions/reclassifications/unblocking (MAC);- the Appointing Authority (AA) or the Authority Authorized to Conclude Contracts (AACC) of employment (the Management Board (MB)/ the Executive Director/ the Director of the HRD / the President of the Boards of Appeal (BOA));- the IT technicians, if there is a need of technical assistance with the Human Resources Information System (HRIS);- the Finance Department and PMO (promotion/reclassification decisions, adaptation of salary). <p>Publication of lists in Insite accessible to statutory staff:</p> <ul style="list-style-type: none">- lists of staff eligible for promotion/reclassification;- lists of staff proposed for promotion/reclassification;- lists of staff promoted/reclassified. <p>In particular for the promotion/reclassification/unblocking of top grades:</p> <ul style="list-style-type: none">- list of potential candidates for the published posts;- list of candidates selected and appointed to top grades. <p>These lists could include: the name, surname, career stream/classification of the post occupied, function group, grade and statutory link.</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data are stored in secure IT applications (ShareDox, HR “Allegro” database and “SAP SuccessFactors”) according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in the files.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU. The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. “SAP SuccessFactors” is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on promotion/reclassification exercise including promotion/reclassification/unblocking of top grades: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f98b2f1e-e1cd-48d6-8276-a838ad2c4b6e
EDPS Prior consultation	NO



Reference number	DPR-2018-036
Name of the processing operation	Processing personal data within the framework of Calls for Talent
Last Updated:	01/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Calls for talent are published on Insite throughout the year on a Department need basis and are open to all statutory staff (officials, temporary and contract agents) who have successfully passed the probationary period, as well as to Seconded National Experts.</p> <p>Staff members are invited to express their interest by completing their Talent Profile in the HRD Portal . Candidates can also send their CV and a motivation letter.</p>
Purpose of the processing	<p>The purpose of Calls for talent is to identify internal talents to cover specific Department needs in the form of determined assignments. Data will be processed by representatives of Departments publishing the Calls for talent and representatives of Human Resources Department to review the received expression of interests and select the best talent profiles.</p> <p>The participation in Calls for talent is taken into account for the annual appraisal exercise (objectives are updated and input is provided on jobholder's performance) .</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Data Subjects	Statutory staff (officials, temporary and contract agents)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed:</p> <ul style="list-style-type: none">• staff member full name, personnel number, gender, date/place of birth, nationality, email, telephone, work activity;• staff member's CV, photo (voluntary), education, languages, expertise/talent, skills, working experience, position applied for, motivation letter, type and duration of contract, grade/step, tasks in/outside EUIPO, administrative status, assignment and training in/outside EUIPO.• Data related to the application to Calls for talent (CV/motivation letter /emails).
Retention period	<p>Data related to the application to Calls for talent will be stored electronically for a maximum period of 2 years:</p> <ul style="list-style-type: none">- CV- Motivation letter- emails. <p>However, data related to the general management of skills, expertise, talents which are stored in HR "SAP SuccessFactors in the cloud" will be kept during the duration of the employment activity of the data subject at EUIPO.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The staff of Human Resources Department in charge of Recruitment/ Selection procedures/ Calls for talent, the Management and authorized staff of the EUIPO's Departments concerned.</p> <p>Data stored in HR "Allegro" database may be accessible to external contractors/ subcontractors, namely Adequasys (France). They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting the HR "Allegro" database and integrations with SAP BPC and Business Object systems. Data may also be accessible to Sopra Esteria (Spain) for the maintenance of integrations with Insite, AEOS and SuccessFactors IT systems.</p> <p>This information may be accessible by external contractors/subcontractors, namely SAP, IECISA and EVERIS. They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting "SAP SuccessFactors" and the integrations of SuccessFactors with Remedy and Insite.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to Calls for talent is stored in secure IT applications according to the security standards of EUIPO.</p> <p>The Human Resources database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the framework of Calls for talent:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/5cddb5c7-b62a-4ece-903d-a1f50935d865</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-037
Name of the processing operation	Processing personal data within the framework of Structural Teleworking at EUIPO
Last Updated:	16/12/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service (HRD)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing data of EUIPO's staff members concerning requests for structural teleworking with regard to different criteria such as the possibilities of teleworking, the interests of the service and the individual's motivation.</p> <p>The data subjects are officials, temporary agents and contract agents that have an arrangement of either structural or occasional teleworking.</p> <p>Apart from the data processed by Human Resources Department (HRD), the Infrastructure and Buildings Department (IBD), on behalf of the HRD, establishes a risk assessment, including health and safety risks related to occupational risk prevention. The persons concerned are informed about the prevention measures applicable to their working place.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of the processing personal data is is to process requests of staff members for teleworking in compliance with:</p> <ul style="list-style-type: none">- Decision No MB- 19-28 of the Management Board of 24/12/2019 concerning teleworking at EUIPO;- Decision No ADM 04-10 Rev of 29/03/2012 concerning occasional and regular teleworking agreements signed until 23/12/2019;- Decision No ADM 04-30 of 31/01/2005 concerning the Office's committee on health and safety at work. <p>The risk assessment (including health and safety risks) established by the IBD has the purpose to ensure that teleworker's working place complies with Spanish Law 31/95 on occupational risks prevention.</p>
Data Subjects	<p>The data subjects for structural teleworking are officials, temporary agents and contract agents that have an arrangement of either structural or occasional teleworking.</p> <p>Line managers in the scope of their opinion on granting teleworking.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>For the purpose of the proper execution of the teleworking agreements, the Office will collect and process the following data:</p> <ul style="list-style-type: none">- Director / Line Manager name and professional coordinates;- Name and surname of the teleworker / office location and phone number / personal number / email address;- Home and / or telework location address and telephone / GSM number;- Type of interest in telework;- Current post and suitability for telework (compliance with the selection criteria);- Opinion of the line manager;- Telecommunication provider diagnostic / status of VPN-IP line or alternative;- Special needs except for health related needs;- IP (computer address) / professional/mobile number;- Data on individual production, productivity and performance / conduct in the service / job description, organization of working time, (arrangements at work or at home);- Risk assessment processed by IBD in compliance with Health and Safety rules. The risk assessment includes the name and surname, address, email and telephone of the teleworker. <p>The Office may further combine the above mentioned data with other data for the purpose of the annual appraisal exercise. Such processing operations will be subject to a separate notification to the Data Protection Officer and separate information to the Teleworker.</p>
<p>Retention period</p>	<p>Teleworking agreements and related working documents will be retained for 3 years after the teleworking ceases. Requests of teleworking not granted will be retained for 2 years.</p> <p>As included in the Specific Privacy Statement on teleworking published under the previous Decision (ADM- 04-10 Rev), occasional teleworking agreements signed under that previous Decision will be retained for 3 years after the entry into force of the new Decision on Telework. (MB-19-28).</p> <p>Anonymous statistic reports will be stored for a period of 5 years according to the EUIPO retention policy.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The line managers of the teleworker, their assistants / secretariat / or Human Resources Correspondents (HR), staff of HRD processing teleworking agreements, including the welfare officer and external or internal staff of IBD processing computer and installation connections.</p> <p>Staff of the telecommunication company having a contract with EUIPO might have access to the necessary data for an eventual connection of telephone lines at the teleworker's home.</p> <p>Access to data is given to internal/external staff of DTD (Operations & Infrastructure Service) in charge of the technical coordination with the provider for the installation of telephone connections at the teleworker's home.</p> <p>The Office may disclose appropriate information to authorised Office staff or other authorised persons indicated by the teleworker for the compliance of "access to the place of telework, with prior warning, for the reasons of installation, maintenance of the working equipment provided by the Office and for verification of health and safety requirements of the teleworker's workplace" or any other provision of the Structural Teleworking Agreement.</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" under request and supervision of EUIPO .</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data is stored in secure IT applications (ShareDOX, HR "Allegro" database and "SAP SuccessFactors") according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>The Office will ensure that any eventual contractor, who has access to personal data for the compliance of the Structural Teleworking Agreement , is bound by a contractual clause guaranteeing appropriate security measures and confidentiality.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data within the framework of structural teleworking at EUIPO: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3076b9fd-7abc-493c-be5e-a125014dcd0b
EDPS Prior consultation	NO



Reference number	DPR-2018-038
Name of the processing operation	Processing of personal data within the framework of Working Time Management, Flexitime and Leave
Last Updated:	26/08/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Working Time Management, Flexitime and leave, including part-time work, leave on personal grounds / unpaid leave, special leave / parental leave / family leave / maternity leave / travelling time due to special leave. The processing of data includes the verification of the supporting documents (e.g.: marriage certificate, birth certificate, death and sickness certificates of the relatives, etc.).</p> <p>Flexitime: Data is collected to keep a record of the hours worked by staff in the general context of 40- hour week which gives staff the flexibility to decide, within the interest of the service, when they wish to start/finish work. This flexibility is limited to the hours defined as flexitime.</p> <p>Leave: Data is collected and managed by the Entitlements and Staff Welfare Service of the Human Resources Department (HRD) for the purposes of leave management of the staff members. This data may also be used for further processing in the context of the invalidity procedure.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of this operation is the management of data related to presences and absences in compliance with the Staff Regulations (SR), the Conditions of Employment of Other Servants (CEOS) and the implementing provisions on working hours, part-time work and leave. It includes the management of individual data contained in the HR Information System under working time management/ absences (annual leave/ special leave/ sickness)/ working hours/ requests for flexitime/ part-time/ leave on personal grounds/ unpaid leave/ parental leave/ family leave/ maternity leave/travelling time due to special leave.</p> <p>Data is collected and managed by the Entitlements and Staff Welfare Service of the Human Resources Department (HRD) for the purposes of leave management of the staff members.</p> <p>Data collected for the management of absences/ leave may also be used for further processing in the context of the invalidity procedure, as foreseen in Article 59 (4) of the Staff Regulations.</p>
Data Subjects	<p>Statutory staff members: officials, temporary agents and contract agents.</p> <p>Non-statutory staff: seconded national experts (SNE), trainees and agency staff (interims).</p> <p>Concerning special categories of leave, relatives of EUIPO staff, including spouse, children and relatives in ascending line.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The following data are processed only on need to know basis and by authorized staff:</p> <ul style="list-style-type: none">- Name, personal number, civil status and statutory status of the staff members and SNE;- Name and personal number of trainees and agency staff (interim staff);- Individual request for all types of leave;- Dates of leave/ absence/ sickness;- Name of relatives (spouse/ child/ ascendant.) of the staff members and SNEs mentioned in the supporting documents when necessary, e.g. in case of request of absence linked to family/ parental leave or special leave due to serious/ very serious illness of a relative and spouse in the case of marriage, etc.;- Certificates of marriage, birth, adoption of a child, death of relatives, etc.;- Certificates related to sickness of the staff members and their relatives. These certificates are directly sent by the staff member to the Medical Service. The authorised staff of the HRD that deals with absences is informed of the validation of the certificate by the Medical Service;- In case of leave due to serious/ very serious sickness of relatives (spouse/ child/ ascendant) the medical certificate should include that the staff member was with the sick person on the stated dates.
<p>Retention period</p>	<p>Personal decision:</p> <p>Data related to the personal decision of the AA/ AACC concerning part-time work, leave on personal grounds/unpaid leave, parental/family leave, as well as birth certificates related to maternity leave is kept in the personal file of the person concerned for the same period of time established at the Office as for the personal files. This retention period is necessary to keep track when the total time granted reaches the maximum permitted by the SR and for entitlement rights of the person concerned /or descendants (e.g. in case of transfer of the staff member to other institutions and for pension calculation).</p> <p>Flexitime:</p> <p>Data related to the working hours will be retained during the current calendar year. They will be deleted once the transfer of unused days of annual leave to the following year has been closed, and at the latest by the end of June, unless there is an open procedure for "underperformance or disciplinary issues (conduct in the service)" and proof of not respecting the working hours is needed.</p> <p>Absences (My Absences) and Leave (My Working Conditions):</p> <p>Data will be kept for up to 5 years/or the time necessary for the budgetary discharge for staff who leave the Office (e.g.: payment of annual leave not taken). In case of invalidity procedures, data is retained for the time necessary for further processing as foreseen in Article 59(4) of the SR.</p> <p>Special leave:</p> <p>Supporting documents are retained for up to 2 years (e.g.: removal, marriage, sickness of relatives).</p> <p>In case of death of a family member of the person concerned, data is retained for the whole career (e.g.: in case of transfer to other institutions).</p> <p>Maternity leave data is retained for the same period as the personal file in case that the descendants and/or the administration might need this information for entitlements rights of the person concerned/or descendants for pension calculation.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Access to:</p> <ul style="list-style-type: none">- Officials / temporary agents/ contract agents / SNEs for register/consultation of working hours, request of flexi leave or other leave, cancellation and rectification;- Agency staff and trainees to register working hours. <p>Data can also be disclosed to:</p> <ul style="list-style-type: none">- The hierarchy and the persons appointed by the line managers of the person concerned (for consultation and validation);- The authorized staff of HRD managing absences and entitlements for the verification of working hours, flexitime and leave in compliance with the implementing rules (consultation of absences, verification of supporting documents and register of approval in the database);- The authorized staff of the Office's Medical Service receiving the certificates related to sickness for validation;- The Appointing Authority (AA) and the Authority Authorized to Conclude Contracts of employment (AACC);- The staff of PMO managing the remuneration of the Office's staff in case of part-time work, parental/ family leave/ unpaid leave or any other working condition. The note to PMO includes the name of the person concerned, personal number, period of leave and the name of the relatives concerned (child, spouse, parents, etc.);- A limited number of staff of the Finance Department (Verification Office) for the verification of the instructions sent to PMO having an impact on the remuneration of the staff member concerned;- Employment agency (interims) in order to comply with Spanish national law governing hiring of agency staff (temporary leave replacement) . Processing of data by the Interim agency is subject to the national legislation (Spain) implementing the General Data Protection Regulation;- External contacts in case of absence of the staff members due to leave, if he/she discloses the information by setting their out of office auto reply in their email account.- For organizational purposes EUIPO's staff members have access to the planning of absences of their colleagues working in the same Department/ Service. This information is strictly limited to the name/ surname/ dates of requested absences not yet approved /and dates of absences approved. There is no access to the reasons of absence;- The staff of the Information Centre (Customer Services Department) has also access to data with regard to staff member's availability in order to attend incoming calls, and generally improve EUIPO users' satisfaction. The access to data is limited to the absence's planning of HR database, which has been integrated in the CRM system, without any information referring to the reason of absences. <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>The Human Resources database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Cloud systems “SAP SuccessFactors have 24/7 security monitoring and alerting, security incident and threat response procedures, and automated security measures to prevent unauthorised access.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. “SAP SuccessFactors” is also certified in ISO 27001.</p> <p>Supporting documents, except medical files, are kept in locked cupboards by the Entitlements and Staff Welfare Service (HRD). The electronic files are stored according to the Office’s IT security measures.</p> <p>Information stored in Sharedox is protected by the following security measures:</p> <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access will be allowed.• Authentication and authorization to view and access information based on roles.• Servers are physically protected at the Data Protection Centre.• Networking security configured to prevent external threats from accessing the servers. <p>A declaration of confidentiality is signed by the persons having access to the HR database. All authorized staff members of HRD dealing with health related operations (e.g.: sickness leave) are requested to sign a confidential declaration.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on Working Time Management Flexitime and Leave: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/b7b7c223-9198-43c3-b2cb-a356b76b0b5b</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-039
Name of the processing operation	Individual Medical Files
Last Updated:	27/09/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	HRD / IDCQ Hospitales y Sanidad, S.L.U.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data included in the individual medical files.</p> <p>All documents concerning the health status of statutory staff members shall be kept in an individual file which contains data related to the medical examination before taking up duties at EUIPO, the annual medical examinations or other medical examinations required by the Medical Service.</p> <p>The data subjects are candidates who have been offered an employment or individuals who are employed in EUIPO as officials, temporary agents or contract agents .</p> <p>The individual medical file can also contain health data of relatives of the staff member concerned, whenever relevant to justify the sickness or handicap of a member of his/her family.</p> <p>EUIPO is assisted by an external Medical Service which processes the necessary personal data in order to establish a medical file for each new recruited EUIPO's staff member and to maintain it updated until the end of service of the person concerned.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of processing individual medical data is to survey and promote staff health according to the obligations of the Staff Regulations (SR) and Conditions of Employment for Other Servants (CEOS). Health data will be kept in an individual medical file in compliance with:</p> <ul style="list-style-type: none">- Articles 10-16 and Article 25.1.(h) of Regulation (EU) 2018/1725;- Article 26 (a) of the SR and Articles 11 and 81 of the CEOS;- Decision N° ADM 18-32, dated 06/08/2018, on the definition of the responsibilities of the EUIPO's Medical Service;- The Conclusion of the Heads of Administration N°221/04, dated 19/02/2004 on the access of officials to their medical files .- Real Decreto 22/10/1995 of 28 December - Spanish epidemiological surveillance network;- Orden SCO/3270/2006 of 13 October - food transmission of salmonellosis;- Orden SSi/445/2015 of 9 Mars modifying Annexes I,II and III of the Real Decreto 2210/1995.
Data Subjects	Statutory staff: officials, temporary agents and contract agents. The Medical Service can also keep health data of Seconded national experts (SNE's) and trainees, in particular concerning absences due to sickness.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The data processed by the authorised persons of the Medical Service are the following:</p> <p>Identification Data: Surname, forename, personal number, gender, marital status, data and place of birth, nationality, postal address, email address, telephone numbers, position applied (nature of work), administrative status (type of contract) and risk assessment questionnaire.</p> <p>Medical Data: Reports of medical examinations, results of laboratory tests, medical certificates, specific medical check-ups, medical history, family history and health documents related to sick leaves, periods of absences and other medical records.</p> <p>Data related to staff member's relatives: Identity of children, spouse or other relatives and their sickness certificates /or health reports, sent by the staff member to the Medical Service in order to support his/her request for special leave, family leave or special family allowances (e.g. in case of child's handicap).</p> <p>Data processed by the Medical Service in case of inquiry related to food poisoning: Surname, forename, contact data (telephone and office numbers), birth data, symptomatology and dates, doctor's name/ telephone in case of medical consultation/or hospitalization, personal data (name/telephone nr.) of other persons presenting the same symptomatology.</p>
<p>Retention period</p>	<p>The health data collected are kept in safe custody in the individual medical record up to 30 years, from the date of end of service of the person concerned.</p> <p>Data on candidates not ultimately recruited shall be kept for a period of one year during which the candidates can ask for the return of medical data provided from the Medical Service of the EUIPO. Beyond this period, the data is destroyed. In the event of a formal appeal, all data held at the time of appeal will be retained until completion of the appeal process.</p> <p>Non-medical related documents: emails, reminders, planning of medical appointments etc. are not kept in the medical records and are automatically deleted once it has served its informative purpose at every medical review.</p> <p>Due to legal obligations, the Medical external provider keeps the data according to the Spanish Law (retention period: Article 17(1) and (2) of Spanish Law 41/2002 .</p>



Recipients of the data	<p>Medical Service: only the doctors, the nurse and the assistant have access to the medical file.</p> <p>In accordance with Article 26(a) of the SR and Articles 11 and 81 of the CEOS, staff members shall have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the Appointing Authority (AA) and the Authority Authorised to Conclude Contracts (AACC).</p> <p>In the case that data subjects have symptoms of food poisoning, the Medical Service will carry out an inquiry with the persons concerned by the intoxication and will keep the related health data in the medical file. The Medical Service will send to the Infrastructures and Buildings Department (IBD) an anonymous report only with the conclusions and the symptomatology.</p> <p>IBD will analyse the anonymous report in order to take a decision whether the protocol food poisoning should be activated or not.</p> <p>In case of having to inform the Spanish Public Health Service, the Medical Service is obliged to share certain personal data (names, contact information, symptomatology) with the Public Health Service.</p> <p>Transfers may take place, for example, if health data needs to be sent to external doctors appointed by the data subject or to the Medical Service of other institution in case of transfer of the person concerned. Medical data are transferred only to health professionals after the consent of the data subject concerned.</p> <p>IT technicians (internal or external staff) may have access to the Medical database "Preven" for maintenance and software renewal. They do not have access to the medical data.</p> <p>In addition, certain administrative details may be disclosed on a temporary basis to the Director of Human Resources Department, the Head of Service of Entitlements and Staff Welfare Service, the Social Assistant, the Appointing Authority (AA), the Authority Authorised to Conclude Contracts AACC), the Legal Service and the Court of Justice in case of complaints. Upon request, administrative details may also be disclosed to the Internal Audit, the Court of Auditors.</p> <p>The data disclosure or transfer is done in compliance the relevant current legislation and established case law. No personal data is transmitted to parties which are outside the recipients and the legal framework mentioned.</p> <p>Authorised staff dealing with administrative documents in connection with health data is requested to sign a declaration of confidentiality equivalent to a health professional.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	External doctors and Medical Service of other institutions. Medical data are transferred to health professionals (doctor, nurse, medical assistant) and with the consent of the data subject



General Description of security measures	<p>Medical files are kept on paper by the Medical Service in a separate file for each staff member and stored in secured archives that are only accessible to the doctors, nurse and assistant of the Medical Service.</p> <p>Electronic medical data stored in "Preven database" are password protected under sign-on system and automatically connected to the user ID and general password "Access" database is password protected under sign-on system and automatically connected to the user ID and general password.</p> <p>For data processing related to annual medical check-ups EUIPO service-provider/contractor ('IDCQ Hospitales y Sanidad S.L.U.') use their own systems.</p> <p>EUIPO contractor/service provider ('IDCQ Hospitales y Sanidad S.L.U.') subcontracted the services related to pre-recruitment medical visits to 'Mapfre' which use their own systems for data processing.</p> <p>The access to medical files is granted only to the Medical Service.</p> <p>Medical files are kept according to the security measures of EUIPO Information Systems under confidential documents.</p> <p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorisation process. Mechanisms of access tracking and monitoring of use of systems are established. Authorised users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on Individual Medical Files in EUIPO : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/4112b7e9-4cbf-4a4d-94e0-8b889c981eea
EDPS Prior consultation	NO



Reference number	DPR-2018-040
Name of the processing operation	Processing personal data within the framework of the management and consultation of the personal file
Last Updated:	16/10/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data to establish the personal file of EUIPO's staff members (officials, temporary agents and contract agents).</p> <p>Documents uploaded to the personal file shall be registered, numbered and filed in serial order.</p> <p>The personal file shall not contain any reference to the staff member's political, trade union, philosophical or religious activities and views, or to his/her racial or ethnic origin or sexual orientation.</p> <p>A staff member shall have the right, even after leaving the service, to acquaint himself/herself with all documents in his/her personal file and to take copies of them.</p> <p>The personal file shall be confidential and may be consulted only on a secure electronic medium (Open Text Tool - Personal File Repository).</p> <p>As from 2020, the paper versions of the personal file will be dismissed: the members of staff will be notified individually and will be given three months to recover the original documents. Until their phasing out, the personal file in paper may also be consulted in the offices of the Human Resources Department (HRD). When there is a complaint and upon request, the personal file can be forwarded to the EU Court of Justice.</p> <p>HRD establishes also a personal file for Seconded National Experts (SNE's) and Special Advisers working for the Office.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>In compliance with Article 26 of the Staff Regulations (SR) and Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS) of European Union each statutory staff member shall have one only personal file.</p> <p>HRD processes the data in order to establish a personal file for each new recruited EUIPO's staff member and to maintain it updated until the end of service of the data subject. The personal file contains:</p> <ul style="list-style-type: none">- all documents concerning the administrative status and reports relating to the staff member's ability, efficiency and conduct, as well as any comments done by the data subject member on such documents;- administrative acts and documents known to the staff member and which are necessary for the application of the SR/CEOS.



Data Subjects	<p>Statutory staff: (officials, temporary agents and contract agents). Seconded National Experts (SNE's) and special Advisers. Whenever relevant for the processing of individual rights, data concerning relatives (spouse, children, dependent persons, etc.) of the data subject. Line manager's (opinion) / Previous employer's (opinion) / Persons to contact in case of accident.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following documents containing personal data are processed and uploaded to the personal file only on a need to know basis by authorized staff of HRD:</p> <ul style="list-style-type: none">- Identity card/ passport/ NIE/ nationality/ birth certificate/ personal number/ telephone / address/ recruitment place/ photo (if voluntary uploaded to the CV by the staff member),/ education diplomas/ professional experience and expertise/ certificate of good conduct /police record/ criminal record;- Opinions from previous employers concerning the new recruited staff member (reference check before recruitment);- Job offers / contracts / trainings;- Documents related to the staff member's reports concerning his/her ability, efficiency and conduct, as well as the line manager's opinion and any comments done by the staff member on such documents;- Decisions on appointments/ working conditions/ assignments (Department/Service) / nomination / promotion, / retirement/ invalidity / administrative enquiries and disciplinary measures;- Documents necessary to establish/ and/ or update the statutory entitlements (staff member's marriage or /divorce/ or legal separation certificate) / birth and school certificates of the dependent children / the staff member's annual confidential declaration including data about the spouse's annual income and any conflict of interests;- Documents related to staff member's retirement to be sent to the Commission for payment of retirement/ invalidity or unemployment allowances;- Full name and contact details of the persons to contact in case of accident (telephone number and/or address);- Documents of any person treated as if he/she were a dependent child of the staff member by special decision of the Appointing Authority (A.I.P.N.) or the Authority Authorized to Conclude Contracts (AACC). It includes full name, birth date, address, civil status, annual income and fiscal declaration of the dependent person, as well as of any person having also legal obligations of maintenance (e.g. spouse/ all children, etc.). These data are requested only on a need to know basis in order to determine if the staff member concerned fulfills or not the conditions to receive family allowances for the dependent person (compliance with national law applicable in each Member State / Article 2 (4) of Annex VII of SR and Commission Decision COM N°50/2004 applied by analogy to EUIPO);- Documents justifying the installation and / or reinstallation of the staff member, the removal, as well as the origin place;- Data related to the bank account numbers and the notes sent to PMO concerning the payment of remuneration;- Certificates of work requested to HRD by the staff member concerned;- Any other relevant data supplied by the staff member and necessary to manage his/her file. <p>The personal file of "Seconded National Experts (SNE's)" contains the following personal data:</p> <ul style="list-style-type: none">- Full name, personal number, telephone, address, identity card/ passport/ NIE/ nationality/ correspondence with the national administration concerning the secondment/ CV / education diplomas/ professional experience certificates;- SNE's annual reports relating to his/her ability, efficiency and conduct, as well as any comments done by them on such documents;- The bank account number and the notes sent to the Finance Department for the monthly payments of allowances;- The sickness insurance justification. <p>The personal file of "Special Advisers" contains the following personal data:</p> <ul style="list-style-type: none">- Full name, telephone, address, Identity card / NIE / passport/ nationality/ Notification to the budgetary authority specifying the remuneration contemplated;- The contract and corresponding exchange of letters;- The bank account number and the notes sent to Finance Department for the payment of remuneration.



Retention period	<p>The staff member personal file is kept during 8 years after the extinction of all rights of the person concerned and of any dependents, and at least 120 years after the birth data of the person concerned.</p> <p>Documents related to disciplinary measures are submitted to special conditions .</p> <p>For data that can be destroyed in a shorter period of time, the EUIPO's retention period and schedule for files will be applied.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Each staff member can consult his/her own personal file.</p> <p>The consultation of the personal file can be done on a secure electronic medium (Open text Tool - Personal File Repository). Until their phasing out, the personal file in paper may also be consulted in offices of HRD and in the presence of authorized staff of HRD (Entitlements and Staff Welfare Service).</p> <p>The persons who request to consult a personal file shall complete a "consultation form" which includes:</p> <ul style="list-style-type: none">- Name and personal number of the person to whom the consulted personal file belongs;- Name and quality (function) of the person who requests the consultation of the personal file of another person;- Date of consultation / return of the personal file and signature of the person who has requested the consultation;- Reference of which part of the personal file has been consulted. <p>On a need to know basis, access to part / or whole personal file can be given to:</p> <ul style="list-style-type: none">- Authorized staff of HRD working in HR processes related to the data subjects;- A limited number of authorized staff working on appraisals/ promotions / job profiles (HRD - Career and Development);- HRD Director / HRD Heads of Service ;- Legal Service;- HRD Social Assistant. <p>Upon request and on a need to know basis, access to a part /or whole personal file can also be given to:</p> <ul style="list-style-type: none">- Financial Officer (FD) and Internal Audit Service and the EU Court of Auditors for audit purposes;- Line managers /reporting officers can consult the appraisals of their actual staff or/ of an eventual future staff member. They can also consult part of the file related to education, professional experience, languages, technical skills and expertise, competencies and trainings;- Eventually the future line manager can consult part of the personal file concerning disciplinary measures (if the case);- Legal Service and Court of Justice in case of complaints / OLAF within the framework of their enquiries;- The AIPN and the AACC;- The Executive Director / the Deputy Executive Director and authorized staff of the Cabinet;- The personal file can also be sent to other institutions (in case of staff member's transfer). <p>The line manager's assistants in charge of resources issues may also be authorized to access the same personal data as their line managers.</p> <p>Access to the electronic personal file may be allowed on a temporary and restricted basis to DTD (IT technicians) for customization, development, updating, technical tests, repair, suport and improvement of the database. (Open Text Tool - Personal File Repository).</p> <p>All consultation / access to part or whole personal file is done only on a need to know basis and by authorized persons.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	
General Description of security measures	<p>The electronic personal file is stored inside "Open Text Tool" (Personal File Repository) kept in EUIPO Servers and accessible through HR database "SAP SuccessFactors".</p> <p>Personal files are kept according to the security measures of EUIPO Information Systems under confidential documents.</p> <p>HR database" has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HR and other departments (staff member, line manager, reporting officer or IT technician).</p> <p>Personal files on paper are kept in secured cupboards by a limited number of authorized staff of HRD. Paper files archived in ARCADE are kept as confidential in conformity with EUIPO security measures applied for the storage of confidential documents.</p> <p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorization process. Mechanisms of access tracking and monitoring of use of systems are established. Authorized users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers.</p> <p>The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>Until their phasing out the personal file on paper is stored in secured cupboards of HRD by a limited number of authorized staff of HRD for the duration of the staff member's employment, plus 5 years. After this period of time, the personal file is archived in ARCADE according to EUIPO rules for the storage of confidential documents. As from 2020, when the members of staff will recover the original documents, HRD will only keep the electronic personal file stored inside "Open Text Tool" (Personal File Repository).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on Processing of personal data on the management and consultation of Staff member's personal files:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/709665aa-02ab-4b89-8d59-4af326255319</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-041
Name of the processing operation	EUIPO Car park management
Last Updated:	15/05/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processor: Head of Common services (CS), IBD Security services in CS, IBD External processor: External provider of security services Securitas and its subcontractor Nsecure.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The management of EUIPO Car Park includes processing of personal data of the EUIPO internal staff or external resources who have been authorised to use a parking place. The request for authorisation is done in My service Desk. Security services register the information in MS Access. Part of the information related to the management of the parking is as well registered automatically in the access management system AEOS when the vehicle passes through the parking barrier. Additionally security services register the information related to security breaches in the Car parking as described in the QSD-0116 Manual EUIPO Car park rules.
Purpose of the processing	The purposes of the processing operation are: <ul style="list-style-type: none">• to avoid that non-authorized vehicles enter the Office's car parks;• to ensure that the Car Park Rules are respected and that the breaches of the Car Park Rules have been addressed with the corresponding measures thus minimising the possibility for the breach to reoccur (removal of the vehicle or withdrawal of the authorisation for the use of the parking in case of serious violations of these car park rules, or reckless driving, speeding).
Data Subjects	All users of EUIPO car park
Description of categories of persons whose data EUIPO processes and list of data categories	The persons whose data is processed are the users of EUIPO Car Park. The personal data that is being processed is as follows: <ul style="list-style-type: none">• For the purpose of issuing the car badges: personnel number, name and surname, car trademark, model and colour, plate number, department and administrative status of the staff member and type of assigned parking place.• For management of accesses: personnel number, name and surname, car trademark, model and number plate, access-related information (point of entry, date and hour).• In order to manage breaches of EUIPO Car Park Rules: personnel number; name and surname of the rule perpetrator; department; trademark and model of the car; plate number; place and category of breach; picture/video recording of the breach and/or the perpetrator. Only the video recordings and pictures taken by the Security services can be used as evidence for a breach of the car park rules. Video recordings and pictures taken by third parties or the Video surveillance system cannot be used as evidence material for the investigation of a breach of the Car park rules.



Retention period	Personal data related to access (point, date and hour of access) are deleted after three months from the date of the access. All the remaining data in AEOS and MS access- personnel number, name and surname, car trademark, model and number plate, department, administrative status of the staff member, etc. are stored for the maximum of 3 months after the person has finished his/her contract with the Office. Personal data related to infringement of the car park rules in the table of breaches in Sharedox are kept for 12 months after the infringement date except for data related to severe and unacceptable infringements, which will be retained till the person who has committed the infringement works in the Office.
Recipients of the data	<ul style="list-style-type: none">• EUIPO Security Service team; Head of Common Services and IBD Director for control purposes;• External security company Securitas in charge of registering all requests for parking authorisations in the Access data base and to print the badge that allows them to access the car park;• Security guards: to manage daily control;• Nsecure computer experts responsible for the maintenance of AEOS and DTD production technicians responsible for the maintenance of Access data base;
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	All personal data related to this procedure is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/12f432a9-dea1-4724-9de3-a3fda5ee58a8
EDPS Prior consultation	NO



Reference number	DPR-2018-042
Name of the processing operation	Processing of personal data within the framework of the Certification Procedure
Last Updated:	08/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The certification procedure enables officials of the function group Assistant (AST), grade 5 or higher, to be appointed to posts of function group Administrator (AD), provided that they :</p> <ul style="list-style-type: none">- Have been selected to take part in a compulsory training programme;- Have successfully completed this training programme;- Have been successfully recruited on an AD post within the Office through the internal mobility procedure. <p>A call for applications with the number of officials authorized to take part in the training programme is published in EUIPO's Insite, as well as the working method used for the selection of candidates and related information.</p>
Purpose of the processing	<p>The certification procedure is based on Article 45a of the Staff Regulations (SR) and replaces the internal competition. The Decision ADM-06-15 (amended by Decision ADM-11-06) establishes the provisions concerning the certification procedure at EUIPO.</p> <p>The selection of candidates is done on the basis of the annual reports referred to in Article 43 of the Staff Regulations (SR) and their level of education and training and taking account of the needs of the services.</p> <p>is to enable officials of the function group Assistant (AST), grade 5 or higher, to be appointed to posts of function group Administrator (AD), provided that they :</p> <ol style="list-style-type: none">1. Have been selected to take part in a compulsory training programme;2. Have successfully completed this training programme;3. Have been successfully recruited on an AD post within the Office through the internal mobility procedure. <p>The certification procedure is based on Article 45a of the Staff Regulations (SR) and replaces the internal competition. The Decision ADM-06-15 (amended by Decision ADM-11-06) establishes the provisions concerning the certification procedure at EUIPO.</p> <p>A call for applications with the number of officials authorized to take part in the training programme is published on Insite, as well as the working method used for the selection of candidates and related information.</p> <p>The selection of candidates is done on the basis of the annual reports referred to in Article 43 of the Staff Regulations (SR) and their level of education and training and taking account of the needs of the services.</p> <p>The processing of personal data is necessary to support the Appointing Authority when taking decisions to adopt the list of AST officials who are entitled to take part in the aforesaid training programme.</p> <p>The training programme and tests are organized by EPSO.</p>
Data Subjects	Statutory staff members: officials group AST, grade 5 or higher.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed:</p> <ul style="list-style-type: none">- Staff member full name, personnel number, email, telephone;- Department/Service, function group, grade, seniority in grade;- Languages competencies (in particular candidate's capacity to work in English or in French), language chosen for the tests;- Priority area for the certification training;- Preferred city for the training (Brussels or Luxembourg);- Level of education (diplomas), trainings attended throughout the last past 5 years, level and relationship with the priority area chosen for the certification training;- Professional experience within the EUIPO as official or temporary staff member (acquired in one or several posts that have implied carrying out activities/ tasks/ or responsibilities in the priority area for which the staff member is applying);- Professional experience as described before, but outside the EUIPO;- Any other professional experience acquired in professional areas, different from the ones corresponding to the priority area chosen for the training;- Annexes joined by the candidate to his/her application form, such as justification of academic education/ training/ professional experience/ language level and any other relevant documents;- Data included in the three last appraisal reports of candidates referred to in Article 43 of SR, in particular the overall assessment awarded, the comments of the reporting officer on the performance, competencies and conduct in the service, as well as the justification concerning the professional potential of the candidate;- The recommendation of the Management Advisory Committee to the Appointing Authority for decision taking. <p>Data published in EUIPO's Insite and accessible to all statutory staff:</p> <ul style="list-style-type: none">- List of admissible candidates (full name, function group/department);- Draft list of officials authorized to take part in the training programme (full name);- Final list of officials authorized to take part in the training programme (full name);- List of officials who have successfully completed the training programme (full name).
Retention period	<p>All personal data provided by candidates in the context of this procedure will be retained for 7 years.</p> <p>Publications in EUIPO's Insite of the lists of candidates/participants/successful officials : 1 year (until the publication of the next Certification programme).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p> <p>In case of complaint, all documents are kept until a final decision on it has been taken.</p>
Recipients of the data	<p>The staff of Human Resources Department in charge of Recruitment/Selection/ Certification procedures/ the Management and authorized staff of the EUIPO's Departments.</p> <p>The Management Advisory Committee and the Appointing Authority (A.I.P.N.).</p> <p>The Joint Committee, after the publication of the draft list of successful candidates for its opinion and in case of appeals, and for the follow-up on the results of the procedure.</p> <p>Staff of EPSO working with the certification procedure. (they receive the list of candidates selected by EUIPO's A.I.P.N. to participate in the training programme and tests) .</p> <p>EUIPO's statutory staff has access to the lists published in EUIPO's Insite concerning the Certification programme.</p> <p>EUIPO's contractors and subcontractors may have access to data for maintenance and development of applications supporting the HR "Allegro" database and "SAP SuccessFactors" under request and supervision of EUIPO.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Paper documents are kept in secured cupboards by authorized staff of HRD. Electronic data are stored in Sharedox / HR "Allegro" database and its modules (stored in MySQL database).</p> <p>HRD is working on the new HR database "SAP SuccessFactors" in the cloud. Data will be transferred from HR portal modules (HR database Allegro) to the new HR database "SAP SuccessFactors". For "SAP SuccessFactors" data are stored in the cloud in servers in SAP Germany and SAP Holland data centers.</p> <p>All personal data related to the Certification procedure is stored in secure IT applications according to the security standards of EUIPO.</p> <p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the framework of the Certification Procedure:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/bd8b1924-27ff-4323-843e-233d80339445</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-043
Name of the processing operation	Remunerations – (payments / recovery of overpayments / retentions)
Last Updated:	02/04/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Service – Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of data concerning the payment of remunerations / recoveries/ and retentions of salary for EUIPO's statutory staff members.</p> <p>The processing of data includes operations related to payments of pensions to third persons and retentions of remuneration due to a legal obligation related to a judicial decision or an administrative body decision.</p> <p>HRD also processes the necessary personal data for the payment of pension, invalidity and unemployment allowance by PMO.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>Data are processed in compliance with the rules of the Staff Regulations (SR) and the Conditions of Employment of Other Servants (CEOS).</p> <p>The purpose of the processing operation is the exchange of data with the Office for Administration and Payment of Individual Entitlements (PMO) and the Finance Department (FD) for the monthly payment of remunerations and/or recovery of overpayments for EUIPO statutory staff.</p> <p>Monthly payment of remuneration, recovery of overpayments / /retentions of remuneration, including those related to a judicial decision or an administrative body decision.</p>
Data Subjects	EUIPO Statutory Staff (officials/temporary agents and contract agents)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data necessary for the payment of remunerations, pension, invalidity, and unemployment.</p> <p>Name, surname, personal number, function group, grade, step, bank account number, NUP, birth date, gender, nationality, country of residence, marriage status, gender and birth date of spouse, children, assimilated persons and other third persons, contractual relationship, amounts to be paid and different concepts of payment (ex: salary %, % of activity, allowances, retentions for pension, sickness, accident, unemployment, insurances, transfer of part of the remuneration. etc.).</p> <p>Data related to "saisies-cessions" retentions, pension payment to third persons, and /or any other payment and/or retention due to a legal obligation imposed by a court or administrative body decision.</p> <p>Data related to recovery of overpayments including information about the personal/financial situation of the staff member concerned. These data shall be collected only by the EUIPO's social assistant and is necessary in order to determine and justify both the monthly amount and the duration of the retention on the salary of the person concerned.</p> <p>The social assistant also needs to collect these data when a staff member requests an advance of salary outside taking up duties.</p>



Retention period	<p>Working documents related to monthly remuneration - payments or recovery of overpayments: according to EUIPO retention policy.</p> <p>Any data/document important for the staff member's career, especially for determination of pension rights at the end of the career, is stored in the personal file and kept during 8 years after the extinction of all rights of the person concerned and of any dependents, and at least 120 years after the birth data of the person concerned.</p> <p>Electronic pay slips are stored inside OpenText tool (personal file repository) for the same period as the personal file.</p> <p>Data /Files (hardcopy and electronic) concerning "saisies-cessions" retentions / and payments of pensions concerning legal obligations are kept during a period of 7 years after the last payment is done (termination of the procedure) and then destroyed (time necessary for budgetary discharge).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>A limited number of authorised staff of the Entitlements and Staff Welfare Service (HRD), including the social assistant. The Director of HRD, the Head of Service of Entitlements and Staff Welfare Service. Authorized IT administrators.</p> <p>The Appointing Authority (AA) and the Authority Authorised to Conclude Contracts of employment (AACC), on a need to know basis for taking decisions. The authorised staff of FD and of PMO in charge of remunerations. In case of retentions of remuneration related to a court/administrative body decision, PMO will receive only the requested necessary data to work in the file.</p> <p>In addition, some personal data may be disclosed, under request, where appropriate, in compliance with the relevant current legislation and established case law, and on a temporary basis to the court. In case of retentions of remuneration related to a decision of justice, the court will receive the requested necessary data to work in the file.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>Files related to remunerations are kept according to the security measures of the EUIPO Information Systems under confidential documents. The access to these files is done on a need to know basis and is limited only to authorized staff working in remuneration files.</p> <p>HR database is password protected under sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the Data Processing Centre. Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU. The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. SAP SuccessFactors" is also certified in ISO 27001.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on Remunerations (Payments/ Recovery of overpayments / Retentions) published in Insite /HRD/Data protection: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/a8e71e7b-7e58-45af-8b37-8497409f118e</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-044
Name of the processing operation	IBD training map
Last Updated:	07/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: IBD management IBD management and team leaders process the data for control purposes. IBD secretariat and DMO process the data for the purpose of maintenance of the data base and organization of the trainings.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The training maps of IBD teams were established as part of the IBD team objectives in 2015.</p> <p>The training map of Facility management and the central teams services represents a registry of the trainings to which the teams' staff has subscribed and their training needs.</p> <p>The training map of Common services service (CSS) has a broader function and presents a detailed overview of the learning needs of CSS staff. The plan is based on a gap analysis- comparison between the available and required skills and competencies of the job holder. The analysis serves to the HoS of CSS as human resources management tool, defining individual general and technical learning needs as required by the job profile. The scales indicating the level of skills are aligned with the Job & Competency Mapping of the Office. The analysis of the competences and skills is done by the CSS team leaders on an annual basis.</p> <p>The training maps of all teams are used to develop learning and training plan for IBD staff and serves as a support for the HoS in terms of performance management and evaluations.</p>
Purpose of the processing	<p>The purposes of the processing operation are to:</p> <ul style="list-style-type: none">• provide information regarding the individual learning needs of IBD staff;• ensure the elaboration of structured and need-based department/service learning plan;• ensure and be able to demonstrate the compliance with the applicable regulation regarding periodical appraisals of statutory staff: the reporting officer shall, jointly with the jobholder identify the jobholder's training needs and discuss with the jobholder the impact of training on his/her efficiency during the period in question, his/her future needs in terms of training, and possible further developments in his/her career;• foster staff engagement and motivation in line with the EUIPO Strategic plan 2020, LoA 1 Build a dynamic, knowledgeable and collaborative organisation. <p>The training maps of both services in IBD are used as well to provide sufficient information for the evaluation of the individual objective: Foster staff engagement and take responsibility for own professional growth and the Individual key performance indicator: Identify and propose at least one learning need for each staff member, part of the annual appraisal.</p>
Data Subjects	IBD internal staff



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data that is being processed in the CSS's Training map is as follows:</p> <ul style="list-style-type: none">• Name and surname;• Required level of skills/competencies according to the Job & Competency Mapping of the Office and the individual job description;• Current level of skills/competencies;• Gap analysis of skills/competencies;• Need-based department/service learning plan and its follow up. <p>The personal data that is processed in the training maps of FM teams and the central teams is as follows:</p> <ul style="list-style-type: none">• Name and surname;• Trainings subscriptions (per competency);• Trainings requested to Academy;• Training needs
Retention period	<p>The data in the training map of FM teams and the central teams is stored for the period of 5 years.</p> <p>The data in the training map of CSS is stored for the period of 1 year from the day the person leaves CSS.</p>
Recipients of the data	<p>IBD management and team leaders have access to the data for control purposes. IBD secretariat and DMO have access to the data for the purpose of maintenance of the data base and organization of the trainings.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	<p>NO</p>
Are there any transfers of personal data to third countries or international organisations?	<p>NO</p>
General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement Training map: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/aeda1499-b736-4ad9-ba04-145d6e98a1df</p>
EDPS Prior consultation	<p>NO</p>



Reference number	DPR-2018-045
Name of the processing operation	Monitoring of CSS annual objectives
Last Updated:	16/12/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Head of Common services (CSS) in IBD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The HoS of CSS is closely monitoring the completion of the CSS team objectives through the use of several data bases that contain personal data. These data bases provide relevant information on the progress of the team and individual objectives and serve as performance management and assessment tool.</p> <p>The excel table CSS objectives 20XX, provides a break-down of the annual objectives of the CSS team into individual KPIs, thereby allowing the HoS, team leaders and staff members to keep track of their objectives. On the basis of the general information provided in this table, two types of progress reports are elaborated:</p> <p>Individual progress reports through which is monitored the progress on the individual objectives of each CSS staff member, not only at the mid-term and appraisal interviews, but during the whole year, on a quarterly basis.</p> <p>Progress report of Common Services objectives through which is monitored on a quarterly basis the progress on CSS annual objectives in order to ensure that all objectives are successfully met till the end of the year.</p>
Purpose of the processing	<p>The purpose of the processing operation is to ensure and be able to demonstrate the compliance with the applicable regulation regarding periodical appraisals of statutory staff:</p> <p>„the reporting officer shall, jointly with the jobholder, assess the jobholder's performance during the reporting period and consider the latter's efficiency, the ability he has demonstrated and his conduct in the service during the reporting period“.</p> <p>Another purpose of the processing operation is to ensure and justify:</p> <ul style="list-style-type: none">• the completion of CSS annual objectives (based on the completion of the CSS staff's individual objectives);• the results of the annual appraisal exercise.
Data Subjects	CSS statutory staff



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data that is being processed in excel table CSS objectives 20XX is as follows:</p> <ul style="list-style-type: none">• Name and surname of all CSS staff;• Individual key performance indicators (KPIs) per person. <p>The personal data that is being processed in excel table Individual progress reports is as follows:</p> <ul style="list-style-type: none">• Name and surname;• Status and progress on KPI. <p>The personal data that is being processed in the word file Progress report of Common Services objectives is name and surname of CSS staff and more details on the individual objective (learning needs, trainings completed, etc.) on which is based the estimated progress of the team objective .</p>
Retention period	<p>The personal data are stored for the period of 1 year and 3 months in case there is no appeal procedure initiated. In case of appeal procedure initiated by the staff member, the data are stored till the completion of the procedure.</p>
Recipients of the data	<p>CSS statutory staff has access to the list of objectives (CSS objectives 20XX) and to the Progress report of Common Services objectives for information and in order to ensure the accomplishment of all team objectives for the year; Each staff member + TL + HoS have access to the individual progress reports (example) in order to be able to follow up on them and ensure the accomplishment of all individual objectives for the year.</p> <p>IBD Director has access to the Progress report of Common Services objectives for control purposes.</p> <p>Human Resources Department receives the data and process it according to DPN-2018-005 Staff Appraisals.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	<p>NO</p>
Are there any transfers of personal data to third countries or international organisations?	<p>NO</p>
General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/5886ae3f-7266-4b37-bc5c-21361a97238c</p>
EDPS Prior consultation	<p>NO</p>



Reference number	DPR-2018-046
Name of the processing operation	Compliance with EUIPO's Guidelines on management of external resources'
Last Updated:	28/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Head of Common services (CSS) in IBD, IBD management and IBD secretariat External processor: IDOM
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Further to the establishment of the Office's 'Guidelines for the management of external resources', in December 2015, Common Services in IBD proposed an implementation scheme with the objective to comply with the EUIPO's requirements in terms of external HR management ("Rules for the implementation of the guidelines on the management of external resources in IBD Common Services"). This objective has also been integrated into the CSS annual objectives for 2018.</p> <p>The excel table 'functional matrix' represents an action plan deliverable of the above-mentioned rules (cf. page 6, point 2):</p> <p>'No internal staff executing the same task as external resources. The outsourced task shall be clearly distinguishable from the rest of the processes. No replacement of internal staff by external resources'.</p> <p>In order to make sure that all the tasks performed by externals do not overlap with those carried out by statutory staff, CSS has elaborated and maintained a capacity management and competency matrix, taking into account the different job profiles in CSS.</p> <p>The table is monitored / updated on an annual basis and is not being used for evaluations.</p> <p>Apart from the Functional matrix, other data bases maintained in CSS in order to ensure the compliance with the Guidelines for management of external resources are as follows:</p> <ul style="list-style-type: none">• List of Contractors and Contract managers• List of Service managers for CSS;• List with generic mailboxes;
Purpose of the processing	The personal data is processed for the purpose of ensuring the compliance with Guidelines on management of external resources.
Data Subjects	CSS external and internal staff



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data processed in the Functional matrix is: staff member position; staff/resources status (external/internal); functions, tasks and details of tasks as follows:</p> <ul style="list-style-type: none">• whether the task can be or cannot be executed by external staff;• where the task is executed inside or outside EUIPO;• back-up available or not;• description of task in detail;• performance period;• time in min. to perform per unit;• number of units per period;• FTE - Full Time Equivalent;• cumulative FTE. <p>The personal data processed in the List of Contractors and Contract managers is as follows: name, surname, company of the contract manager, generic mailbox.</p> <p>The personal data processed in the List of Service managers for CSS is as follows: name, surname, company, service mailbox.</p> <p>The personal data processed in the List with generic mailboxes is name and surname of the person and the generic mailbox to which he/she has access.</p>
Retention period	<p>The personal data in the Functional matrix, the List of service managers and the List of generic mailboxes is stored for the period for which the person has a contract with the office. The personal data in the List of Contract managers is stored for the period for which the company has a contract with the office or the period for which the concrete person is entitled to perform the duties of a contract manager .</p>
Recipients of the data	<p>The CSS statutory staff has access to the Functional matrix in order to ensure they comply with the guidelines. External resources (IDOM) can be granted access on need-to-know basis (for audit and control purposes).</p> <p>As far as the Lists of contract managers, service managers and generic mailbox are concerned, only IBD management and IBD secretariat have access to the data for the purpose of contract management.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to [process name] is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f01848b2-b8f9-4210-b388-116cd2ce9e2c</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-048
Name of the processing operation	Mail and parcels distribution
Last Updated:	26/02/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal Processor: Internal Mail Distribution Coordinator IBD/EUIPO External Processor: External Provider of Archives, Reprography and Mail Distribution (EULEN).
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Internal distribution services in EUIPO include:</p> <ul style="list-style-type: none">• distributing mail from/to individual mailboxes,• preparation and collocation of identification labels on the individual/group mailboxes and offices;• custody and delivery of parcels. <p>These services are provided by a Service provider in line with the requirements specified in the contract and the work instruction QSD-0089 WI-Distribución interna. The external provider personnel receive the information regarding the exact location of each person that works in the EUIPO installations (onsite staff) from Remedy (New staff/r Move staff/Leave staff products). Once they receive the Remedy ticket for a person entering/moving/leaving in the Office, the Internal mail distribution team prepares and allocates the identification labels to the corresponding mailbox and office. In order to ensure the timely delivery of mails, the external provider maintains a table with the exact location of all EUIPO staff's office and mailbox. Mail Distribution team may receive information about the location of all staff and resources working in EUIPO premises from the Space management team in IBD in order to actualise its data base. Both internal mail and external mail are delivered to the in-tray or mailbox (in the mail sorting units in the corridors on each floor) that is closest to the user's office and bears the name of the employee, client, agent, external office/ company or department.</p> <p>The external provider sends a mail to the addressees informing them for the receipt of a parcel. The parcels are picked up from the Internal Mail Distribution personally by the addressee who signs for acknowledgement of save receipt of the parcel.</p>
Purpose of the processing	The purpose of the processing operation is to ensure timely and proper distribution of mails and parcels.
Data Subjects	All EUIPO staff and external resources who works in the office (onsite). Regarding the list of Parcels distribution, data subjects are the addressees of the parcels that have picked them up.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data processed is as follow:</p> <ul style="list-style-type: none">• In the Excel table with the exact location of EUIPO staff: name, building, floor, office number, location details, company.• In the Parcels' distribution lists: name, surname and signature. <p>The name and surname of all onsite staff is indicated on the offices' doors and the mail sorting units in the corridors on each floor.</p>



Retention period	<p>The retention period of the data is as follows:</p> <ul style="list-style-type: none">• the Excel table with the exact location of EUIPO staff is stored for the period of the contract of the person with the office;• the Parcels' distribution list is stored on paper for 6 months from the date of completion of the list.
Recipients of the data	<p>Mail distribution coordinator and the external provider of mail distribution have access to the Excel table in the folder Y:. Only the external provider has access to Parcels' distribution list stored on paper.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to [process name] is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>The paper documentation is locked in secured cupboards.</p> <p>The external provider staff signs an awareness declaration that the providers send to EUIPO in order to guarantee the compliance with the confidentiality clauses of their contracts.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement mail and parcel distribution:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/92320aae-68b6-4105-8d5c-1b7d5171c560</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-049
Name of the processing operation	Management of TM & Design paper documentation (TM & Design archive and TM & D Reprography).
Last Updated:	09/08/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal Processor: Coordinator of Archives services in IBD External Processor: External Provider of Archives, Reprography and Mail Distribution (EULEN)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO disposes of TM & D archive where the TM & D documentation is stored. The documentation can be loaned to EUIPO examiners upon official request by mail to Logistics team, IBD. The process of loaning of documentation (original or copy) from the TM & D archive is properly documented and includes processing of personal data in several data bases as follows:</p> <ul style="list-style-type: none">• Transmission sheet (that describes when the document has been loaned and returned, and provides the document traceability);• Excel sheet of requested documentation;• Excel sheet of documentation pending return;• Excel sheet of documentation returned;• Excel sheet of the documentation provided in copy to examiners; <p>The Transmission Sheet is a multipage form (4 pages).</p> <ul style="list-style-type: none">- White page – once signed by the Internal Mail Distribution, white page remains with the Archives (retention period 5 years from the return date of the TM or D documentation);- Yellow page - once signed by the examiner, yellow page remains with the Internal Mail Distribution (yellow page is destroyed by the Internal Mail Distribution, once the document is returned to the Archives);- Pink page - once signed by the Internal Mail Distribution, pink page remains with the Examiner;- Green page – once signed by the Archives, green page remains with Internal Mail Distribution (retention period 5 years from the return date of the TM or D documentation). <p>EUIPO trademark examiners sign the transmission sheet at the moment they receive/return the documentation. At the end of the service, logistics team may assess the satisfaction of the users of the service sending them a survey by mail. The survey does not contain personal data but the channel through which it is collected (Outlook) makes the person identifiable. For this reason the access to the mails is restricted and a retention period for their storage is established.</p> <p>The data from the transmission sheet is inserted in the Excel sheets described above in order to easily track the current location of the documentation, control the compliance with the established service level agreements and for elaboration of reports/statistics.</p> <p>When EUIPO trademark examiners need to copy/print TM documentation, they send their request by mail to the Logistics team of Infrastructures and Buildings Department (internal staff). At the end of the service, logistics team may assess the satisfaction of the users of the service sending them a survey by mail. The survey does not contain personal data but the channel through which it is collected (Outlook) makes the person identifiable. For this reason the access to these mails is restricted and a retention period for their storage is established.</p>



Purpose of the processing	<p>The purposes of the processing operation are as follows:</p> <ul style="list-style-type: none">• keep track and audit trail on the TM & D documentation and easily locate it at any time;• ensure the integrity of the TM & D documentation and the quality of the services provided to the users of TM & D documentation archive and TM & D documentation reprography services (The reprography services notified in this document are requested by mail and refer to TM documentation only. The central reprography services requested by the Remedy product Reprography requests are not subject of this record) ;• comply with requirements of internal and external audit;• comply with the applicable Financial regulation.
Data Subjects	Users of the TM & D archive and TM & D Reporgraphy services.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal information processed is as follows:</p> <ul style="list-style-type: none">• in the transmission sheet: name, surname, signature, date, office number of the requester.• in the Excel sheet of requested documentation: name, surname and date of loaning;• in the Excel sheet of documentation returned: name, surname and date of return;• in the Excel sheet of documentation pending return: name and surname of the person to whom the documentation has been loaned and, if applicable, of the person to whom the documentation has been passed;• in the Excel sheet of the documentation provided in copy to the examiners: name, surname and date of delivery;• in the Archives surveys and Reprography surveys : there is no personal data in the surveys, but the channel of collection of the surveys (Outlook) reveals the name of the person.
Retention period	<p>The retention period of the data is as follows:</p> <ul style="list-style-type: none">• For the Transmission sheet: till 5 years from the return date of the TM or Design documentation;• For the Excel sheet of requested documentation, the Excel sheet of documentation returned and the Excel sheet of the documentation provided in copy to examiners: 7 years because the authorising officer shall conserve the supporting documents relating to operations carried out for a period of five years from the date of the decision granting discharge in respect of implementation of the budget of the Office.• For the mails that contain the Archives /Reprography surveys: 1 year from the date of the receipt of the fulfilled survey.• For the Excel sheet of documentation pending return: till the documentation is returned.
Recipients of the data	The staff responsible for TM Archives and TM reprography in the Logistics team in IBD has access to all data. The external provider EULEN has access to the transmission sheets and the excel tables in Y: but does not have access to the surveys.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this process name is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p> <p>The paper documentation is locked in secured cupboards.</p> <p>The external provider staff signs an awareness declaration that the providers send to EUIPO in order to guarantee the compliance with the confidentiality clauses of their contracts.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement TM archive and reprography management: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6cdf81e8-7a0d-47d2-b0a1-804d861c726f
EDPS Prior consultation	NO



Reference number	DPR-2018-050
Name of the processing operation	Confidential destruction of documents
Last Updated:	09/08/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal Processor: Coordinator Confidential destruction process External Processor: External Provider of Archives, Reprography and Mail Distribution (EULEN)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	EUIPO staff can destroy confidential documentation by writing e-mail to the Logistics team and fulfilling the request for destruction of documents T-0021. The confidential destruction includes processing of personal data in the following documents: <ul style="list-style-type: none">• T0021 protocol for destruction• Excel sheet with all confidential destructions performed. EUIPO gives the right to the requester to be present at the destruction of the document in order to ensure the confidentiality of the process.
Purpose of the processing	The purpose of the processing operation is to ensure that there is an audit trail that proves that the documentation has been destroyed confidentially, permanently and irrevocably.
Data Subjects	EUIPO staff who has requested confidential destrucion of documentation.
Description of categories of persons whose data EUIPO processes and list of data categories	The T0021 protocol for destruction contains the following personal data of the person who has requested the destruction: name, surname, department, service, signature, number of boxes. The Excel sheet with all confidential destructions performed contains the following personal data: name and department of the requester, number of boxes, kgs, date of request and date of destruction.
Retention period	The data is retained for the period of 7 years because the authorising officer shall conserve the supporting documents relating to operations carried out for a period of five years from the date of the decision granting discharge in respect of implementation of the budget of the Office.
Recipients of the data	Logistics team in IBD and the external provider of the confidential destruction of documents have access to all data.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>Paper documentation is locked in secured cupboards.</p> <p>The external provider staff signs an awareness declaration that the providers send to EUIPO in order to guarantee the compliance with the confidentiality clauses of their contracts.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement confidential destruction :</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6b5c0971-909f-4018-b6b5-e7535143f422</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-051
Name of the processing operation	Record on data procession in the context of the Observatory Studies
Last Updated:	04/02/2019
Controller Organizational entity	Observatory
Controller contact details	Observatory@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In compliance with the mandate of Regulation (EU) No 386/2012, the Observatory publishes between 10 and 20 studies every year. There are 4 different ways of how the studies are carried out:</p> <ul style="list-style-type: none">• Directly by the Observatory staff: these studies are based on public information and only on company level, the data subjects are not natural persons.• Processed by a provider: in this case the data subjects are identified and selected by the Observatory staff as described above, and the information is stored and processed by the provider. The Observatory receives the resulting reports.• Endorsed to a provider: in this case the data subjects are identified, selected and the information is stored and processed by the provider. The Observatory only receives the resulting reports.• In collaboration with an institution or body: again, these studies are based on public information and only on company level, the data subjects are not natural persons.
Purpose of the processing	<p>Personal data is gathered to identify and contact contributors, collaborators or in some cases subjects of a study. In the above context, personal data may be forwarded to consultants or collaborating institutions or bodies, for them to contact potential contributors for information.</p> <p>Also, personal data may appear in the studies published by the Observatory in the acknowledgments, the listing of contributors, etc.</p>
Data Subjects	Contributors, collaborators or subjects of a study.
Description of categories of persons whose data EUIPO processes and list of data categories	<ul style="list-style-type: none">– Personal data such as names, e-mail addresses and sometimes telephone numbers may be forwarded to consultants or collaborating institutions or bodies, for them to be able to contact contributors for information– Names and professional affiliations may appear in the acknowledgements for their contribution in a particular study– Names and professional affiliations may appear in the reference as a source of information
Retention period	<p>Names of natural persons and professional affiliations mentioned in the studies stay published as long as the document in question remains on the Observatory web page.</p> <p>Additional information such as e-mail addresses, and sometimes telephone numbers and physical addresses of contributors, will be kept only for the time necessary to achieve the purpose for which they will be processed.</p>
Recipients of the data	<p>Providers and/or collaborating institutions or bodies for them to be able to contact the data subjects for information</p> <p>.</p> <p>Any personal data included in the report, such as the acknowledgements and references, are made available to the general public, through the publication of the study on the Observatory WEB.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	All personal data related to an Observatory study is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6871be97-96af-47bf-bb2d-ed51513613cb
EDPS Prior consultation	NO



Reference number	DPR-2018-053
Name of the processing operation	Processing personal data within the framework of Internal Mobility procedures at EUIPO
Last Updated:	28/07/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Head of Staffing, Development and Recognition Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data of statutory staff members (officials and temporary agents) concerning the candidate's applications for the Internal Mobility procedures at EUIPO.</p> <p>The Office may engage a member of temporary staff (2f) at grades AD 9, AD 10, AD 11 or, on an exceptional basis, at grade AD 12 . Those engagements shall be exceptional and justified by the Office in a central record kept by the Human Resources Department (HRD) in which personal data will be stored.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of processing personal data is:</p> <ul style="list-style-type: none">- to manage administratively the candidate's application(s) for an internal vacancy at the EUIPO, as well as the different stages of the internal mobility procedures, including the selection of candidates to work in third countries/ international organisations / EU delegations.- to process data to be uploaded in a central record kept by HRD concerning the engagement of a temporary staff members (2f) at grades AD 9, AD 10, AD 11 or, on an exceptional basis, at grade AD 12 . <p>The personal data are collected and processed in accordance with:</p> <ul style="list-style-type: none">- Articles 4, 7, and 29 (1) of the SR and Articles 10(1) and 55 of the CEOS;- Articles 3 to 6 of the Decision N°MB-16-16, on mobility issues (relate to movements within and between the European institutions).
Data Subjects	Statutory staff members: officials and temporary agents
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <ul style="list-style-type: none">- All personal data provided by the candidate as required by the vacancy notice (mainly CV/Talent Profile and possibly motivation letter). <p>Data processed in the central record registering the engagement of temporary staff (2f) at grades AD 9 to AD 12:</p> <ul style="list-style-type: none">- Vacancy notice reference and year of publication/ legal basis and justification/ full name of the person concerned recruited from the reserve list and comments if necessary (i.e. availability, start date). <p>Failure to provide the personal data required by the vacancy notice (mainly CV and possibly motivation letter) will exclude the candidate from the selection procedure.</p>
Retention period	<p>The processing of personal data starts from the moment the candidate submits his/her application to the vacancy. All personal data provided by the candidates in the context of this procedure will be stored electronically for a maximum period of 2 years.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Personal data will be supplied to the interested parties in the internal mobility exercise, i.e., the staff members of the Human Resources Department (HRD) , in charge of internal mobility and personnel administration, the Management of the organizational unit concerned and the selection committee members.</p> <p>Data kept on the central record are accessible to the AACC, the management and authorised staff of HRD, as well as to the Selection Committee for the part of the central record related to the selection procedure of which it is in charge of.</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p> <p>Data of Office´s staff selected to work in third countries /EU delegations will be disclosed, on a need to know basis, to authorized staff of EEAS / EU delegation for assistance in administrative procedures with the authorities of the host country.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	Within the framework of the Service Level Agreement between EEAS and EUIPO.
General Description of security measures	<p>Data stored in HR "Allegro" database may be transferred to external contractors /subcontractors, namely Adequasys (France). They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the application supporting the HR "Allegro" database.</p> <p>Regarding "SAP SuccessFactors" data are stored in the cloud in servers in SAP Germany and SAP Holland data centers. These information may be accessible by external contractors/subcontractors, namely SAP and EVERIS. They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting "SAP SuccessFactors".</p> <p>The data are not used for any other purposes nor disclosed to any other recipient. Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p> <p>Candidate's personal data are stored and processed according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients.</p> <p>The HR database "Allegro"/"SAP SuccessFactors", including "Alfresco/ShareDox" (storage in personal file) have restricted access rights designed by Departments. The accesses are given individually to each profile following the type of function in the Department.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Any information communicated to the administration or to the members of the selection committees which relates to internal mobility and reassignment procedures is considered to be confidential and may not be used without the consent of the persons concerned.</p> <p>Data processed by EEAS/EU delegations are stored on EEAS servers according to their security measures and processes accesses being provided only on a "need to know basis".</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data within the framework of within the framework of Internal Mobility procedures in EU: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/21827e3c-64e0-4a08-93a1-e5829e5c8536
EDPS Prior consultation	NO



Reference number	DPR-2018-054
Name of the processing operation	Processing personal data (including externalisation tasks)
Last Updated:	08/09/2020
Controller Organizational entity	Finance
Controller contact details	Director of the Finance Department FD.DataProtection@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Data is collected and managed by the Office to ensure that the revenue is assigned and payments are made to the correct counterparty. EUIPO is assisted by an external service provider for data key-in purposes and linking payment procedures who abides by the provisions related to the protection of personal data according to Regulation (EU) 2018/1725. The processing of personal data is not intended to be used for any automated decision making, including profiling.
Purpose of the processing	The purpose of the processing operation is: - the management of third party files (name, addresses, telephone, emails, contact person, bank accounts, IBAN and BIC codes, identity card number, passport number) - the key-in of invoices (name, addresses, telephone, fax, emails, contact person, bank account references (IBAN and BIC codes), VAT number, identity card number, passport number) - the key-in of data to allow for the payment of staff salaries, allowances and reimbursements, missions, trainings in/outside the Office, removal, travel expenses/place of origin, list of holidays not consumed by staff, reimbursement of some medical expenses (glasses, speech therapist, annual visit) - the key-in to allow the payment of Seconded National Experts, trainees, external resources and agency staff, external participants in meetings. - the identification and linking of payments and management of clients address, name, emails, fax, phone number and also the management of phone calls, by internal/external staff - to manage the list of inventories with the name of the users - to manage access rights to Clarity (user-id access).
Data Subjects	Personal data processed can concern: 1. EUIPO statutory staff and their relatives 2. Seconded National Experts, trainees 3. External resources, external participants in meetings and payers.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Personal data processed can concern:</p> <ol style="list-style-type: none">1. EUIPO statutory staff and their relatives2. Seconded National Experts, trainees3. External resources, external participants in meetings and payers. <p>The personal data for the 3 groups are collected in a third parties' file form.</p> <p>The categories/types of personal data processed may contain the following information:</p> <ul style="list-style-type: none">• identification data:<ul style="list-style-type: none">o name (first name, surname)o gender, nationality, place and date of birtho passport number or ID numbero signature of person or authorised representativeo title, position, department and companyo contact details (website and email address, fax, business and mobile telephone number, official postal address, country of residence)• bank account reference (IBAN and BIC codes), VAT number, national insurance number.
Retention period	<p>The data is subject to the administrative retention period stated in the Office's retention policy in force. Once the period has elapsed, paper documents stored in the Office Archives will be destroyed.</p> <p>The retention period runs from the date the file is closed. Furthermore, data is also kept until the deadline for filing a claim has been totally exhausted, and/or for the time necessary to resolve an appeal, a disciplinary procedure or an audit, if one started before the end of the above period.</p>
Recipients of the data	<p>Personal data collected will be treated confidentially and processed solely by authorised staff members and the external provider resources.</p> <p>The personal data may also be disclosed to the following recipients:</p> <ul style="list-style-type: none">• agency staff and/or trainees supporting statutory staff in carrying out their functions• EUIPO's Legal Service• EUIPO's Internal Audit Service• European Court of Auditors, OLAF, the European Court of Justice and other institutions (officials transfer). <p>Access may be allowed on a temporary and restricted basis to IT-technicians for customisation, development, updating, technical tests, repair, support and improvement of the database.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>All personal data related to this procedure are stored in secure IT applications according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients.</p> <p>The SAP and the third party files have restricted access rights designed for each type of information. The access rights are granted individually depending on the job profile.</p> <p>Working Excel sheet and Access tables have also restricted access rights.</p> <p>The processing of personal data by external providers is governed by the signed Contract (General Terms and Conditions applicable to supply, services and works Contracts with EUIPO) and Declaration of confidentiality and of absence of conflict of interests.</p> <p>EUIPO Staff and external resources in contact with medical expenses, are requested to sign a Declaration of Confidentiality. These documents are kept in a safe in Accounting and Treasury team.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on processing personal data (including externalisation of tasks) :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/8c86a0c2-9986-4ece-a520-595071f67a02</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-055
Name of the processing operation	Pre-selection, selection and recruitment procedures
Last Updated:	25/10/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Staffing, Development and Recognition Service HRD Head of Entitlements and Staff Welfare Service HRD For Agency Staff (Interims) Framework Contract cascade with Randstadt / Manpower/ Adecco EPSO (in some cases assists EUIPO with the selection of statutory staff)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

The EUIPO processes personal data to select personnel with a view to their recruitment (e.g. transfer, inter-agency mobility, CAST permanent) and /or to establish reserve lists of suitable statutory staff candidates (e.g. external procedure). In some cases, EPSO assists the European institutions and other EU bodies and agencies with the selection of statutory staff.

Data processing starts from the moment a candidate submits an application/registers in a database or, regarding candidates on a reserve list, when they confirm their interest in the recruitment process.

Candidates will provide the Office with data on their identity and qualifications because of the very nature of the selection/recruitment process.

The Office may engage a member of temporary staff at grades AD 9, AD 10, AD 11 or, on an exceptional basis, at grade AD 12. These engagements will be exceptional and justified by the Office in a central record kept by the Human Resources Department (HRD) in which personal data will be stored.

The Office may, by way of exception, organise an internal selection procedure enabling contract agents to advance to the next higher function group.

Data is processed in two main phases:

Selection phase

- Data submitted by candidates by means of the application or registration in the CAST permanent database will be processed to evaluate their eligibility, expertise and profile for a selection procedure. This evaluation is based on elements provided by the candidate in his or her CV and possibly by a motivation letter, as well as information introduced by candidates in their online account (Office website/EPSO website)



Purpose of the processing	<p>The purpose of processing personal data is to organise selection procedures for:</p> <ul style="list-style-type: none">- statutory staff (officials, temporary and contract agents);- trainees, national experts and agency staff. <p>Data are processed according to the Staff Regulations (SR) and Conditions of Employment of Other Servants (CEOS) of the European Union (EU), EUIPO administrative decisions and the framework contract under which agency staff can be hired.</p>
Data Subjects	<p>Candidates for the selection of statutory staff members (officials, temporary agents, contract agents). Candidates for the selection of trainees, national experts and agency staff (interims).</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories/types of personal data processed are the following:</p> <p>Selection phase: name, surname, address, email address, phone number, gender, nationality (proof of national identity card), date of birth, as well as data regarding professional experience and working periods including in other Institutions/Agencies), education, language and skills. This information is completed by a CV and a motivation letter both of which are uploaded by candidates in their online account. Adding a photo to the CV is entirely voluntary.</p> <p>Candidates are requested to provide at least two names and phone numbers of previous employers in their CV as the Office carries out reference checks as part of the selection process.</p> <p>Further personal data processed during the selection phase will be the results of the candidate's performance during the written and oral tests.</p> <p>Recruitment phase: when relevant reference check of selected candidates, availability to take up duties at the Office, medical aptitude of the candidate to perform the work at the Office (only mention "apt" / "not apt"), extract from the national police or criminal record / certificate of good conduct, proof of education and professional experience (originals need to be presented and certified copies are kept in the personal file of the person concerned), working periods in other Institutions/Agencies (including the function group, grade, step and seniority), name of persons to be informed in the event of accident including their contact data, as well as any requested document necessary to establish the classification in grade, the step, the seniority date and individual entitlements of the person concerned according to the SR and CEOS.</p> <p>Employers of agency staff (interims) and experts are obliged to request that their employees request the national police or criminal record extract and medical aptitude certificate (according to national legislation).</p> <p>Data processed on the central record registering the engagement of temporary staff f at grades AD 9 to AD 12: vacancy notice reference and year of publication, legal basis and justification, full name of the person concerned recruited from the reserve list and comments if necessary (i.e. availability, start date).</p>



Retention period

Personal data will be kept only for the time needed to achieve the purpose(s) for which it is processed. In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal process.

Officials, temporary agents and contract agents :

- For successful candidates: data of successful applications is kept in the personal file of the established statutory member of staff, in accordance with Article 26 SR. The personal data from the recruitment file is kept for 8 years after the expiry of all the rights of the person concerned and of any dependents, and for at least 120 years after the date of birth of the person concerned.

- For unsuccessful candidates: data is kept on file for 2 years after the candidates have been notified that they were unsuccessful.

- For statutory staff candidates whose names were placed on a reserve list but who are not offered a job at EUIPO or who do not take up a job offer: data is kept on file for 2 years after the expiry of the reserve list.

National experts:

- For successful candidates: data is kept for 7 years after the end of the period of service at EUIPO for reasons of budgetary discharge, control and audit;

- For unsuccessful candidates: data is kept for 2 years as from the date of notification of unsuccessful candidates.

Trainees:

- For successful candidates: data is kept for 7 years after the end of the period of service at the Office for reasons of budgetary discharge, control and audit.

After that, only the following essential data for providing a trainee's certificate is kept for a maximum of 50 years: first name, last name, length of traineeship, department involved in the training, traineeship report, nature of the work performed and remuneration received).

- For unsuccessful candidates: data is kept for 2 years after the official starting date of the traineeship period.

Agency staff:

- For successful candidates: data is kept for 7 years after the end of the period of service for budgetary discharge, control and audit;

- For unsuccessful candidates: data is kept for a maximum period of 5 years.

Spontaneous applications:

The Office does not consider any unsolicited applications. Candidates can only apply for a vacancy published through the channels indicated in the vacancy notice. Spontaneous applications will be deleted not later than 3 months after the date of receipt.



Recipients of the data	<p>Candidates' data is disclosed to HRD staff working in selection/recruitment procedures, the Department/Service line managers concerned and staff authorised by them, as well as Selection Committee members.</p> <p>Processing on behalf of the controller, with due respect of Article 29 of Regulation (EU) 2018/1725, will also need to be done by external providers.</p> <p>The EUIPO's reserve lists and expiry dates are published on the Office's website. Currently only the reserve list for officials, published by EPSO, includes the names of the successful candidates who gave prior consent. Reserve lists may be shared with other EU agencies, upon request and after having received the candidates' agreement.</p> <p>Personal data concerning trainees is also disclosed to Academy staff working with HRD on the selection of trainees, in particular the Pan European Seal Programme.</p> <p>Relevant data of candidates successfully recruited is disclosed, on a need-to-know basis, to AA/AACC, the Entitlements and Staff Welfare Service (HRD) to establish individual rights, the Office's Departments/Services (management and authorised persons for information and logistical purposes, the Finance Department and the Paymaster Office (PMO) for payments and to the Communication Service (CS) to update the staff directory.</p> <p>Data kept on the central record is accessible to the AACC, the management and authorised staff of HRD, as well as to the Selection Committee for the part of the central record related to the selection procedure of which it is in charge.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>Candidates' personal data is processed and stored in ShareDox, HR "Allegro" database and its modules (stored in MySQL database), as well as in HR "SAP SuccessFactors" in the cloud.</p> <p>Data kept in the staff member's personal file is stored in "OpenText tool" (personal file repository) kept in the Office's servers and accessible through "SAP SuccessFactors".</p> <p>Data stored in HR "Allegro" database may be transferred to external contractors /subcontractors. They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the application supporting the HR "Allegro" database and integrations with SAP BPC and Business Object systems. Data may also be transferred to an external contractor/subcontractor for the maintenance of integrations with Insite, AEOS and SuccessFactors IT systems.</p> <p>Regarding "SAP SuccessFactors", data is stored in cloud in servers in SAP Germany and SAP Holland data centers. This information may be accessible by external contractors/subcontractors. They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting "SAP SuccessFactors" and integrations of SuccessFactors with Remedy and Insite.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient. Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p> <p>Candidate's personal data is processed and stored according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients.</p> <p>The HR database "Allegro"/"SAP SuccessFactors", including "Alfresco/ShareDox" (storage in personal file) have restricted access rights designed by Departments. The accesses are given individually to each profile following the type of function in the Department.</p> <p>The HR database is password-protected under single sign-on system and connected automatically to the user's ID and general password. Replacing users is strictly prohibited. E-records are held securely to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Processing personal data within the framework of pre-selection, selection and recruitment procedures at the EUIPO : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/68285d66-748e-46a4-88ce-d5551d57b80b</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-056
Name of the processing operation	Processing of personal data within the framework of the Seat Agreement between EUIPO and the Ministry of Foreign Affairs, European Union and Cooperation (MAEC)
Last Updated:	10/02/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Joint Controller organizational entity	Other
Joint Controller contact details	Delegate of Data Protection dpd@maec.es
Name and contact details of processor	Head of Entitlements and Staff Welfare Service - HRD Spain: Ministry of Foreign Affairs, European Union and Cooperation (MAEC) and other other Spanish Services Tax Administration and Traffic Authority.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>Processing of personal data within the framework of the Seat Agreement establishing the provisions applicable to the relations between the EUIPO and Spain, in particular to the privileges, immunities, exemptions and tax facilities granted to the Office and to its accredited statutory staff.</p> <p>EUIPO staff members may request HRD to launch the following procedures:</p> <ul style="list-style-type: none">- Accreditation card for themselves and/or for their dependent family members;- OI plate for their car and/or an exemption of taxes for the acquisition of a vehicle for those who fulfill certain conditions;- Value added tax reimbursement for the acquisition of furniture and personal possessions for staff who fulfill certain conditions;- Importation/exportation of goods, for staff who fulfill certain conditions;- Non-EU driving permit exchange. <p>Depending on the procedure and nationality of the staff members concerned, different documents with personal data will be sent by HRD to the Ministry of Foreign Affairs, European Union and Cooperation (MAEC).</p> <p>The Seat Agreement is also used by the Office in order to facilitate the entrance, stay and residence of Seconded National Experts (SNE) of Non-EU member States and trainees.</p> <p>Specific situations concerning vehicles owned by EUIPO (official cars) / or by the staff members with OI plate:</p> <p>Offenses against road safety</p> <p>According to Spanish law, EUIPO has the obligation to provide to the Spanish authorities, under their request, the name of the person who has committed an offence in light of the traffic rules while driving a car owned by EUIPO and the name of the staff member whose OI-plated car was allegedly involved in an offence against road safety. This task is performed by HRD after informing the person concerned.</p> <p>Infringements of traffic concerning car vehicles:</p> <p>In case of an infringement to the traffic rules, HRD verifies the identity of the car owner and sends the letter received from the Spanish authorities:</p> <ul style="list-style-type: none">- either to the IBD Department, if the car is owned by EUIPO with / or without OI plate;- or to the staff member concerned, if his/her car uses an OI plate. <p>HRD informs the Spanish authorities that the staff member concerned has been requested to do the necessary directly with the authorities .</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The processing of data by the HRD is necessary to help staff to complete the forms/ file concerning their requests related to the privileges, rights or benefits applicable to EUIPO's statutory staff as established in Article 3 of the Seat Agreement.</p> <p>In compliance with the Spanish Law, the processing of data may also be used in the following specific situations concerning vehicles owned by EUIPO (official cars) / or by the staff members with OI plate:</p> <ul style="list-style-type: none">- Infringements of traffic concerning car vehicles;- Offenses against road safety.
Data Subjects	<p>Statutory staff members: officials, temporary agents, contract agents and their family members.</p> <p>Non statutory staff: Non-EU Seconded National Experts and trainees.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The data processed of the staff members, SNEs and trainees concerned are the following:</p> <p>Personal data:</p> <ul style="list-style-type: none">- Name, surname/ gender/ civil status/ date and place of birth/ country of origin;- Name of the staff member's father and mother;- Nationality/ Identity card N°/ type and N° of Passport/ Residence permit N°/ date of issue and expiry date of these documents;- Personal address/ personal telephone number;- Previous residence in Spain (Yes/or No)/ date of arrival in Spain/ Social security N°;- Driving permit/ vehicle registration documents and N° of plates;- Invoices of furniture and personal possessions for VAT reimbursements;- Photo and signature. <p>Professional data:</p> <ul style="list-style-type: none">- Working place/ category/ date of appointment/ job title;- Lucrative activity in Spain (if yes, which one). <p>In case of offenses / infringements of traffic, the content of the letter received from the Spanish authorities normally reveals the following data:</p> <ul style="list-style-type: none">- Model of vehicle and plate number;- Date, place and details of the infringement;- The picture taken by speed cameras may also be included in the letter. <p>Depending on the type of procedure, some of the above indicated data can also be processed for the spouse and children of the person concerned (e.g.: full name, birth date, country of birth, gender, passport/ identity card, address, country of origin, previous residence in Spain).</p>
<p>Retention period</p>	<p>The processing of personal data starts from the moment the staff member submits a request.</p> <p>All personal data processed in the framework of the Seat Agreement procedure will be stored electronically and / or on paper for a maximum period of 4 years after the end of service of the staff member concerned.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Spanish Authorities: Staff of the MAEC and other Spanish Services (inter alia, Tax Administration and Traffic Authority).</p> <p>EUIPO: Authorized staff of HRD working in the files /HRD management/ the Appointing Authority (AA) and the Authority Authorized to Conclude Contracts (AACC).</p> <p>Letters received from the Spanish authorities concerning offences and/or infringements of traffic rules:</p> <ul style="list-style-type: none">- For cars owned by EUIPO (both ordinary and OI plates), HRD will transmit the letters to the Head of the Common Services - IBD;- For cars of EUIPO's staff members using an OI plate, HRD will transmit the letter to the person concerned. <p>In the exceptional event that the purpose of the letter received from the Spanish authorities may not be identified based on the information included in the envelope, the Office Mailroom may open the letter prior to forwarding it to HRD.</p> <p>Furthermore, EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud or for supporting administrative procedures under request and supervision of EUIPO .</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to Seat Agreement procedures are stored in secure IT applications (ShareDOX, HR "Allegro" database and "SAP SuccessFactors") according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in these files.</p> <p>Appropriate levels of access are granted individually only to the above recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID. and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>MAEC: security measures according to LOPD 15/1999 and to the General Data Protection Regulation (EU)2016/679 of 29 April 2016.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing personal data within the framework of the Seat Agreement between EUIPO and the MAEC:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/025f7051-96d8-4b58-9ccf-edc15834c215</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-059
Name of the processing operation	Processing personal data in the follow-up on individual production procedures
Last Updated:	25/07/2019
Controller Organizational entity	Finance
Controller contact details	Director of the Finance Department FD.DataProtection@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of personal data of statutory staff members (officials and temporary agents) concerning the individual production and timeliness carried out according to Decision ADM 18-73 and tasks measured in the Finance Department. The processing of personal data is not intended to be used for any automated decision making, including profiling
Purpose of the processing	The purpose of processing personal data is: - FD Department can measure the production quantity data relating to tasks, according to Decision ADM 18-73 and Article 43 of the Staff Regulations, for the purpose of eventually using this objective information as one of the elements to be taken into consideration in the appraisal report of both the data subject concerned and their managers. The list of tasks measured may be considered during every appraisal exercise. Should this happen, it will be communicated to the staff whose activities are to be observed.
Data Subjects	Staff members (officials and temporary agents)
Description of categories of persons whose data EUIPO processes and list of data categories	The data processed are the following: <ul style="list-style-type: none">• the identification of the file concerned• type of tasks• the date when the task was allocated to the data subject• the date when the task was executed in the system• the date when the task was due• if the task was completed in due time (timeliness)• the outcome of the task• the organisational unit (service/team) where the tasks were performed• the name and/or identifier of the data subject who performed the task• task allocation (proportion of time dedication to specific tasks or areas of activity).
Retention period	Your personal data will be kept only for the time necessary to achieve the purposes for which they will be processed. The data will be only retained for a maximum period of two years after the end of the appraisal period in order to allow the management to use the data for the appraisal of the staff members concerned, and the latter to exercise their rights as provided for in the internal rules on appraisal and/or in Article 90(2) SR. After this period, all individual data extracted in electronic form will be deleted and no longer archived, and all other copies in any form will be destroyed unless they need to be kept longer to establish, exercise or defend a right in a legal claim pending before the court.



Recipients of the data	<p>Personal data is disclosed to the following recipients: FD management, FD team leaders.</p> <p>Information concerning management of FD staff work reports will be shared only with those required on a need-to-know basis. Personal data is not used for any other purposes or disclosed to any other recipient(s).</p> <p>Personal data will not be communicated to third parties, except where necessary for the purpose(s) outlined above.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>Personal data is stored in secure IT applications according to the Office's security standards, as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients.</p> <p>These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within in the follow-up on individual production procedures :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/487e770d-c16c-4919-ac48-09ad92659f33</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-060
Name of the processing operation	Processing personal data in procurement and grant procedures
Last Updated:	07/09/2020
Controller Organizational entity	Finance
Controller contact details	Director of the Finance Department FD.DataProtection@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of personal data for procurement and grant procedures and calls for expressions of interest for the selection of experts. The processing of personal data is not intended to be used for any automated decision making, including profiling.
Purpose of the processing	The purpose of processing personal data is: Data is collected and managed by the Office to evaluate the eligibility of economic operators/applicants, partners/affiliated entities and subcontractors to participate in procurement or grant procedures, and/or evaluate the content of tenders or proposals submitted during the procurement/grant procedures with a view to awarding the contract or agreement . Certain data is necessary for the execution of the contracts/agreements awarded.
Data Subjects	Personal data processed can concern the tenderer/applicant, their partners and affiliated entities, subcontractors and their staff (both natural and legal persons).
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data processed can concern the tenderer/applicant, their partners and affiliated entities, subcontractors and their staff (both natural and legal persons). The categories/types of personal data processed are as follows: <ul style="list-style-type: none">• identification data:<ul style="list-style-type: none">o name (first name, surname, previous surname);o gender, nationality, place and date of birth;o passport number and ID number;o signature of person or authorised representative;o title, position, functions, department and company;o contact details (website and email address, fax, business and mobile telephone number, official postal address, country of residence);• personal data contained in certificates for social security contributions and taxes paid, extracts from judicial records;• bank account reference (IBAN and BIC codes), VAT number, national insurance number;• documents for the evaluation of selection criteria or eligibility criteria (expertise, technical skills and languages, educational background, professional experience including details on current and past employment); proof of security clearance and declaration of honour that they are not in one of the exclusion situations and/or administrative sanctions referred to in Article 136 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012, hereinafter Regulation 2018/1046.



Retention period

Procurement and grant procedures:

For successful tenderers/applicants, procurement and grant files are subject to an administrative retention period of up to 7 years following the signature of the contract, in line with the Office's retention policy and schedule for financial files. For unsuccessful tenders/proposals the retention period lasts up to 5 years.

Personal data referring to natural persons published on the Office website for both procedures shall be removed 2 years after the end of the financial year in which the funds were awarded. The same shall apply to personal data referring to legal persons for whom the official title identifies one or more natural persons.

Selection of experts:

Files including personal data related to the selection of experts are to be retained until the end of the validity period of the relevant lists of experts, and then stored in the archives for an additional 5 years. Extracts from judicial records can be kept only for 2 years after the completion of a particular procedure. Files related to unsuccessful candidates will be deleted at the end of the selection process, before the relevant list of experts is published.

Once the period mentioned above has elapsed, paper documents and media stored in the Office Archives will be destroyed.

The retention period runs from the date the file is closed. Furthermore, data is also kept until the deadline for filing a claim has been totally exhausted, and/or for the time necessary to resolve an appeal, a disciplinary procedure or an audit, if one started before the end of the above period.



Recipients of the data	<p>Personal data collected will be treated confidentially and processed solely by authorised staff members dealing with procurement and grant procedures, including staff dealing with financial matters and members of the opening and evaluation committees, exclusively for management and administration purposes. If applicable, external experts and contractors assisting the Office with evaluations may be granted access to personal data on a need-to-know basis after signing a Declaration of confidentiality and of absence of conflict of interests.</p> <p>Some personal data is also disclosed to the public in order to meet the obligation to publish information on the outcome of procurement and grant procedures. The information disclosed is as follows:</p> <ul style="list-style-type: none">• for procurement procedures involving contracts worth more than EUR 15 000, the following data will be published in supplement S of the Official Journal of the European Union and/or on the website of the Office:<ul style="list-style-type: none">o name of the contractor;o subject matter of the contract;o amount legally committed.• procurement procedures involving contracts worth EUR 15 000 or less are not published, in order to protect personal data;• for grant procedures:<ul style="list-style-type: none">a) the name of the beneficiary;b) the locality of the beneficiary, namely:<ul style="list-style-type: none">i. the address of the recipient when the beneficiary is a legal person;ii. the region on NUTS 2 level when the beneficiary is a natural person;c) the amount legally committed;d) the nature and purpose of the grant.• scholarships and other direct support paid to persons most in need are exempt from publication. <p>Furthermore, upon request, data may be transferred to the legal advisors of the Office, the European Court of Auditors, the European Anti-Fraud Office (OLAF), the Internal Audit Service of the Office and the Court of Justice. The data transferred is limited to that strictly necessary for managing the procurement and/or grant procedures, or for official investigations or audits</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>Personal data is stored in secure IT applications according to the Office's security standards, as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients.</p> <p>These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data in procurement and grant procedures :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/50fc8e82-0979-406a-8bc6-318bcf5d3d0f</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-061
Name of the processing operation	Reimbursement of expenses related to language stays for dependent children of EUIPO's staff members.
Last Updated:	03/06/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO facilitates the learning of languages for dependent children of its statutory staff members by reimbursing part of the expenses related to language stays taking place in official learning centers during the summer school holidays and outside the children's home (e.g.: summer camps, etc.).</p> <p>It concerns officials, temporary agents, contract agents and their dependent children who are between 6 and 17 years old.</p> <p>The staff members concerned shall send to the Human Resources Department (HRD) the following documents supporting their applications:</p> <ul style="list-style-type: none">- Invoices and proof of payment of the activity;- Invoices and proof of payment of collective transport (if applicable)- Activities programme that prove overnight stay and language lessons or immersion programme;- Income proof of the family members who do not work at EUIPO. <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p> <p>Processing of personal data within the framework of the reimbursement of expenses related to language stays for dependent children of EUIPO's staff members.</p>
Purpose of the processing	<p>The processing of personal data is necessary to assess the admissibility of the applications and to grant the reimbursement of the language stays expenses in accordance with the rules laid down by the Decision ADM N°11-22 of 04/04/2011.</p> <p>The reimbursement of the language stay will correspond to the lowest ceiling indicated in the DEC ADM N°11-22: either the income group's one or the 50% of eligible expenses.</p>
Data Subjects	Statutory staff members: officials, temporary agents and contract agents Family members: family composition of the staff member concerned (e.g.: children/ spouse/ other persons)



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The individual data of the persons concerned and their family members are processed only on a need to know basis.</p> <p>Staff member and other family members:</p> <ul style="list-style-type: none">- Name, surname and personal number;- Composition of the family (number of dependent children/persons);- Income (salary slips) of the children's father / mother working at EUIPO;- Income (salary slips) of other family members not working at EUIPO;- Unemployment certificate and allowances received by the children's family members (if applicable);- Bank account number. <p>Staff member's children participating in the language stay, programme and costs:</p> <ul style="list-style-type: none">- Name / surname / date of birth;- Programme of activities stating the children's residence outside their family home during the learning stay;- Starting date / End date;- Total costs, including transport;- Amount to be reimbursed.
Retention period	<p>Successful applications for the reimbursement language stays expenses are kept during a period of 7 years after the last payment is done (time necessary for budgetary discharge).</p> <p>Applications which have not been accepted are kept during a period of time not longer than 4 months for eventual appeal purposes.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Data are disclosed to staff and line managers of HRD and Finance Department (FD) working in these files.</p> <p>Data can also be disclosed to the Appointing Authority (AA)/ Authority Authorized to Conclude Contracts (AACC) and the Social Assistant (HRD).</p> <p>EUIPO contractors and subcontractors might have access to data for maintenance and development of the applications supporting "HR Allegro" and "SAP SuccessFactors" under request and supervision of EUIPO.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient. Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Personal data are stored in secure IT applications (ShareDOX, HR "Allegro" database and "SAP SuccessFactors") according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in these files.</p> <p>Appropriate levels of access are granted individually only to the above recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID. and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data within the framework of reimbursement of expenses related to language stays : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/b3d16704-8b01-40ef-bd65-3dfd019f077e
EDPS Prior consultation	NO



Reference number	DPR-2018-062
Name of the processing operation	Processing personal data in the context of the Orphan Works database
Last Updated:	22/01/2019
Controller Organizational entity	Observatory
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	EUIPO IT administrators for the purposes of maintenance of the database.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>As foreseen by Article 3 of the Directive 2012/28/EU, EUIPO is responsible for the establishment and management of a single publicly accessible online database of orphan works.</p> <p>This database is accessible from the Observatory's website and is used by different user profiles (Beneficiary Organisations, Competent National Authorities, general public). The processing of data is automatic, i.e. the data is provided via the Orphan Works database.</p>
Purpose of the processing	Following the mandate of Directive 2012/28/EU, it is implemented as a single EU database by means of which it can develop a collaboration network in order to ensure the exchange of the information related to orphan works between all the Member States
Data Subjects	Identified authors, claimers and beneficiary organisations



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>1. IDENTIFIED AUTHORS: The database can store and process personal information (names and surnames) of natural persons related with orphan works, namely identified right holders, such as authors, co-authors, performers, phonogram producers, producers of first fixation of film, co-producers, publishers, broadcasters, translators etc.</p> <p>2. CLAIMERS: In addition, the database can store and process personal information (names, surnames, e-mails, addresses, telephone numbers) of potential right holders that would like to file a claim for a status change of orphan work. Such information will not be disclosed to the public and will be made available only to the beneficiary organisations using orphan works (libraries, museums, archives, broadcasting organisations).</p> <p>3. BENEFICIARY ORGANISATIONS: The database will also contain personal information (names, surnames, e-mails, addresses, telephone numbers) of individual users that login with the appropriate credentials to the orphan works database, such as representatives of beneficiary organisations and Competent National Authorities. Personal information of individual users of the database will not be disclosed to the public.</p> <p>4. NEW RECORD: When filling in a new record of orphan work the user may, when such information is available, provide personal data, such as name and surname of identified right holder. In case the right holder has remained anonymous, the user may specify this in the database. If right holder has been identified and located and authorised use of work in relation to rights he/she holds (applicable for partial orphan works), the user will specify "identified and located" in the appropriate field.</p> <p>The user will be informed about the success of the orphan work record's submission via an automatic notification generated by the database. Once the information is forwarded by the Competent National Authority, an automatic e-mail notification will be sent to the record's submitter.</p> <p>In all the processes related to orphan work record, such as update of orphan work record or information about possible errors in the record, claiming of status change of orphan work record, the user will be informed by sending an automatic e-mail notification by the system.</p> <p>It should be noted that the EUIPO will not have the possibility to record or modify any data contained in the database, as only the beneficiaries of the orphan works in the Member States will be able to do so.</p>
<p>Retention period</p>	<p>Taking into account that one of the purposes of Directive 2012/58/EU is to facilitate right holders' identification in respect of works that appear to be orphans, personal data related to orphan works will be stored in the database for an unlimited period of time.</p> <p>When the status of orphan work is changed to not orphan or to partial orphan, personal data of identified and located right holders of such works will not be displayed to the general public. The retention period of data for works declared as not orphans will be established for a minimum period of 70 years from the entry in the database. Any extinction of the retention period will be decided by the beneficiary organisation that controls the data.</p>
<p>Recipients of the data</p>	<p>BENEFICIARY ORGANIZATIONS:</p> <p>The data will be made available only to the beneficiary organisations using Orphan works database (libraries, museums, archives, broadcasting organisations). The list of beneficiary organisations using the Orphan Works database is stored in ShareDox under:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/3d6158fb-fba9-43e6-ba67-d5c76c55a926</p> <p>Information about identified and located right holders which authorized use of work in relation to rights they hold (partial orphan works) will be made available to the relevant beneficiary organizations but not to the general public. From the general public such data will be hidden and replaced by a mention "identified and located".</p> <p>GENERAL PUBLIC:</p> <p>The general public will have access to personal information (such as names and surnames) of right holders of orphan works which have been identified but not located.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	Beneficiary organizations from Norway, Island and Lichtenstein (EEA countries).
General Description of security measures	<p>All personal data related to Orphan works is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Captcha is implemented for public forms, e.g. claiming of status change, registration of organisation user form.• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing personal data in the context of the Orphan Works database:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/b4d7e065-564f-47a5-8557-4248af18e524</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-066
Name of the processing operation	Machine Translation service for the Office's IP Case Law
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euipo.europa.eu.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Through the eSearch Case Law/plus applications, the service provides automatic translation of EUIPO decisions from the Boards of Appeal, EUIPO first instance decisions and Judgements from the General Court and European Court of Justice, free of charge. The service provides users with the possibility of having an immediate and general understanding of the content and meaning of case law documents. The processing operation is fully automated via the Machine Translation Tool. Decisions, source documents and machine translations, are stored in ShareDox, translated by the eTranslation tool provided by the European Commission, and published on the eSearch Case Law application on EUIPO website.
Purpose of the processing	The purpose of the processing operation is to provide an automatic translations service for EUIPO decisions available through the eSearch Case Law/plus applications to the general public.
Data Subjects	Data subjects: <ul style="list-style-type: none">• Parties involved in the appeal and legal representatives.• BoA, CJEU and EUIPO members• BoA Staff in appeal proceedings.
Description of categories of persons whose data EUIPO processes and list of data categories	Data subjects: <ul style="list-style-type: none">• Parties involved in the appeal and legal representatives.• BoA, CJEU and EUIPO members BoA Staff in appeal proceedings. Data categories: Case law decisions published on EUIPO eSearch Case Law/plus application. Specifically the following categories of data are currently automatically translated in Production: <ul style="list-style-type: none">- Identification data: name, surname, address;- Decision: number, date, case reference, outcome, board members name and signature.
Retention period	Indefinitely as it is necessary for the purposes of public tasks entitled to the Office and duty to inform third parties about IP rights.
Recipients of the data	General public and EUIPO staff. Internal processor: Name, position: Team leader of the Advance Linguistic Solutions team Organizational entity: Customer Department (CD), Business Communications Service (BCS).



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the machine translation service is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>The machine translation is produced using eTranslation, a service provided by the European Commission. The connection between the EUIPO and eTranslation is set using the sTesta secure network.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement:</p> <p>https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/eSearch_Case_Law_en.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-067
Name of the processing operation	Mail management services
Last Updated:	18/05/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Joint Controller organizational entity	Infrastructures and Buildings
Name and contact details of processor	Internal processor: Mail management internal coordinator and Head of Common services External processors: Severiano Servicio Móvil S.A. (SSM) DHL Express, S.L.U- hadlfnfg outgoing Office correspondence by post or courier
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Mail management (MM) Services are:</p> <ul style="list-style-type: none">• Mailroom (MR). This area is in charge of handling, digitalising and sorting all incoming correspondence (i.e. mails /parcels that are delivered directly or sent by fax or post to the Office).• Mail Dispatch (MD). This area's main responsibility is to 'identify', divide and index all incoming correspondence that was previously processed by the Mailroom (mail, faxes and some e-communications), and link it to the respective core-business file or forward it to the relevant Office unit to deal with, in accordance with pre-established rules.• Key-in. This area is in charge of keying-in any offline EUTM and RCD applications as well as other key-ins such as oppositions, cancellations, partial surrenders, inspection requests, PER details, invoice details or internal payment orders (i.e. trainees, missions, SNEs, etc.). <p>The Mail Management Services are also in charge of handling all outgoing Office correspondence by post or courier. The process is partially automated. The provider uses Excel sheets, databases and Office IT systems (common ones and specific ones such as Oracle used in the digitalisation process).</p> <p>The external provider keeps the data anonymised for statistical purposes.</p> <p>When mails/packages arrive at the Mailroom, the external provider takes a photo of the data of the sender/addressee available on the front side of the mail/package (name, surname, address) with an Office device (camera) provided to them for this purpose. Afterwards, the provider uploads the photos in an electronic folder (\prod.oami.euprod-cb-mailroom-activities) created by DTD for this purpose and deletes the photos from the Office device.</p> <p>The external provider keys-in data for most of the Office's departments and does not have the responsibility of what is done with that data once digitalised, keyed-in, linked or dispatched to corresponding department. Once the data is digitalised, it is sent to the relevant Office tools to which the Office's Retention Policy applies:</p> <ul style="list-style-type: none">• IP-related documents are sent to Archives.• Non IP-related documents are sent to ARCAD or to the corresponding department.• Digitalised correspondence is stored in DAS and in some instances SAP (financial documents).



Purpose of the processing	<p>The purposes of the processing operation are:</p> <ul style="list-style-type: none">• To ensure sustainable, timely and quality management of EUIPO correspondence;• To ensure timely and quality key-in activities.
Data Subjects	<p>Data subjects are external users and internal staff such as temporary agents, contract agents or officials.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects are:</p> <ul style="list-style-type: none">• external users and internal staff such as temporary agents, contract agents or officials. <p>Types of data processed are:</p> <ul style="list-style-type: none">• Identification data such as name, internal Office ID number and contact details (email, address, telephone number);• Financial data such as bank accounts to debit/link payments• Data contained in IP rights such as trade mark denominations, goods and services, earlier rights, seniorities. <p>Type of incoming documents: emails, faxes, e-filings and post (paper form).</p>
Retention period	<p>The personal data will be kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>The photos of the mails/packages received in Mailroom (with the data of the sender/addressee) stored in an electronic folder are retained for 10 years.</p> <p>The information retained by the external provider in ShareDOX does not include personal data.</p>
Recipients of the data	<p>EUIPO staff (examiners and Finance department), the sender, any person/entity related to the case at hand and the general public at wide as they have access to anything published on the Office's website. Only certain financial data or other data that users specifically request to be kept confidential are not published. Once processed, most of the data is published and available online. Deferred RCD applications and some financial details are only accessible for certain Office staff that needs this information to work.</p> <p>Only certain staff such as Severiano staff (current contract provider), IBD logistics team responsible for the service and MM services contract manager have direct access to the Mailroom facilities and to the folder where the photos of the mails/packages are stored.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	The data is transmitted to DHL Express Spain which transfers it to third countries using binding corporate rules.



General Description of security measures	<p>All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) <p>Confidentiality and data protection clauses are signed-off by the service provider.</p> <p>The Office device which is used for taking of photos of the mails/packages received in Mailroom is used only by authorised staff of the external provider and does not leave the Mailroom which is a restricted area. It is locked in a cupboard when it is not used.</p> <p>The physical access to the Mailroom facilities is restricted, in order to ensure the organisational security measures for the documentation on paper. The access to the Mailroom is limited to Severiano staff, IBD Logistics team responsible for the service and the mail services contract managers . Most staff and all other external providers must request access and are always accompanied by Severiano’s staff.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/884d0522-db19-47e6-a913-cf1cffdb5f46
EDPS Prior consultation	NO



Reference number	DPR-2018-068 (update of DPN-2014-002)
Name of the processing operation	Events Platform
Last Updated:	29/05/2019
Controller Organizational entity	ICLAD
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain
Name and contact details of processor	Personal data is processed by authorised ICLAD staff, supported by the external service providers Deloitte and Pomilio Blumm, acting as external data processors. For event management purposes, personal data is also processed by the Infrastructures and Buildings Department (IBD) and the Communications Service (CS), acting as internal processors.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of personal data in the Events Platform of EUIPO
Purpose of the processing	Personal data is processed for the purposes of management of events, including all external and internal events which the Office manages or is involved in. It is also used to provide a sound system for reporting to fully understand all the events related to the activities of the Office and to keep relevant information related to each event to manage them appropriately.
Data Subjects	The persons attending an event.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories/types of personal data processed include the name and contact details of the person(s) attending an event, department, event title, date, location, country, names in the programme and report, comments by the requester or the ED, email address of the participant's line manager, name of the person representing an external organisation, name of the person responsible for follow-up action, as requested in the Event Participation Form and in the Event Report Form.</p> <p>For the purpose of submission for approval by the Executive Director, the first and last name, email and telephone number of the person requesting the Office to host an event using the Office's facilities (booking EUIPO facilities to celebrate an event, for a guided visit on EUIPO premises for a specific group and for EU institutions and bodies as well as the European IPOs to book the Brussels Liaison Office meeting facilities) will be processed.</p>
Retention period	<p>Personal data will be kept only for the time needed to achieve the purpose for which it is processed.</p> <p>Collected personal data are stored as long as follow-up actions are needed in the context of the event concerned. All personal data will be deleted 10 years after the last action in relation to the event. Personal data which are to be stored for historical, statistical or scientific use should be kept only in anonymous form.</p>
Recipients of the data	The person(s) attending the event, the manager(s) of the EUIPO staff member person attending the event, the Executive Director, the staff of the Missions Office (HRD) and other staff duly authorised to use the Event Platform have access to the data. The staff of the Office having access to Insite using a login and password may only access the event title, date, location and country in the Events Calendar.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to the processing operation is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Confidentiality and data protection clauses are signed-off by the service provider. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement on processing personal data in the Events Platform :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/65fb8752-73fb-4b-b6-bc9d-88cb34abb420</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-071
Name of the processing operation	Management of User Interactions
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euiipo.europa.eu
Name and contact details of processor	External processor: Name, position: Service Manager Organizational entity: exTEL Contact Centre The Information Centre (First Line) services are carried out by the external service provider eXTEL Contact Centre that follows the instructions and acts on behalf of the EUIPO.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

Customer Care Team, comprised by Information Centre (First Line and Second Line) and Complaints, deal directly with Office customers by providing them with information services and managing their complaints. For the purpose of performing these tasks, it is necessary that they collect and process personal data pertaining to individual staff members and customers contacting the Office through phone calls, emails, website (i.e. User Area and online forms), online chat, faxes, letters, personal visits, etc.

This data is also partially passed to and/or extracted and processed by Customer Feedback team for the purpose of analysing and identifying areas of improvement for services rendered to the EUIPO's users.

The processing activity is carried out through various IT tools but revolves mainly around SAP CRM. SAP CRM is an integrated customer relationship management software that compiles information on customers and their interactions with the Office from several sources, such as:

- SAP BCM: the contact centre used by the Information Centre for the handling of telephone interactions with EUIPO customers.
- Mail delivery: the tool used for the delivery and receipt of electronic communications.
- EUIPO Portal: the platform processing all information collected and managed in the EUIPO website (e.g. online forms and surveys, User Area, eSearch plus, etc.)
- LimeSurvey: the online survey tool used to gather feedback from users following an interaction with the Office
- External providers by any communication channel (e.g. phone, email, etc.).
- QFMAN: the system allowing the storage, management and dispatching of faxes and letters.
- PER: the database containing all contact and personal details pertaining to EUTM/RCD Representatives and Owners.

The information stored in SAP CRM is also further processed through the following systems/databases:

- Microsoft Outlook when the interaction requires assistance from another team or department
- BMC Remedy when the interaction relates to a technical incident and is sent to the E-business support line
- MS Access database for the management of interactions requiring follow-up
- MS Access database for the management of Key Users
- Getresponse licence to deliver subscriptions to news and events
- Excel tables on ShareDOX for the follow-up of complaints, suggestions and feedback
- A dynamic excel table on ShareDOX used to monitor the call-back requests sent to OD examiners.
- IPTool in order to make the interactions related to a specific file available to the examiners.
- SAP BusinessObjects and Kibana in order to generate statistical reports.



Purpose of the processing	<p>The purposes of the processing activity covered by this notification are to:</p> <ul style="list-style-type: none">• Facilitate the management of users' interactions with the EUIPO (user queries and complaints).• Improve the efficiency and the quality of the information services rendered to the EUIPO's users.• Contact users for any follow up and for further communications with regard to news on trade marks or designs, invitations to seminars, workshops, and any other communications related to EUIPO products and services. Certificates of attendance may be issued to the participants.• Produce statistical reports with the aim of:<ul style="list-style-type: none">o obtaining metrics regarding user interactions, EUIPO accessibility and response time to ensure compliance with the EUIPO Service Charter;o ensuring that Service-Level Agreements are achieved by the external providers;o Identifying areas of improvement and facilitate the planning and coordination of workflow and teams.
Data Subjects	<p>Data subjects:</p> <ul style="list-style-type: none">• Users contacting the EUIPO• Staff from Information Centre (First Line and Second Line) and Key User Managers
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects:</p> <ul style="list-style-type: none">• Users contacting the EUIPO• Staff from Information Centre (First Line and Second Line) and Key User Managers <p>Data categories:</p> <ul style="list-style-type: none">• Contact information: First name, last name, username, company name, address, country, phone number, fax number, email address.• Interaction data: interaction record/complaint ID, time, date, language, country, status, channel, subject, content or description of the interaction, categorization, File number, Responsible group, Responsible for reply, Employee responsible, Previous interaction• Identification data: PER ID, country, languages, status of the file, examiners in charge of the file and any other data obtained from EUIPO's back office systems.
Retention period	<p>The personal data is kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>Personal data are kept for a period corresponding to the lifetime of the EUTM or RCD file they relate to. Data processed by Customer Feedback Team falls under the established retention period for documents saved in Sharedox (5 years).</p> <p>The certificates of attendance are needed to be kept for 2 years in order to reply to external participants' requests.</p>



Recipients of the data	<ul style="list-style-type: none">• The Customer Department, and in particular, Information Centre (First Line and Second Line), Complaints and Key User Management.• Internal and external staff from DTD for the technical maintenance of the IT tools.• Staff from the E-business support line (DTD)• Examiners• Staff from other departments on a need-to-know basis according to the content of the interaction <p>Internal processor:</p> <p>1.Name, position: Head of Service of the Customer Management Service</p> <p>Organizational entity: Customer Management Service (CMS) – Customer Care Team and Customer Feedback Team</p> <p>2. Name, position: Director</p> <p>Organizational entity: Digital Transformation Department (DTD)</p> <p>Internal processor:</p> <p>1. Name, position: Head of Service of the Customer Management Service</p> <p>Organizational entity: Customer Management Service (CMS) – Customer Care Team and Customer Feedback Team</p> <p>2. Name, position: Director of the Digital Transformation Department (DTD).</p> <p>Organizational entity: Digital Transformation Department</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to Management of User Interactions is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Confidentiality and data protection clauses are signed-off by the service provider. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/Management_of_User_Interactions_en.pdf
EDPS Prior consultation	NO



Reference number	DPR-2018-072
Name of the processing operation	Administrative lists/ excel tables regarding task allocation and distribution (in particular Registry Task Distribution List; List of currently pending tasks; List regarding the Quality Reading Team organization)
Last Updated:	25/03/2019
Controller Organizational entity	Boards of Appeal
Controller contact details	Boards of Appeal (BoA) of the European Union Intellectual Property Office (EUIPO), Avenida de Europa 4, ES-02008 Alicante, Spain BOA-Registry@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The Registry keeps administrative lists in order to allow the efficient distribution and follow-up of its tasks. The lists in form of excel tables provide information on the tasks for which a certain staff member has been trained and on the tasks which it cannot perform. The list of currently pending tasks gives an overview of the things to be done (priority of the task, kind of the tasks, status, leading responsibility, other responsible persons, start date, deadline, notes, effort etc.). In case of the list of responsible persons for quality reading, the information is ordered by languages.
Purpose of the processing	To have an overview of staff resources and profiles and to manage the tasks allocation. The purpose of such lists is, in particular, to be able to: <ul style="list-style-type: none">• Establish and efficiently manage capacities of Registry staff involved in Registry tasks and Registry staff involved in other BoA tasks in a given area (e.g. support of the KIS-Service in the task of quality reading; the term 'quality reading' is used as an equivalent for 'proof reading'. The decisions are not evaluated substance-wise. They are only checked for spelling- and formatting errors.), taking account of e.g. the language profiles of staff members;• assist in the approval of annual vacation, in view of the pending workload and availability of resources;• cover unforeseen absences;• allow Registry staff to check which colleagues they have to contact with regard to a specific issue. <p>The lists are not used for the evaluation of staff performance and they do not contain any information on individual performance. Neither do they contain information on staff absences.</p>
Data Subjects	Registry staff members and with regard to the 'quality reading list' also other BoA staff involved in the task of quality reading.
Description of categories of persons whose data EUIPO processes and list of data categories	Work related personal information of Registry staff and other BoA staff involved in Registry tasks: <ul style="list-style-type: none">• staff member name (in particular requestor; implementer);• work contact details;• indication for which tasks a certain staff member has been trained and which tasks he / she is not able to perform;• indication of languages spoken;• list of currently pending tasks.
Retention period	The lists are permanently updated to reflect the current status quo. Therefore, personal data is only kept as long as it is relevant. The moment a staff member leaves the Registry or stops being involved in quality reading or the moment a task is fulfilled, the respective data is deleted from the lists.
Recipients of the data	Registry staff members and BoA KIS members working closely together with the Registry. The 'BoA Quality Reading team organization'-list is published on the Intranet (Boards of Appeal -> BoA Utilities -> Decision drafting and Quality Reading -> Quality Reading – Team Organization) so that all staff (in particular BoA staff) can easily find out whom to contact with their questions and problems concerning quality reading.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this processing is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network;• Logical security hardening of systems, equipment and network;• Physical protection via secure data centre. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC).</p> <p>Access to EUIPO systems and Databases shall only be accessible with an individual username and password. Pursuant to the security policy at EUIPO, user profiles shall be updated regularly.</p> <p>Access control systems with adjustable permissions are implemented. Only authorized persons (see access rights) have access.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Data protection statement on processing personal data in administrative lists regarding Registry's task allocation:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/a1c07303-afba-494c-9b53-8e0209c73137</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-074
Name of the processing operation	Processing operations of personal data within the framework of the secondment of National Experts to EUIPO - SNE's
Last Updated:	14/05/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	The Head of Staffing, Development and Recognition Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the secondment of national experts to EUIPO (SNE's)</p> <p>SNE's are temporarily on secondment to the EUIPO under agreements for the exchange of staff between the Office and central intellectual property offices/ or any local, regional, national public administration/ or institution/ or any public intergovernmental organisation.</p> <p>Personal data of SNE's is actually processed as follows:</p> <p>Selection phase: EUIPO will open an account to each SNE's employer (e.g.: intellectual property offices) with access to a portal in "SAP SuccessFactors" in the cloud containing the offers on secondment posted by EUIPO.</p> <p>The SNE's employers can upload the candidatures of their employees to the portal and submit them to EUIPO for selection according to the offers on secondment available at EUIPO.</p> <p>Secondment phase: personal data of candidates selected by EUIPO to work at the Office as SNE's will be uploaded to "HR Information Systems" for the managing of their individual rights and obligations by the authorised staff of HRD.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	Any data supplied by the SNE's to EUIPO is processed solely for administrative purposes and for an efficient management of the SNE's rights and obligations in accordance with the Office's decisions ADM 10-10Rev, MB 16-13 and MB 18-14 setting out the rules governing the secondment of SNE's at the Office.
Data Subjects	Non-stutory staff: Seconded National Experts and data related to their relatives and/or persons to contact in case of emergency.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed only on need to know basis and by authorized staff of HRD:</p> <ul style="list-style-type: none">- SNE's full name, photo , CV, educational diplomas, professional experience certificates, personnel number, gender, marital status, date/place of birth, nationality, identity card/passport/NIE, address, email, telephone, work and personal mobile phone, correspondence with the national administration concerning the secondment and the work activity;- SNE's annual reports relating to his/her ability, efficiency and conduct, as well as any comments done by them on such documents .- The bank account number and the notes sent to the Finance Department for the monthly payments of allowances, travel and mission expenses;- Persons to contact in case of emergency: name, mobile phone, address and relation with the SNE, as well as the reference person to contact in the SNE's administration/ institution of origin (Human Resources);- Relatives: full name and birth date of dependent children/ spouse/ partner/ other), as well as data related to schools attended by SNE's dependent children;- The health insurance justification , as well as any other insurance (accident/ death) that can be used in case of emergency;- Data related to working time management/ leave/ absences ;- Any other relevant data supplied by the staff member necessary to manage his/her individual file.
Retention period	<p>For successful candidates: 7 years after the end of the period of service at EUIPO for reasons of budgetary discharge, control and audit purposes.</p> <p>For non-selected candidates: 2 years as from the date of notification on unsuccessful candidates.</p> <p>For data that can be destroyed in a shorter period of time, the EUIPO retention period and schedule for files will be applied.</p>
Recipients of the data	<p>The authorised staff of HRD working on the files. EUIPO's management (Directors/ Heads of Service/ AIPN/ AACC). The Line managers may access the following information of SNE's working in their Services: working time, absences, annual reports and any other data necessary for the management of their staff (CV, skills, competencies, languages and trainings).</p> <p>The Line manager's assistants in charge of resources issues may also be authorised to access the same personal data as their line managers.</p> <p>The Academy (ACA) for the organisation of trainings. The Finance Department (FD) for allowances payments. Only data strictly necessary for the participation in training and/or payments will be provided to ACA and FD.</p> <p>The International Cooperation and Legal Affairs Department (ICLAD) may need to add the name and department of work of the SNE's on the briefings to be sent to the Office's management concerning the framework with the intellectual property National Offices.</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member; line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p> <p>A declaration of confidentiality is signed by the persons having access to the HR database.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing of personal data within the framework of the secondment of National Experts to EUIPO - SNE's:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/974d1372-6a81-4eec-a7d0-5ef5bd4e386a</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-075
Name of the processing operation	Management of backups of data contained in EUIPO systems
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Data Centre Ops team from DTD, backup administrators and operators from IECISA ALTIA for the management of the backups. Data Centre Ops team consists of internal staff members from DTD. IECISA ALTIA is an external service provider for the DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The DTD is in charge of the technical details and procedures ensuring the proper copying and archiving of data from EUIPO systems and implementing the necessary technical security measures to ensure that backed up data is protected. Backup involves daily data duplication from the systems to internal backup servers, weekly copying of that data on tapes, and secure storage of the backup media. Every week all the data of the EUIPO systems is copied to tapes. At the end of each month, a monthly backup of all the data is created and stored.
Purpose of the processing	Back up of data contained in EUIPO systems is performed for the purposes of archiving and preserving the data and making it possible to restore it back to a particular point in the past in case of a data loss event, like data deletion or corruption, hardware failure, malicious hacking, user error or any other unforeseen event.
Data Subjects	Any person whose personal data have been collected and are processed by information systems running on the EUIPO IT Infrastructure, including all statutory staff, service providers, and external users/clients.
Description of categories of persons whose data EUIPO processes and list of data categories	Backups consist of all types of data that is collected, processed and stored by information systems running on the EUIPO IT Infrastructure. They can include data such as: - Login details; first name, last name; company; EUIPO personal number; ID Card number; department, service; administrative address; phone extension; mobile phone; email address; list of user's IT inventory; contract type, card plate number or user location; - Personal data of users (first name, last name, company name, phone number, email address); - Business information (business name; business group; business type); - Information copied from EUIPO back office systems (ID numbers, languages, status of the file, examiners in charge of the file); - Information interaction data (type of interaction- calls, emails, complaints; date and time; number; categorisation; solutions); - Participation in events (event name, event organiser, event date); - System information related to the logs of users' activities on production systems (user name, originating machine, IP address, destination URL, web browsing history, time stamp, browser type, browser language, browser screen size); - Any files stored on user' area of EUIPO computers.
Retention period	The retention period of backups depend on the nature of the information being backed up, though in all cases, the maximum retention period is of one year. A different retention period applies to the Analytical Accounting and Performances Reports that should be 2 years after the year appraisals – according to the decision No. ADM-11-80 – article 11.
Recipients of the data	n.a.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Several security measures are applied throughout the activities involved in the backup management.</p> <ul style="list-style-type: none">• Standard security measures of the EUIPO Information Systems:<ul style="list-style-type: none">- Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed.- Access to the backup system is subject to justified approval based on position and roles.- Authentication and authorization based on roles. The content accessible and the operations available differ depending on roles.- Servers are physically protected at the Data Processing Centre.- Network security configured to prevent external threats from accessing the servers.• Other security measures:<ul style="list-style-type: none">- Backup Data is compressed when stored by the internal backup system. This information is not accessible without a valid username and password to access the backup system.- Data is encrypted before it is copied on removable media.- The removable media are put in secure fire and waterproof cases with tamper-evident security seals.- All persons dealing with personal data in the context of the management of log files, at any stage, shall sign a confidentiality declaration and/or non-disclosure agreement.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the management of backups:</p> <p>http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/500c3bbf-c287-4a23-804f-7528ec102cf9/DPR-2018-075.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-076
Name of the processing operation	Management of personal data in the Business Continuity Plan
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	Digital Transformation Department BCP@euipo.europa.eu
Name and contact details of processor	Data Centre Ops team and BCP Coordinator from DTD Administrators and operators from IECISA ALTIA for the management of the BCP Website. Unisys consultants for BCP coordination tasks. F24 Admins for the management of the BCP members' availability Data Centre Ops team consists of internal staff members from DTD. IECISA ALTIA and Unisys are external service providers for DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	In the framework of the implementation of its Information Security Policies, notably in the context of the ISO 270001 certification, EUIPO has developed a Business Continuity Plan (BCP). The implementation of this BCP implies the setting up and maintenance of levelled Recovery Teams in accordance with potential contingency plans. Recovery Teams are lists of people designated to trigger the recovery strategies and/or prevention measures and to be involved in dealing with a potential contingency. More information on the BCP can be found here: http://insite/digital-transformation-department/business-continuity
Purpose of the processing	Personal data is managed in the context of the BCP as it is necessary to know and reach the staff that will need to trigger the recovery strategies of the Office in the shortest time possible.
Data Subjects	Any staff member that acts as a BCP member.
Description of categories of persons whose data EUIPO processes and list of data categories	The following information is collected in the context of the BCP: - First name - Last name - Level of Recovery Team - Role and availability - Phone number (EUIPO extension) - Mobile number (EUIPO mobile) - Phone number (personal) - Mobile number (personal) - EUIPO Email
Retention period	Information is stored for as long as a staff member is part of the BCP. Once a staff member leaves the BCP, information is removed after two months.
Recipients of the data	N/A
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to the Business Continuity Plan is stored in secure IT applications according to the security standards of EUIPO (Sharedox). These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>Information stored in the BCP Website is protected by the following security measures:</p> <ul style="list-style-type: none">• BCP information stored in the BCP Website is protected by access control measures and requires a valid username and password. No anonymous access allowed.• BCP Website communications are encrypted, to ensure confidentiality of the data exchanged.• BCP Website infrastructure is hosted in Europe, with high physical and logical security measures to prevent unauthorized access or modification of the information.• BCP Website infrastructure service provider does not have access to the information stored in the BCP Website. <p>Information stored in the FACT24 is protected by the following security measures:</p> <ul style="list-style-type: none">• Personal data is stored in the FACT24 tool, protected by access control measures and requires a valid username and password. No anonymous access is allowed.• Data is encrypted while stored and in transit.• FACT24 is hosted exclusively in Germany, in compliance with German data protection laws.• FACT24 systems are protected by continuously updated security measures, such as virus scanners and perimeter security.• Information is only made available within F24 to those that absolutely need the data to fulfil their contractual and legal obligations.• F24 is certified in ISO 27001 for the secure management of information.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Data Protection Statement on the processing of personal data in the context of the Business Continuity Plan (BCP): http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/c337cd8d-58bc-4d2a-8f76-241dd19974b6/Privacy%20Statement%20BCP.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-077
Name of the processing operation	Management of Communication Correspondents Network
Last Updated:	29/03/2019
Controller Organizational entity	Communication
Controller contact details	Controller contact details: Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain. Contact: Head of Communication Service: PersonalDataCS@euipo.europa.eu
Name and contact details of processor	Team leader of Internal Communication, CS Communication correspondents of all EUIPO departments
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In order to ensure that EUIPO staff is duly-informed about all matters/events/news in the Office that affect them, a network of Communication Correspondents has been created as described in details in the QSD-0099 - MANUAL Communication Activities. The Communication Correspondents Network (CCN) is composed of representatives of each EUIPO department who:</p> <ul style="list-style-type: none">• assist the CS to gather and disseminate information across EUIPO, and provide feedback on communication issues;• Improve internal communication in their department through various communications activities and actions like the sharing of information through different communication channels (TV monitors and emails). <p>With regard to the work of the CCN, personal data is processed within the following data bases:</p> <ul style="list-style-type: none">• Data base of all Communication Correspondents;• Data bases of communication material (photos, videos, testimonials of the staff) of each department which is managed by the corresponding CC;
Purpose of the processing	<p>In the Data base of all Communication Correspondents the personal data are processed for the purpose of ensuring the normal functioning and management of the activities of the CCN and the easy communication and coordination between the Correspondents.</p> <p>In the Data bases of communication material managed by each department's Communication Correspondent, personal data are processed for the purpose of engagement of staff in the Office activities and in order to ensure that EUIPO staff is duly informed about all news and events that take place in the Office.</p>
Data Subjects	EUIPO Communication Correspondents members of each department.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>In the data base of all Communication Correspondents, the personal data processed are as follows: name, surname and mail address.</p> <p>In the data bases of communication material managed by each department's CC, the personal data processed are as follows: photos, videos, testimonials of the staff of the department.</p>



Retention period	<p>The retention period of the personal data in the data base of the CCN is the period for which the person performs the role of a CC.</p> <p>The retention period of the personal data stored in the data bases of the communication material in each department is as follows:</p> <ul style="list-style-type: none">• 6 months for photos• 3 years for videos;• 15 days for communication material stored on Brightsign server. <p>For some of the data with historical value (videos where top management participates) the personal data can be stored for a longer period. Being this period based on the retention criteria for multimedia content of events concerning the communication service annexed to this notification.</p>
Recipients of the data	EUIPO staff
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Informations stored in Sharedox and on Brightsign are protected by the standard security measures of the EUIPO Information Systems:</p> <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed.• Access to the system is subject to justified approval based on position and roles.• Authentication and authorization based on roles. The content accessible and the operations available differ depending on roles.• Servers are physically protected at the Data Processing Centre. <p>Network security configured to prevent external threats from accessing the servers.</p> <ul style="list-style-type: none">•
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement Communication Correspondents:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/bdbf8027-dd13-438c-a5f6-eec1d332a24f</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-078
Name of the processing operation	PER. Persons Module
Last Updated:	20/07/2020
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	PER (Persons Module) is the EUIPO database of the OAMISIS Production system allowing examiners to manage Representatives, Owners and Dossiers (RCD applications and Appeals) information.
Purpose of the processing	The collection, storage and processing of such data shall serve the purposes of: (a) administering the applications and/or registrations (EUTM/RCD) as described in this Regulation and in acts adopted pursuant to it; (b) accessing the information necessary for conducting the relevant proceedings (examination, opposition, cancellation, RCD invalidity, recordals, appeals, PUB and MPS) more easily and efficiently; (c) communicating with the applicants and other parties to the proceedings (ex parte & inter parte); (d) producing reports and statistics enabling the Office to optimise its operations and improve the functioning of the system (as foreseen in Article 6(1) of Decision No EX-14-3 of The President of OHIM) and Article 112(2) EUTMR.
Data Subjects	Individuals whose data have been entered as EUTM/RCD particulars, Oppositions, Cancellations, RCD invalidities, Recordals and Appeals, as well as Owners, Holders, Applicants and Representatives.



Description of categories of persons whose data EUIPO processes and list of data categories

With regard to persons information, the service supplies the following data if available with regard to a particular Owner/Applicant/Liquidator or Representative as well as regard to RCD applications and Appeals:

- Representative:



Retention period	Indefinite (for reasons of legal certainty), as foreseen by Article 111(9) EUTMR and Article 7(1) of the Decision No EX-14-3 of the President of the OHIM.
Recipients of the data	Individuals or public and private entities (data is considered to be of public interest and may be accessed by any third party as stated in Article 111(9) EUTMR and Article 8(1) of the Decision No EX-14-3 of The President of the OHIM. All EUIPO staff and external provider of mail services has view access to the PER Module; examiners in charge of “owners and representatives” data have edit rights. The parties to the procedures of the EUIPO and any third parties have access through eSearch on the EUIPO website to the information stored in the database.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	To WIPO, for the International Applications only. The EUIPO acts as the office of origin whenever an international application is based on an EU trade mark. The EUIPO's transfers to WIPO all the data related to the International Applications in a weekly (daily) extract from EUIPO's systems in the form of XXX file. In terms of personal data, the extract includes the following particulars: Owner/Applicant or Representative - Representative :



General Description of security measures	<p>The management of access and right is done at ADM level. Examiners need to authenticate against ADM to enter the application. Moreover each examiner is assigned some ADM profiles and each profile is given some rights in the application. Each user is provided a username and password which gives access to certain features (in order to access the EUIPO systems and databases). The basic permissions in PER allows to see the details but additional permissions are needed to update the data and/or link/unlink this owner/representative to dossiers.</p> <ul style="list-style-type: none">• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers. <p>The information is also available directly in the database. The access to the database is restricted to some DTD staff internal and external. Confidentiality and data protection clauses are signed-off by the service provider.</p> <p>All the standard security measures available for EUIPO's databases. The Office's server has been certified by an international certifying authority (Verisign Inc.), which guarantees that users have in fact connected to the Office. All information transmitted via the internet is encrypted using SSL protocol.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement PERSONS module:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3442f513-28f1-4d14-8271-e000da1b3788</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-079
Name of the processing operation	Processing personal data within the framework of the Mentoring Programme.
Last Updated:	08/04/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Staffing, Development and Recognition Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing of data within the framework of the EUIPO Mentoring programme consists of :</p> <ul style="list-style-type: none">- buddy mentoring, each department identifies volunteer buddy mentors through either call for interest or any other way suitable for the unit. Mentors are subsequently assigned to each newcomer by the respective department Director. The population of newcomers also includes staff taking up duties in another department as a result of internal mobility or reassignment.- leadership mentoring, a pool of volunteer managers (mentors) is made available for mentees with the coordination of the Human Resources Department (HRD). A call for interest for team leaders (mentees) is published on Insite. The list of interested mentees is filtered by the HRD according to the criteria published in the call. The matching mentor-mentee is coordinated by the responsible HR staff for the mentoring programme. <p>In case that a mentorship relation does not work for either party, the mentor assigned to the mentee may change upon request of either of the parties by providing a justification (verbally or in writing) to the responsible staff for the programme in the department (buddy mentoring) or in HRD (leadership mentoring). The justification may contain statements and opinions about the effectiveness of the mentorship relation.</p> <p>Mentors and mentees are bound to keep the information shared between them confidential.</p> <p>HRD collects feedback from the parties involved. Feedback sought will refer to:</p> <ul style="list-style-type: none">- time spent in mentoring related activities (meetings, and preparation and follow up work);- recommendations for improving the mentoring programme;- added value of the programme for the mentee/mentor. <p>The time of the mentors dedicated to this activity will be recognised in the appraisal exercise.</p> <p>The mentoring programme will be offered to all statutory staff members and seconded national experts.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>



Purpose of the processing	<p>The processing of data is based on the specific note on the mentoring programme approved by the Executive Director on 30/05/2018 which establishes the main aspects of this activity.</p> <p>The EUIPO mentoring programme consists of two schemes and their purposes are the following:</p> <ol style="list-style-type: none">1. Buddy mentoring for newcomers: Provide support to newcomers for a smoother and more effective integration into the Office and in Alicante; and2. Leadership mentoring for team leaders: Provide interested team leaders with support for the development of their leadership skills. <p>The mentoring programme is offered to EUIPO's statutory staff members and seconded national experts.</p>
Data Subjects	<p>Statutory staff members: (officials, temporary and contract agents)</p> <p>Seconded National Experts: SNE's</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data for mentors and mentees is processed only on need to know basis and will be accessed by authorised staff of HRD and of the respective Departments:</p> <ul style="list-style-type: none">- staff member full name, personnel number, email, telephone;- department/service, function group, grade, seniority in grade. <p>Moreover for the 'leadership mentoring' programme the following data will be processed:</p> <ul style="list-style-type: none">- for mentees: curriculum vitae or talent profile and motivation letter (this information will also be shared with the respective mentors);- for mentors: a brief summary of their profile ("bio") (this information will also be shared with the mentees). <p>The feedback collected by HRD from the parties involved will include all the above mentioned data and the following:</p> <ul style="list-style-type: none">- time spent in mentoring related activities (meetings, and preparation and follow up work);- recommendations for improving the mentoring programme;- added value of the programme for the mentee/mentor.
Retention period	<p>All personal data provided by staff in the context of this procedure will be retained for 7 years.</p> <p>In case of complaint, all documents are kept until a final decision on it has been taken.</p>
Recipients of the data	<p>Data are accessible to HRD staff working on the mentoring programme, the respective mentors, authorised staff of the Departments concerned and the Cabinet (for the 'leadership mentoring').</p> <p>Data available to all EUIPO staff:</p> <ul style="list-style-type: none">- List of volunteer mentors for both mentoring schemes. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Paper documents are kept in secured cupboards by authorised staff of HRD. Electronic data are stored in Sharedox / HR "Allegro" database and its modules (stored in MySQL database).</p> <p>HRD is working on the new HR database "SAP SuccessFactors" in the cloud. Data will be transferred from HR portal modules (HR database Allegro) to the new HR database "SAP SuccessFactors".</p> <p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director or IT-technician. The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the framework of the Mentoring programme:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/9458849d-206d-404d-9a48-38f7d8b0a65d</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-080
Name of the processing operation	Publication of a list containing personal data referring to specific decisions concerning the administrative status of statutory staff (officials, temporary and contract agents) - Article 25 of the SR and Articles 11 and 81 of the CEOS
Last Updated:	12/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing of data consists of making available in MyPortal "SAP SuccessFactors" personal data referring to the following specific decisions concerning the administrative status of EUIPO's officials, temporary agents and contract agents:</p> <ul style="list-style-type: none">- Entry into service (appointments and transfers for Officials and new contracts for Temporary and Contract agents);- Assignment / Reassignment of service according to an internal mobility procedure or in the interest of the service;- Change of place of employment;- Contract renewals (first and second renewal);- Secondment to another institution/body;- Termination of service. <p>The list will be published, once, every quarter and will be accessible only to EUIPO's statutory staff . Promotions/reclassification of staff and appointment of managers are made available to all statutory staff by their publication on Insite. Data regarding administrative decisions affecting the working conditions of EUIPO's statutory staff members (for ex CCP, unpaid leave, parental and maternity leave) will not be included in this list.</p>
Purpose of the processing	The processing of data is necessary for the performance and the support of tasks carried out by EUIPO as mandated by the Staff Regulations (SR) and the Conditions of Employment of Other Servants of the European Union (CEOS) and more specifically Article 25 of the SR and Articles 11 and 81 of the CEOS.
Data Subjects	EUIPO's statutory staff members (officials, temporary and contract agents)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data processed by HRD will be uploaded to the list published in "My Portal - SAP SuccessFactors":</p> <ul style="list-style-type: none">- Entry into service (including appointments/ transfers of officials, new contracts for Temporary and Contract Agents): full name, statutory link, grade/ function group, assignment (department) and entry date;- Reassignment: full name, statutory link, grade / function group, reason (by internal mobility /or in the interest of the service), former / new department and date;- Change of place of employment: full name, statutory link , grade / function group, reassignment (department), new place of employment and date;- Contract Renewals : full name, statutory link, starting date of the first and second contract renewal;- Secondment: full name, statutory link, grade /function group, Institution or body of destination;- Termination of service: full name, statutory link, grade /function group, last assignment (department) and date (the reason of termination of service will not be published).
Retention period	<p>The publication will be done once, every quarter, and the list will remain published in MyPortal and stored in ShareDox for a period of time of 3 months until the publication of the new updated list.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The staff of Human Resources Department working with the HR “Allegro” database. The data will be extracted from the existing HR “Allegro database” and “SAP SuccessFactors” in the cloud to be uploaded to the list published in MyPortal. This list will be accessible only to EUIPO’s statutory staff members.</p> <p>Furthermore, EUIPO’s contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR “Allegro” database and “SAP SuccessFactors” in the cloud under request and supervision of EUIPO .</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data is stored in secure IT applications (ShareDOX, HR “Allegro” database and “SAP SuccessFactors”) according to the security standards of EUIPO.</p> <p>Appropriate levels of access are granted individually only to the above recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein. Replacing users is strictly prohibited.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. “SAP SuccessFactors” is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the publication of a list specific decisions concerning the administrative status of statutory staff: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/e4e3d43b-c808-407c-9108-b6816d82de1f</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-082
Name of the processing operation	Management of faxes
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Opentext: DTD external service provider for the management of Faxes.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Opentext is a cloud-based system that will be used for sending and receiving fax in the Office, including the faxes received for the filing of trademarks and designs. As this is a service available to clients, it has high availability requirements. This means it is important to have the system available, even if the event of an incident disabling EUIPO's IT infrastructure.
Purpose of the processing	Opentext requires personal data to have a log of faxes sent and received, for billing purposes.
Data Subjects	Any person that sends or receives a fax from EUIPO
Description of categories of persons whose data EUIPO processes and list of data categories	The information collected by Opentext is the minimum required for billing purposes: - Telephone number that sent the fax; - Telephone number that received the fax; - Fax name and timestamp of the call (Metadata associated with the phone number). It must be noted that the document that is being transmitted via fax is only temporarily stored in encrypted form while in transit and is not accessible to anyone.
Retention period	Personal data as described above is kept for as long as there is a contractual relationship, for billing purposes. Opentext is in the process of implementing a records management policy to include stricter retention periods for inactive information, but at the time of this notification, it has not yet been implemented.
Recipients of the data	N/A
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO



If so, to which ones and with which safeguards?	<ul style="list-style-type: none">• Opentext uses multiple automated backup systems for performing regularly scheduled backups of production systems and data. The periodicity is daily incremental, and weekly full backups.• OpenText personnel perform quarterly backup restoration tests.• OpenText has implemented access control mechanisms to prevent unauthorized access:<ul style="list-style-type: none">o Username and Password, in a network domaino Secure password composition ruleso Access restrictions based on roles• Opentext uses system and network hardware with built-in redundancy, to minimize the possibility of incidents related to unavailability: server clustering, Load balancing, multiple telecom carriers and Internet Service providers.• Opentext has implemented real-time monitoring, focused on availability, processing performance, capacity management and incident response. In addition, access to the information is managed through an Access Request and Access Revocation process, to ensure that information is accessible only to those who require it.• Opentext encrypts information while at rest and in transit.• Opentext is certified in SOC 2.• Virtustream, the company that owns the UK datacentre, is also SOC 2 certified.
General Description of security measures	<p>Security measures implemented by Opentext are the following:</p> <ul style="list-style-type: none">• Opentext uses multiple automated backup systems for performing regularly scheduled backups of production systems and data. The periodicity is daily incremental, and weekly full backups.• OpenText personnel perform quarterly backup restoration tests.• OpenText has implemented access control mechanisms to prevent unauthorized access:<ul style="list-style-type: none">o Username and Password, in a network domaino Secure password composition ruleso Access restrictions based on roles• Opentext uses system and network hardware with built-in redundancy, to minimize the possibility of incidents related to unavailability: server clustering, Load balancing, multiple telecom carriers and Internet Service providers.• Opentext has implemented real-time monitoring, focused on availability, processing performance, capacity management and incident response. In addition, access to the information is managed through an Access Request and Access Revocation process, to ensure that information is accessible only to those who require it.• Opentext encrypts information while at rest and in transit.• Opentext is certified in SOC 2.• Virtustream, the company that owns the UK datacentre, is also SOC 2 certified.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the management of personal data related to faxes: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/Management_personal_data_related_faxes_es.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-086
Name of the processing operation	General Media and Broadcaster contact details
Last Updated:	29/03/2019
Controller Organizational entity	Communication
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain. Contact: Head of Communication Service: PersonalDataCS@euipo.europa.eu
Name and contact details of processor	Editorial Team
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Collection of Data for the purpose of Media content
Purpose of the processing	We process this data to provide media with content about the Office that they request. This can take the form of press releases linked to Office outputs (in the context of LoA 6 of SP2020) or individual requests from journalists based on I-related stories they are covering themselves.
Data Subjects	Media professionals
Description of categories of persons whose data EUIPO processes and list of data categories	This data consists of contact names, email addresses and sometimes phone numbers of journalists across the EU and beyond. The data is organised per category, with each category corresponding to the media sector to which a particular journalist belongs. Specifically, we collect the following personal data: Name of journalist/media professional Email of journalist/media professional Telephone number of journalist/media professional Name of media Category division Role of the journalist/media professional
Retention period	Personal data will be kept for as long as the journalist/media professional is active and of interest to EUIPO
Recipients of the data	No
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	Information stored in ShareDOX is protected by the standard security measures of the EUIPO Information Systems: <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed.• Access to the system is subject to justified approval based on position and roles.• Authentication and authorization based on roles. The content accessible and the operations available differ depending on roles.• Servers are physically protected at the Data Processing Centre.• Network security configured to prevent external threats from accessing the servers.• The processing of this information will be both manual and automated
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	GENERAL MEDIA CONTACTS PRIVACY STATEMENT.: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/5dce34c6-61b2-463d-90a1-c6fb6c1181dc
EDPS Prior consultation	NO



Reference number	DPR-2018-087
Name of the processing operation	Processing of personal data on Missions
Last Updated:	21/02/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing personal data of EUIPO's staff members going on mission or of the persons carrying out the authorized travel. They may be officials, temporary and contract agents, Seconded National Experts (SNE's) and trainees.</p> <p>The data processed are related to the estimation of costs, liquidation of expenses, insurance coverage, priority pass to the airport lounges and statistics.</p> <p>Before leaving on mission, the persons concerned have to complete the event participation form and receive the approval to travel on mission from the International Cooperation and Legal Affairs Department (ICLAD) . Oral hearings do not need event approval.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The processing of personal data is necessary for the management of missions by the Human Resources Department (HRD) in compliance with the Staff Regulations (SR), Conditions of Employment of Other Agents (CEOS) and the Guide of Missions:</p> <ul style="list-style-type: none">- Article 71 of the SR, Articles 11 to 13a of Annex VII of the SR;- Articles 22 and 92 of the CEOS;- Guide of Missions C (2017)5323 of 27/09/2017;- Article 19 of Decision ADM N°10-10Rev of 08/09/2011 (SNE);- Decision MB 16-13 of 31/05/2016 (SNE).
Data Subjects	Staff members (officials, temporary and contract agents, Seconded National Experts (SNE's) and trainees
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <p>Name and surname of the person travelling on mission, personal number, Department/Service of assignment, email, telephone, location of the mission, working dates, purpose of the mission, passport /or NIE references, bank account number, invoices related to the reimbursement of travel tickets, accommodation, transport used, certificate of attendance for external training, Priority Pass used /or not at airport lounge (name of invited guests and indication of professional reasons), name of third party paying the mission, combination of the mission with annual leave/bank holiday or weekend.</p>



Retention period	<p>Data related to the liquidation of mission expenses, payments to the Travel Agency, Insurance and Priority Pass is kept during 7 years for budgetary discharge by the Court of Auditors, control and audit purposes.</p> <p>The Priority Pass is immediately destroyed and /or deactivated by the end of service of the person concerned /or if the person concerned no longer fulfils the conditions to receive a card.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p> <p>Data related to statistics / historical purposes is archived during 7 years.</p>
Recipients of the data	<p>The personal data is accessible to:</p> <p>The person travelling on mission, his/her assistants under authorisation, the Line Managers and staff authorised by them, the authorised staff of the Institutional Relations Service of the ICLAD (external events) or of the Academy (external training), the Authorizing Officer by Sub-Delegation, a limited number of authorized staff of HRD and FD (reimbursement of mission expenses).</p> <p>The Travel Agency/ Insurance Company/ Priority Pass Group and the Mail room uploading in "SAP workflow" the reimbursement of travel expenses to travellers.</p> <p>In case of emergency, EUIPO will use the "Tripcare Service 24h / 7" proposed by the Travel Agency to obtain information concerning staff members on mission (name/surname, destinations, departure/return dates, nr. of traveling days, flight number/company, email address and mobile telephone at work /or personal). These data are kept by the travel agency on the EUIPO's traveller's profile tool and can be accessible through the "Tripcare emergency tool 24h/7 in order to evaluate the situation and propose the best alternatives to the traveller.</p> <p>Only on a strict need to know basis and in case of emergency, a limited number of EUIPO's staff working in the following Departments/ Services has access to the "Tripcare emergency service 24h/7": HRD/ Mission's Office/ Cabinet/ Infrastructures and Buildings Department (IBD)Security Service).</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database. under request and supervision of EUIPO .</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>All personal data are stored in secure IT applications (ShareDox, Outlook /SAP Finances HR "Allegro" database. according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in the files.</p> <p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director or IT-technician. The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU. Data will be processed and stored only in EU.</p> <p>The following external providers processing data related to missions within the framework of the contract with EUIPO are made aware of data protection rules through the General Terms and Conditions applicable to supply services/ works Contracts with EUIPO: Travel Agency/ Missions' Insurance/ Priority Pass Group and Mail Room.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on processing personal data within the framework of Missions for EUIPO's staff members.: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/25d3fd62-dd3f-443f-a2fc-1cfdeb38b199</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2018-089
Name of the processing operation	Coordination of The Communication Correspondents' Network (CoCoNet)
Last Updated:	29/03/2019
Controller Organizational entity	Communication
Controller contact details	Head of Communication Service: PersonalDataCS@euiipo.europa.eu EUIPO, Avenida de Europa 4, 03008 Alicante, Spain.
Name and contact details of processor	CoCoNet Team : Communication Service/IBD/POMILIO BLUMM
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The Communication Correspondents' Network (CoCoNet) is a European network of communication correspondents, established in 2013. The network includes representatives from the field of communication of each National Office (NO). At the beginning of 2016, the EPO, which had previously participated in the CoCoNet as an observer, confirmed its interest in becoming a full member of the network. The EPO also proposed expanding the CoCoNet to include its partner IP offices which either be European patent offices or non-European IP Offices. The network expanded with the European Patent Office (EPO) becoming a full member, along with the IP Offices from non-EU members of the European Patent Office. In 2018 the EUIPO and EPO actively worked together with 40 IP Offices, 31 EU and 9 non-EU partners.</p> <p>EUIPO and EPO signed in 2011 a Memorandum of Understanding (see Annexx)</p> <p>Objectives of the network are:</p> <ul style="list-style-type: none">• Increase common working.• Foster cooperation to rise awarness and promote the IP system.• Share best practices (campaign ideas, promotional materials, videos...etc.)• Exchange ideas and learn about social media (tools, practices...etc.)• Exchange ideas and learn about media relations (use of tools, communicating jointly...etc.)• Strengthen relations and create synergies (tailor messages, reach target audience more effectively) <p>Members of the network meet twice a year during annual meetings and trainings. Annual meetings are focused on cooperation with managerial staff. They provide a continuous dialogue among the members of the network and update the objectives to be achieved. They also allow the exchange of ideas and concerns, as well as coordination of actions to be implemented.</p> <p>The trainings are intended to other colleagues in the national and regional IP Offices who work in communications and public awareness areas (also CoCoNet members). The aim of the sessions is to provide them with practical trainings in the field of communication.</p> <p>Each year EUIPO (with the support of IBD or POMILIO BLUMM) organize one of those cyclical events, the costs of the second one are covered by EPO.</p> <p>In the framework of the network EUIPO actively disseminate the Observatory studies and create joint pan-European media campaigns. Related to the campaigns, EUIPO also work on introducing common indicators for the IP Offices that they can use when sending feedback on their disseminations. In addition, the members of the network receive monthly correspondence email regarding upcoming activities of CoCoNet, EUIPO and EPO and NOs news.</p> <p>In addition, the cooperation actions seek to promote the industrial property system by encoragin and supportinf the development of innovation strategiesand raising awarness about the importance of the syste through the dessiminaion of inofromation regarding IP.</p>
Purpose of the processing	<p>The personal data are collected to coordinate: monthly correspondence mailing, distribution of invitations and agendas of upcoming events, registration for the events, dissemination of news related to network, EUIPO or EPO activities, OBS studies, joint actions and campaigns, joint developments of educationa and awareness-raising promotional initiatives,conducting studies ans specific consultation regarding relevnat matters to both Institution, etc.</p>
Data Subjects	<p>Members of the network</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Personal data: name, surname, office name, job position, Email address, landline phone, mobile phone.</p>



Retention period	<p>As long as the person is a member of the network.</p> <p>Participation in the network is open to representatives from the field of communication of EU and non-EU National IP Offices. Representative becomes a member of the network based on the formal exchange of the emails between EUIPO and NO. Member may resign from participation in the network on the basis of an e-mail exchange.</p>
Recipients of the data	<p>Observatory – sometimes OBS uses data base to distribute the invitation for their events (for instance: Ideas Powered Youth Event).</p> <p>EPO – EPO uses our contact lists to distribute the invitation to upcoming CoCoNet meetings and to pass all organizational information.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Information stored in Sharedox and in the TMDN.org folder is protected by the standard security measures of EUIPO Information Systems:</p> <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password.• Access to the system is subject to justify approval based on position and roles.• Servers are physically protected at the Data Processing Centre.• Network security configured to prevent external threats from accessing the servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>CoCoNet Privacy Statement FINAL:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3bded1d9-4516-4e26-9c3a-7b24fbf78946</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-090
Name of the processing operation	Processing of personal data in the area of Staff Evaluation
Last Updated:	12/07/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	The Head of Staffing, Development and Recognition Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The overall assessment of EUIPO's staff member's work covers the evaluation of his/her efficiency, aspects of conduct in the service and competencies to perform his/her duties, including the quality of the work.</p> <p>If the jobholder's overall performance assessment does not correspond to the level required for the post occupied, a Personalised Support Plan (PSP) for the improvement of professional performance is prepared by the reporting officer together with the concerned jobholder and is attached to the appraisal form of the next appraisal period. The PSP will include the list of improvements needed and actions to be taken by the jobholder in order to bring performance to a satisfactory level. The actions taken by the reporting officer/Office in order to support and monitor the performance improvement of the jobholder will also be specified in the PSP. All the information afore mentioned will be discussed in advance between the reporting officer and the jobholder. A Mid-year review will take place to monitor progress of the PSP and, if necessary, more frequent reviews can be held quarterly or monthly.</p> <p>The processing operation is also necessary for blocking the advancement in step if the last finalised report concluded that performance was unsatisfactory.</p> <p>For new recruited staff members a probationary report is established in order to assessing the ability of the probationer to perform the duties pertaining to his/her post and also on his/her efficiency and conduct in the service.</p> <p>For officials appointed in management positions an assessment is made of his/her performance during the first nine months following his/her appointment.</p> <p>The performance evaluation of the jobholders is used for the contract renewal of temporary and contract agents at the Office.</p> <p>A proposal of work evaluation is established for the Seconded National Experts (SNEs) with the same periodicity as for the staff members.</p> <p>The performance data collected and stored by the IT tool monitoring individual production, task allocation and timeliness will be used as one of the assessment elements of the data subject concerned, as well as of the respective management responsible. The information collected will be compared with established reference numbers in proportion of the time allocated to the task and established procedures for the appraisal.</p> <p>If during the reporting period of the appraisal exercise the jobholder dedicated a significant period of time to the activities such as:</p> <ul style="list-style-type: none">- participation in knowledge circles;- participation in projects;- temporary assignment to another service or department (not related to mobility);- duties carried out in a service to which he/she was not formally assigned, including participation in calls for talent;- secondment in the interest of the service within or outside the Office, for less than 4 months;- participation at conferences or courses in the framework of the Academy <p>and these activities form part of the jobholder's objectives, the reporting officer must consult the staff member's to whom the jobholder was reporting for these activities (leaders of knowledge circles / project managers / the Academy) for the relevant period to gather input on the performance of the jobholder. Consultation is done with a specific compulsory input form.</p>



Purpose of the processing	<p>The purpose of the periodical appraisal report is to assess the work carried out by the staff members during the annual appraisal period, in particular their ability, efficiency and conduct in the service, in compliance with Article 43 of the Staff Regulations (SR), Articles 15, par. 2 and 87 of the Conditions of Employment of Other Servants (CEOS).</p> <p>A Personalised Support Plan (PSP) for the improvement of the jobholder's professional performance will be established in case that his/her work assessment does not correspond to the level required for the post occupied.</p> <p>The appraisal report is used to block the advancement in step in line with Article 44 of SR and Articles 20 and 92 of CEOS or in case that the appointing authority decides to downgrade/dismiss the official having considered that he/she did not show any progress in his/her professional competence in accordance with Article 51(1) (a) of the SR.</p> <p>The evaluation on the work of SNE's is done with the same periodicity as for EUIPO's staff members with the purpose to contribute to the appraisal conducted by their by their employer .</p> <p>The probationary report for new recruited staff is done with the purpose of assessing the ability of the probationer to perform the duties pertaining to his/her post and also on his/her efficiency and conduct in the service, in compliance with Article 34 of the SR and Articles 14 and 84 of the CEOS.</p> <p>For officials appointed in management positions an assessment is made of his/her performance within the meaning of Article 43 during the first nine months following his/her appointment aiming to confirm the adequacy of the management competences for the purpose of advancing to the next step in grade according to Article 44 of the SR.</p> <p>The performance evaluation of the data subject is also used for the purpose of contract renewal in accordance with the Guidelines for the renewal of temporary and contract agents at the Office, in particular the evaluations on efficiency, conduct in the service and the abilities of the jobholder through the duration of the contract</p>
Data Subjects	<p>Staff members (officials, temporary and contract agents)/ staff members on probationary period / Seconded National Experts of EUIPO).</p> <p>Reporting officers: as far as it concerns their assessment and comments when completing the Evaluation/ PSP concerning the jobholder.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>The following data is processed:</p> <ul style="list-style-type: none">- employee self-assessment, work objectives (what was to be accomplished) and related actions, success criteria or key performance indicators (KPI), as well as data collected and stored by the IT tool concerning individual production, task allocation and timeliness as compared to the reference numbers (in proportion of the time allocated to the respective task) and timeliness established in the data subject objectives;- description of competencies including conduct in the service, languages level, efficiency, quality of work, mid-year review, reporting officer's general assessment and comments, potential to assume another function or other duties, trainings, countersigning officer's assessment in case of unsatisfactory performance, appeals assessor's comments and the jobholder's comments;- Personalised Support Plan for the jobholder in case of unsatisfactory performance (list of improvements of the professional performance and actions to be taken by the person concerned). List of actions to be taken by the reporting officer in order to monitor and support the performance improvement of the jobholder. The results of the PSP will be reflected in the Mid-year review and, if the case, in more frequent reviews held quarterly or monthly. All data (assessment and comments) included in the PSP will be processed to state the improvements done by the jobholder.- input on the performance of the jobholder for other activities and contribution of the former reporting officer to the appraisal report ;- the ad hoc Group's contribution to the appraisal report or its opinion, and the comments of the Chair of the ad hoc group in case of appeal ;- the probationary report also includes the conclusive assessment of the probationary period and the recommendation on confirmation / extension / termination of the appointment of the employee. If applicable, the report of the work done by staff members in Training Units during their probationary period is taken in account for the conclusive assessment.
<p>Retention period</p>	<p>Annual appraisals / probationary reports and Personalised Support Plans:</p> <p>Electronic word files used for the drafting of the individual reports (stored on the individual PCs of the reporting officers until the reports are deemed final) will be deleted by the reporting officers at the conclusion of the annual appraisal exercise or probationary report.</p> <p>The final report, including the PSP (completed and signed) is stored in the personal file (Allegro/Alfresco/Sharedox/Open text personal file repository) in accordance with Article 26 of the Staff Regulations and kept during the same period of retention as for the personal files.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The staff of Human Resources Department in charge of Appraisal-Evaluation procedures, the Management and authorized staff of the EUIPO's Departments.</p> <p>Reporting officers: as far as it concerns their assessment and comments when completing the Evaluation/ PSP concerning the jobholder.</p> <p>The employers SNE's (National IP Offices - authorized staff of HR).</p> <p>The authorised staff working in HRD, Financial Office (FD) and PMO will be informed if a staff member has been evaluated as unsatisfactory in order to block the advancement of step/downgrade or dismiss, as well as for renewal of contracts (only the strict necessary information is disclosed).</p> <p>The Joint Reports Committee consulted by the AA if the probationary report recommends dismissal or extension of the probationary period.</p> <p>The Management Committee, the Joint Committee, and the authorized staff working in HRD for Certification and promotion procedure purposes.</p> <p>The Joint Promotion and Reclassification Committee and the delegation of the Staff Committee for promotion procedure purposes.</p> <p>Third persons to whom the data subject (statutory staff and SNE's) can send his/her appraisal/ evaluation/ report on the work done at EUIPO (e.g.: candidature to a job - references). The report on the work done by trainees at EUIPO can also be sent by the trainees concerned to third persons.</p> <p>Data stored in HR "Allegro" database may be accessible to external contractors/ subcontractors, namely Adequasys (France). They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting the HR "Allegro" database and integrations with SAP BPC and Business Object systems. Data may also be accessible to Sopra Esteria (Spain) for the maintenance of integrations with Insite, AEOS and SuccessFactors IT systems.</p> <p>Data may also be accessible by external contractors/subcontractors, namely SAP, IECISA and EVERIS. They receive and process the data in the context of the contract with EUIPO for the maintenance and development of the applications supporting "SAP SuccessFactors" and the integrations of SuccessFactors with Remedy and Insite.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to Appraisals/Evaluation of staff members is stored in secure IT applications according to the security standards of EUIPO.</p> <p>The Human Resources database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data within the framework of Appraisals-Evaluation of EUIPO's staff members: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/df1eac4b-f523-4152-8d83-20a29ca49d8a
EDPS Prior consultation	NO



Reference number	DPR-2018-091
Name of the processing operation	Activities during school holidays for dependent children of EUIPO's statutory staff members - Farm school.
Last Updated:	25/04/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service - HRD - Center of Activities (framework of the agreement between Granja Escuela Laloma S.L. and EUIPO)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of personal data within the framework of activities for dependent children of EUIPO's staff members – Farm school during school holidays In the framework of the EUIPO's social policy, the Office organizes outdoor activities during the European School holidays for EUIPO's staff children who are between 3 and 12 years old. The staff members concerned shall send to Human Resources Department (HRD) the proof of payment for the enrolment of their children in the outdoors activities. The inscription and medical form requested by the Centre of activities shall be sent to the Centre directly by the staff member concerned. The processing of personal data is not intended to be used for any automated decision making, including profiling.
Purpose of the processing	The processing of personal data is necessary to establish the enrolment lists and to assess the admissibility of the applications in accordance with the rules laid down in the contract established between the EUIPO and the Centre entrusted to the outdoor activities. The personal data are collected and processed in accordance with: - Article 1e of Staff Regulations - Articles 10 and 80 of the Conditions of Employment of Other Servants.
Data Subjects	Internal Staff: officials, temporary agents and contract agents EUIPO's statutory staff members dependent children
Description of categories of persons whose data EUIPO processes and list of data categories	The following personal data are processed only on a need to know basis: - Full name and age of the children concerned; - Full name of staff member concerned (children's father/mother); - Amount paid and proof of payment; - Dates of participation at the activities.
Retention period	Data related to payments are kept during a period of 7 years for reasons of budgetary discharge, control and audit purposes. Since these activities are recurring, the list of children and parents is continuously kept up to date. Data will be deleted in a period of maximum 3 months from the moment the staff member leaves the Office, the 12th birthday of the child and the last event in which the child participated. In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.



Recipients of the data	<p>Data are disclosed to a limited number of authorized staff of HRD working in these files. The Finance Department (Vendor) only receives from HRD the confirmation of the number of children who participated in the outdoors activities.</p> <p>Data can also be disclosed to the Appointing Authority (AA)/ Authority Authorized to Conclude Contracts (AACC) and the Social Assistant (HRD).</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Personal data are stored in secure IT applications (Sharedox, Outlook, HR "Allegro" database and "SAP SuccessFactors") according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in these files.</p> <p>Appropriate levels of access are granted individually only to the above recipients. The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on Processing personal data within the framework of activities during school holidays for dependent children :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/66598055-b997-4d9a-8b7f-fd09e61f8d56</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-092
Name of the processing operation	Organisation of meetings and events by Communication Service
Last Updated:	21/01/2020
Controller Organizational entity	Communication
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain. Contact: Head of Communication Service: PersonalDataCS@euipo.europa.eu
Name and contact details of processor	Internal processors: Communication service and Common services/ IBD DPN-2019-007 in EUIPO External processors: Event management provider of IBD Pomilio DPR-2019-007 Deloitte
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	When organising meetings and events CS always uses the logistic support of the event management provider of IBD, as described in IBD DPR-2019-007 The only aspect in the organisation of an event by CS that is not done through the support of the events management provider of IBD is the invitation of participants for events/meetings such as: events with key stakeholders (New year cocktail with the authorities, EUIPO Impact study, Schools, etc.), for competition events (Micro story, IP Identical, etc.), others specific events like Design Europa Award. Some of those events may have their own records due to their specificity. When responsible for the invitations, CS will: <ul style="list-style-type: none">• invite the participants through the use of Outlook or Getresponse application (as described in the DPR-2018-058 GetResponse Record);• store in Sharedox the lists of participants and sometimes (when invitation is done through Getresponse) the reports with participation details (who have been invited, who have accepted, who have participated)
Purpose of the processing	CS processes personal data in the process of the organisation of events and meetings for the purposes of the successful management, coordination, accounting and follow-up of the events/meetings.
Data Subjects	EUIPO staff and externals, general public participant or potential participants in the events of managing for CS of EUIPO.
Description of categories of persons whose data EUIPO processes and list of data categories	EUIPO staff and external event/meeting participants. For all events, the personal data processed in the lists of participants in Sharedox are: name, surname, institution, position, email and in some cases DNI (for access management)
Retention period	Personal data will be kept for 1 year from the end of the event.
Recipients of the data	n/a
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to the organisation of meetings and events by the Communication Service in EUIPO is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <p>The security measures applied to the Getresponse tool are described in the DPN-2018-058.</p> <p>The information stored in Outlook is protected as described in the Notification DPN-2016-019 Email Usage.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>PS of CS EUIPO Organisation and Management of Events: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/cbca2cd9-6c96-4f9f-ba05-c88c57f7216b</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-095
Name of the processing operation	EXAMINATION TOOLS
Last Updated:	29/03/2019
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Joint Controller organizational entity	Boards of Appeal
Joint Controller contact details	BOA-QPROs@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Tools for Trade Mark and Design examination and registration processes.</p> <p>This system integrates all the back office core business applications into a single place. It covers:</p> <ul style="list-style-type: none">• IP Tool (for EUTM examination and opposition, recordals, cancellations and RCD Invalidity),• Common Payment System (CPS),• MPS tool (for international applications and registrations),• RCD-EXA tool (for RCD examination) and• BoAST tool (for appeals proceedings). <p>It is foreseen that BoAST, MPS and RCD-EXA tools are soon integrated in the IP Tool.</p> <p>This examination module is connected to other satellite databases (such as PER for all personal data , CPS for payment data, PUB for publication in the EUTM or RCD Bulletin, QFMan and DAS for all correspondence related to EUTM and RCD dossiers, LCT for the language check of the EUTMs) through which different sets of data relating to the core task of the office is updated and fed into the examination tools.</p>
Purpose of the processing	<p>The collection, storage and processing of data shall serve the purposes of:</p> <p>(a) administering the applications and/or registrations (EUTM/RCD) as described in the EUTMR and CDIR Regulations, and in acts adopted pursuant to them;</p> <p>(b) accessing the information necessary for conducting the relevant proceedings (examination, opposition, cancellation, RCD invalidity, recordals, appeals, PUB and MPS) more easily and efficiently; (c) communicating with the applicants and other parties to the proceedings (ex parte & inter partes);</p> <p>(d) producing reports and statistics enabling the Office to optimise its operations and improve the functioning of the system (as foreseen in Article 6(1) of Decision No EX-14-3 of The President of OHIM and Article 112(2) EUTMR).</p>
Data Subjects	Applicants and representatives in trade marks and designs procedures



Description of categories of persons whose data EUIPO processes and list of data categories

together with all the data essential to the core tasks of the office, the IP Tool contains personal data of the owners and representatives as follows:

Representative:



Retention period	<p>Two periods:</p> <ol style="list-style-type: none">1. Indefinite (for reasons of legal certainty), as foreseen by Article 111(9) EUTMR and Article 7(1) of the Decision No EX-14-3 of the President of the OHIM.2. Upon request of a party concerned and as regards the data referred in Article 112(5), the retention period is of 18 months from the expiry of the EU trade mark or the closure of the relevant inter partes procedure.
Recipients of the data	<p>All EUIPO's staff has view access to the IP Tool. Majority of IP examiners from OD and limited number of BoA examiners have edit rights to the trade mark and designs dossiers. A limited number of OD examiners (the ones with "owners and representatives" profile) have edit rights to the PER database which feeds the "Persons" section of the dossiers.</p> <p>A limited number of Finance Department examiners (the ones in charge of fees management) have access to financial data in the CPS database. A limited number of Customer Department examiners (the one in charge of the publications in the bulletins) have edit rights to the PUB database.</p> <p>The parties to the procedures of the EUIPO and any third parties (the data is considered to be of public interest) have access through eSearch to the information stored in the IP Tool.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>AThe security measures include:</p> <ol style="list-style-type: none">1. Role-based access control to the systems and network2. Logical security hardening of systems, equipment and network3. Physical protection via secure Data Centre4. Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) <p>The management of access and right is done at ADM level. Examiners need to authenticate against ADM to enter the application. Moreover each examiner is assigned some ADM profiles and each profile is given some rights in the application. Each user is provided a username and password which gives access to certain features (in order to access the EUIPO systems and databases). The basic permissions in IP Tool allow seeing the details but additional permissions are needed to update the data and/or link/unlink owners/representatives to dossiers.</p> <p>The access to the database is restricted to some DTD staff (internal and external). Confidentiality and data protection clauses are signed-off by the service provider.</p> <p>All the standard security measures available for EUIPO's databases. The Office's server has been certified by an international certifying authority (Verisign Inc.), which guarantees that users have in fact connected to the Office. All information transmitted via the internet is encrypted using SSL protocol.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Data protection section of the EUIPO website: https://euipo.europa.eu/ohimportal/en/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2018-097
Name of the processing operation	Speakers of training and learning activities organised by the Academy
Last Updated:	28/06/2019
Controller Organizational entity	Academy
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	EUIPO Infrastructure and Buildings Department as internal processor and Pomilio Blumm as external processor, providing services to IBD as described in DPR-2019-007.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Academy operates as the Office's training and learning hub aiming to achieve high levels of professionalism and depth of expertise in the Office's workforce in IP-related matters and soft skills. It also reaches out to the broader community of stakeholders, IP specialists, academia and society in general for organising activities on IP dissemination and awareness. Dealing with trainers/speakers/moderators will involve handling personal data. Training and learning activities are organized by liaising with external and internal training providers and/or external organisations. The trainers/speakers/moderators can be internal Office staff members or external providers. Speakers from external service providers or organisations could be contacted to plan the specific objectives and description of the training sessions. Activities can take place both inside and outside the Office. The activities will be advertised by EUIPO. The training sessions may be recorded on video, edited and uploaded on EUIPO systems, and in the EUIPO Academy Learning Portal . If the speaker is external (not EUIPO staff) he/she will sign a statement of authorisation allowing to be recorded and the video uploaded on EUIPO systems. A satisfaction survey to obtain participants' views related to the speaker's performance will be distributed and a report with the speaker's performance will be created</p>
Purpose of the processing	<p>The processing of the speaker's data is necessary for:</p> <ul style="list-style-type: none">• Planning and organising trainings for EUIPO staff or other EUIPO stakeholders,• Selecting trainers/speakers/moderators based on their field of expertise, which may include the launch of calls for expressions of interest,• Security purposes when entering the premises,• Communicating with the speaker before, during and after the training for invitations, definition of the presentation, logistics, and feedback,• Announcing the training. The name of the speaker will be published in the agenda and in the announcement of the training sessions, including in the HR Database Allegro and the Academy Learning Portal• Allowing participants and trainers to network. A participant list may be shared between participants and organisations, which includes data of the speaker,• Ensuring quality control of training activities by means of satisfaction surveys. A satisfaction survey to obtain participants' views related to the speaker's performance will be distributed and a report with the speaker's performance will be created. The result of the speaker's performance will be shared with Academy staff in charge of organising the training and in the HR Database Allegro. For EUIPO staff it will also be shared with line managers or directors, and could be included in the person's appraisal.• EUIPO staff may be requested to complete the satisfaction survey of an event in the HR Database Allegro. An email requesting completion of the satisfaction survey will be sent from the eventsmanagementacademy mailbox.• Producing statistics and reports on various aspects of the training activities, including the speakers' performance, for use by EUIPO and the co-organising institutions of Academy events, such as the European Patent Office or National EU Intellectual Property Offices.• Keeping a database of suitable speakers for Academy events.
Data Subjects	EUIPO staff members, non-EUIPO speakers.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>For external speakers:</p> <ol style="list-style-type: none">1) Name,2) telephone number,3) curriculum vitae,4) nationality,5) gender,6) languages,7) email,8) type of post,9) job profile,10) availability period(s)11) satisfaction rates from surveys,12) photos taken during training and learning activities,13) recordings,14) planning and follow-up documents such as surveys and tables indicating learning needs,15) topic of the presentation,16) research work(s)/project(s),17) other fields of expertise. <p>For internal speakers:</p> <ol style="list-style-type: none">1) information extracted from HR Professionals section of the HR Portal ,2) curriculum vitae,3) satisfaction rates from surveys,4) photos taken during training and learning activities,5) recordings,6) planning and follow-up documents such as surveys and tables indicating learning needs,7) resources Allocation table (trainer's/speaker's/moderator's name),8) topic of the presentation,9) hours spent in preparation and presentation.
<p>Retention period</p>	<p>Your personal data will be kept only for the time necessary to achieve the purpose(s) for which they will be processed.</p> <p>Your data is kept for 5 years; however certain personal data, namely your name and surname, professional entity represented and professional contact details is kept for 10 years only and strictly for the Office's internal purposes, which are analytical, statistical and historical reporting of the number of your attendances to Academy events. Only the Academy, the Cabinet and the Executive Director will have access to this information.</p> <p>For some data of EUIPO staff the retention period specified in DPR-2018-016 applies.</p> <p>Recordings of presentations, which will be used in the eLearning course, will be retained for 10 years. Also for some recordings and photography, the processing is within the framework of DPR-2018-101.</p> <p>External contractors involved in the organisation of the training activities have time limits for storage as described in notification DPN-2017-042.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.</p>



Recipients of the data	<p>The access to the data is for the EUIPO staff involved in the management of training and Learning activities. For internal speakers, the line manager and director have access to the data as well.</p> <p>Co-organising institution, such as IP National Offices or the European Patent Office may process personal data only for the specific organisation of the training activities. This is done in the context of specific events such as IP Regional Seminars (in EU National IP Offices) or the IP Executive Week, which alternates its venue between the EUIPO and the EPO. The data necessary for organising the event, and for security purposes when entering the premises is: full name, ID number, speakers CV, job title, email address, field of expertise, photos taken during the event.</p> <p>For EUIPO staff, HR department will be a recipient of data in compliance with DPR-2018-016.</p> <p>External contractors involved in the organisation of the training activities may also have access to the relevant personal data, as described in notification DPR-2019-007.</p> <p>For recording and photography, the processing is within the framework of DPR-2018-101.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>Co-organisers of Academy events, such a European Patent Office or EU National IP Office are requested to use the data only for the purposes of the training/learning activities as well as for security.</p> <p>EUIPO-EPO memorandum of understanding is available here: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/c5f950a5-42ce-4788-a7a8-615d4a8ce8f7</p>
General Description of security measures	<ul style="list-style-type: none">• All personal data related to [process name] is stored in secure IT applications according to the security standards of EUIPO. These include:• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)• Security measures implemented by the external contractors involved in the organisation of the training activities are described in notification DPR-2019-007.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement for speakers of training and learning activities organised by the Academy: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/a56db7ab-ed56-476d-a73c-89037ca1053d</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-098
Name of the processing operation	Academy Network
Last Updated:	19/03/2019
Controller Organizational entity	Academy
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	EUIPO Infrastructure and Buildings Department as internal processor and Pomilio Blumm as external processor, providing services to IBD as described in DPR-2019-007.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Academy operates as the Office's training and learning hub aiming to achieve high levels of professionalism and depth of expertise in the Office's workforce in IP-related matters and soft skills.</p> <p>It also reaches out to the broader community of stakeholders, IP specialists, academia and society in general for organising activities on IP dissemination and awareness.</p> <p>The Focal Points Network is organized by the Academy. The network's role is liaising with specific contact persons designated from the National IP Offices and the User Associations for specific learning, training and networking purposes. The activities of the Focal Points Network involve handling the personal data of these contact persons.</p>
Purpose of the processing	<p>Processing the Focal Points Network participants' personal data is necessary for:</p> <ul style="list-style-type: none">• Informing of Academy events and activities for dissemination in the respective National Office,• Planning and organising yearly Academy Focal Points meeting,• Establishing videoconferences,• Sending the yearly survey on training needs,• Requesting collaboration in planning and organising Academy-related IP events such as seminars or webinars.
Data Subjects	The contact persons in the National IP Offices, and representatives from User Associations
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data of the contact persons is gathered in an Excel table:</p> <ul style="list-style-type: none">• Country,• Gender,• Name,• Institution,• Function at the Focal Points Network,• Professional position,• Email address,• Phone number,• Preferred language for communication• A conference or a workshop during the focal points meeting may be recorded as described in DPR-2019-007.
Retention period	<p>5 years for all data mentioned in "list of data categories" above</p> <p>10 years for name and surname, professional entity represented and professional contact details and strictly for the Office's internal purposes.</p>
Recipients of the data	<p>The access to the data is limited to the EUIPO Academy staff involved in the management of the Focal Points Network.</p> <p>External contractors involved in the organisation of the Focal Points Network activities may also have access to the relevant personal data, as described in DPR-2019-007.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the Academy Network Meeting (previously known as Focal Points) is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//S...</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/a3e4bd42-8b0f-48da-8697-973f135be870</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-100
Name of the processing operation	SIP Card - Regional Public Health Care System - Spain
Last Updated:	27/09/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service (HRD) - Spain: Public Administrations dealing with SIP cards
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the access of EUIPO's statutory staff and their dependent family members/ relatives covered by the Joint Sickness Insurance Scheme of the EU (JSIS) to the Regional Public Health Care System - SIP Card</p> <p>The "Consellería de Sanitat" (Health Department) has established a system to grant access to the Spanish Public Health Care System within the Valencian Community for statutory staff members (officials, temporary and contractual agents) and their dependent family members as well as pensioners and their relatives covered by the Joint Sickness Insurance Scheme (JSIS).</p> <p>The SIP card will grant the access to the Public Health Centres and Public Hospitals, complementing the Joint Sickness Insurance Scheme of the European Union (JSIS).</p> <p>The processing of personal data is necessary to submit to the "Consellería de Sanitat" the applications sent by EUIPO's staff members to the HRD in order to obtain a SIP card.</p> <p>The "Consellería de Sanitat" will inform EUIPO (HRD) once the SIP application has been processed, as well as from which Health Center the applicant may collect the SIP document.</p> <p>Health Centers are assigned according to the town and area where the person concerned lives.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of the data processing is to conduct procedures related to staff member's request to obtain a SIP Card for themselves and their dependent family members.</p> <p>The personal data are collected and processed in accordance with the Instructions received on 8 April 2015 from the "Consellería de Sanitat".</p>
Data Subjects	Statutory staff members: officials, temporary agents, contract agents and Staff members dependent family members / relatives covered by JSIS



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data of EUIPO staff having requested a SIP Card are processed by a limited number of authorised staff of the HRD:</p> <ul style="list-style-type: none">- Application form: Full name/ birth date/ copy of identity card (DNI-passport) / personal address/ telephone nr°/ email address/ degree of relationship (if the application concerns EUIPO's staff dependent family members);- Certificate of membership from the Joint Sickness Insurance Scheme of the European Union (JSIS): Full name/ personal nr°/ birth date/ starting working date at EUIPO/ type of insurance (primary)/ identity of dependent family members covered by the JSIS (name, birth date/ degree of relationship);- "Certificado de empadronamiento": Full name and address/ start date of registration date;- Copy of the passport / national identity card.
Retention period	<p>The processing of personal data starts from the moment the staff member submits to HRD an application to obtain a SIP card.</p> <p>Personal data will be stored in ShareDox for a maximum period of 1 year after the reception of the notification sent to EUIPO by the "Consellería de Sanitat" confirming that the SIP card has been processed.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Spanish Public Health Care System Administrations dealing with SIP Cards within the Valencian Community / "Conselleria de Sanidad" - Health department.</p> <p>EUIPO: Authorised staff of HRD working in the files / HRD management/ the Appointing Authority (AA) and the Authority Authorised to Conclude Contracts (AACC).</p> <p>In case of a complaint, the staff member's data may be disclosed to the Legal Service and/or to the EU Court of Justice.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Personal data related to SIP Cards are stored in secure IT application ShareDox, HR "Allegro" database and "SAP SuccessFactors" according to the security standards of EUIPO, as well as in specific electronic folders accessible only to authorized persons working in these files.</p> <p>Appropriate levels of access are granted individually only to the above recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing of personal data within the framework of the access of EUIPO's statutory staff to a SIP card:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/93cafcae-2cdc-47ec-98f2-f76fd78c7651</p>



EDPS Prior consultation

NO



Reference number	DPR-2018-101
Name of the processing operation	Recording and photographing
Last Updated:	25/02/2019
Controller Organizational entity	Communication
Controller contact details	Head of Communication Service: PersonalDataCS@euipo.europa.eu EUIPO, Avenida de Europa 4, 03008 Alicante, Spain.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>When CS is responsible for the photographing and/or recording of an event under request of a department/service or in the framework of an event organised by CS or organised by third parties at the Office, CS will perform photo and video of this event.</p> <p>If participants do not want their images or voices photographed/recorded/web-published, for compelling and legitimate grounds, CS gives the opportunity to all participants to opt out from the recording/photographing.</p> <p>In these cases and according to the available resources, the organiser should render the participants an alternative solution e.g. if a participant wishes to make an intervention without being recorded/nor his/her image published on any support, the recording might be stopped during the intervention; the participant's voice might be voiced-over subsequently, etc.</p> <p>The participants in the event will be informed of the housekeeping rules. Additionally, the participants will be notified orally at the start of the meeting/event of recording, streaming or photographing.</p> <p>The recording and/or photographing of minors will be carried out by CS prior consultation, case by case, with the Data Protection Officer in order to set up the adequate procedure to protect minors personal data</p>
Purpose of the processing	CS processes personal data with the purposes of effective promotion of the communication activities carried out at the Office.
Data Subjects	EUIPO staff (both external and internal) and external event/meeting participants.
Description of categories of persons whose data EUIPO processes and list of data categories	EUIPO staff (both external and internal) and external event/meeting participants. Categories of personal data collected: voice, image, pictures, videos, names, statements, opinions and any personal data communicated during the recordings.



Retention period	<p>The time limit for storage of the multimedia material taken differs according to the following multimedia material classification:</p> <p>Historic: 25 years renewable</p> <p>Medium: 7 years renewable</p> <p>Low: 2 years (renewable)</p>
Recipients of the data	<p>Multimedia material taken could be made available to:</p> <ul style="list-style-type: none">• staff accessing communication items through internal intranet (Insite)• general public accessing EUIPO websites or any other communication channel used by Communication Service such as news outlets or social networks (EUIPO has account on Facebook, Twitter, LinkedIn, Youtube and Instagram)
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to recording and photographing of events are stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p> <p>The security measure of the Audio-visual archive management system called 'CatDV': access to the tool is in principle, exclusive to the Integrated Visual Team of Communication Service, though access can be granted to other users depending on the purpose of the recording. This access is managed by the 'Integrated Visual Team'.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement for the processing of personal data in the context of Recording and Photographing by Communication Service :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/cb8fcc3a-b0a7-4c06-bee6-631063ec0d47</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-102
Name of the processing operation	Vaccinations Register - Agreement between the "Consellería de Sanidad - Generalidad Valenciana" and the EUIPO
Last Updated:	18/12/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service - HRD Hospitales y Sanidad, S.L.U Consellería de Sanidad – Generalidad Valenciana
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing data on the Vaccination Register of the "Consellería de Sanidad - Generalidad Valenciana" (RNV).</p> <p>The Medical Service of EUIPO uploads personal data of EUIPO's staff members (officials / temporary agents / contract agents) and Seconded National Experts (SNEs) to the Vaccination Register of the "Consellería de Sanidad". It concerns data of statutory staff /SNE's who request a vaccination or who have an obligation to be vaccinated before travelling on mission.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>Within the framework of the agreement signed on 06/02/2014 between the "Consellería de Sanidad - Generalidad Valenciana" and EUIPO, the Medical Service of EUIPO has a direct access to the Register of Vaccinations of the "Consellería de Sanidad - Generalidad Valenciana".</p> <p>The processing of data is necessary as a measure of preventive medicine to allow the Medical Service to upload personal data of EUIPO's staff members and SNE's to the Register of Vaccinations of the "Consellería de Sanidad".</p>
Data Subjects	EUIPO's staff members (officials / temporary agents / contract agents) and Seconded National Experts (SNE's).
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <ul style="list-style-type: none">- Full name / SIP nr° / DNI or NIE nr° / nationality / date of birth of the persons concerned;- Date of vaccination and type of vaccine.
Retention period	<p>Statutory staff members: 30 years after the end of service at EUIPO.</p> <p>SNEs: 6 months after the end of secondment at EUIPO.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Authorised staff of 'Consellería de Sanidad', as well as the doctor, the nurse and the assistant of the Medical Service of EUIPO.</p> <p>IT technicians (internal or external staff) may have access to the Medical Service's database "Preven" for maintenance and software renewal. They do not have access to the medical data.</p> <p>In addition, data may be disclosed on a temporary basis to the Director of Human Resources Department, the Head of Service of Entitlements and Staff Welfare Service, the Social Assistant, the Appointing Authority (AA), the Authority Authorised to Conclude Contracts (AACC), the Legal Service and the Court of Justice in case of complaints.</p> <p>Authorised staff dealing with administrative documents in connection with health data is requested to sign a declaration of confidentiality equivalent to a health professional.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Personal data collected by the "Medical Service of EUIPO" are registered in the records of Nominal Vaccinations (RNV) of the 'Consellería de Sanidad'.</p> <p>Personal data are kept by the Medical Service in a separate folder for each individual and stored in secured archives that are accessible to the doctor, the nurse and the assistant of the Medical Service.</p> <p>Personal data stored in 'Preven' (EUIPO Servers) are password protected under sign-on system and automatically connected to the user ID and general password. The access to medical files is done only by the Medical Service. Medical files are kept according to the security measures of EUIPO Information Systems under confidential documents.</p> <p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorisation process. Mechanisms of access tracking and monitoring of use of systems are established. Authorised users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement Vaccinations Register Agreement between the 'Consellería de Sanidad - Generalidad Valenciana' and the EUIPO:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/ada1f282-680f-4a46-9e4c-dcc515be3ab2</p>



EDPS Prior consultation	NO
-------------------------	----



Reference number	DPR-2018-103
Name of the processing operation	Knowledge Mapping DTD
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Knowledge Mapping Coordinators EUIPO, Digital Transformation Department (DTD)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The process aims to identify the knowledge available within the department and each team in particular. On a yearly basis, data will be collected on knowledge of systems, technical and organizational knowledge and specific skills of each person. The exercise is voluntary, DTD staff are not required to mandatorily provide this information.
Purpose of the processing	-Identify reference persons within the department. -Identify knowledge gaps, with the aim of fulfil them. -Identify learning paths, in order to schedule them.
Data Subjects	Digital Transformation Department staff members, Second National Experts and Trainees.
Description of categories of persons whose data EUIPO processes and list of data categories	With regard to persons information, the process supplies the following data: <ul style="list-style-type: none">o First name/ Middle name/ Last nameo Knowledge of Systemso Technical Knowledgeo Organizational Knowledgeo Role
Retention period	All the personal data will be kept for two years after the completion of the exercise.
Recipients of the data	DTD Director, Heads of Service and Knowledge Mapping Coordinators will have access to the entire register of information. Each Team Leader and the team members only for the data that corresponding to their team.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>For this process, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. <p>Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Knowledge Mapping Privacy Statement: https://insite.prod.oami.eu/digital-transformation-department/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2018-105
Name of the processing operation	Legal Consultations for EUIPO's statutory staff members / seconded national experts (SNE's) and trainees relating to private legal matters - Spanish law.
Last Updated:	11/04/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	HRD External provider: Lucas-Abolex UTE (Lucas & Asociados Abogados)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the contract between EUIPO and a legal expert (legal consultations for EUIPO's statutory staff members, SNE's and trainees) - Spanish Law - Private legal matters</p> <p>In the framework of the EUIPO's social policy, an expert in Spanish law is available for consultations of EUIPO's staff members (officials, temporary agents and contract agents), as well as seconded national experts (SNE) and trainees. The aim of this service is to offer an initial legal opinion in order to enable the EUIPO staff members to take any possible decision relating to any private matter within the framework of Spanish Law (marriage, divorce, rental, consumer issues, etc.).</p> <p>All data are disclosed to the legal expert by the person concerned.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The processing of personal data is necessary to advice staff members within the framework of the contract between the EUIPO and the external legal expert.</p> <p>The advice is provided for general information purposes only. EUIPO will not be liable for damages of any nature arising from the use of the advice provided.</p> <p>The Human Resources Department (HRD) receives a monthly activity report from the legal expert containing anonymous statistical data.</p>
Data Subjects	Statutory Staff: officials, temporary agents and contract agents Seconded national experts and trainees
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed by the legal expert only on a need to know basis:</p> <ul style="list-style-type: none">- Full name and nationality of the person concerned;- Statutory link (statutory staff/ or SNE/ or trainees) and if it concerns new recruited staff or not;- Legal area and a brief outline of the consultation;- Type of consultation (by interview / by email / by telephone) and language used;- Time spent with consultation (including meetings / research / calls, etc);- Nr° of the file/ date of consultation/ first time of consultation or not/ file open or closed.
Retention period	<p>Personal data processed by the legal expert related to the consultations of EUIPO's staff members will be deleted not later than 1 month after the end of each "one year contract" between EUIPO and the legal expert. It is kept for the above period for audit and contract execution reasons.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Only the legal expert who receives the individual consultations from staff members has access to the data.</p> <p>The monthly activity report sent by the legal expert to authorised staff of HRD does not include the names of the persons having submitted consultations.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Data are stored and processed in EUIPO's secure IT applications (Excel and Outlook), according to the security standards of EUIPO.</p> <p>Appropriate levels of access are granted individually only to the above recipients. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the framework of legal consultations for EUIPO's statutory staff members / :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/4c053191-1e1c-48dc-b639-f95bfd119d9d</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-106
Name of the processing operation	Processing of personal data within the framework of the Data Protection Office tasks and duties
Last Updated:	23/01/2019
Controller Organizational entity	Data Protection Office
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Contact: Data Protection Officer, EUIPO DataProtectionOfficer@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Once EUIPO Data Protection Office receive a consultation or enquiry (request or complaint) from a delegated controller, Data Protection Coordinator, member of an EUIPO Staff Committee, member of EUIPO personnel or from an external user concerning personal data, they will act in accordance with the Updated Work Instructions QSD-0295 DP Office and DPCs.</p> <p>All enquiries and consultations are stored in ShareDOX and Outlook in an individual folder especially created by authorised staff with a number assigned.</p> <p>In the near future, all the enquiries and consultations will be only stored in the EUIPO Data Protection Tool.</p> <p>The DPO may also process personal data to carry out investigations, in relation to a complaint received from or related to an Office's staff member or external user.</p> <p>In the exercise of this task, the DPO shall issue an opinion on draft replies of the controllers to complaints or draw up one. This procedure is done in writing and the related documents are stored in ShareDOX; Outlook and in the DP Tool</p>
Purpose of the processing	<p>Your personal data will be processed to ensure the correct application of the Regulation (EU) 2018/1725, in as much as the provisions concerning the role, duties and tasks of the DPO are concerned.</p> <p>The procedure for the DPO to process enquiries (requests for exercising the data subjects' rights and complaints) as defined in the Decision No ADM 18 65 implementing Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 in the European Union Intellectual Property Office (adopted by the Executive Director and provided to the EDPS as required by Article 44.1 Regulation (EU) 2018/1725 and operationally clarified by the Updated Work Instructions QSD-0295 DP Office and DPCs.</p> <p>The EUIPO DPO process personal data in order to:</p> <ul style="list-style-type: none">• respond to the consultation/enquiries received;• provide opinion, advice and recommendations;• carry out investigations.
Data Subjects	EUIPO staff members and EUIPO external users



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories/types of personal data processed are the following:</p> <p>i. EUIPO staff members:</p> <ul style="list-style-type: none">• name and surname• email address• Department/Service <p>ii. EUIPO external users (anyone sending an enquiry to the Data Protection Office):</p> <ul style="list-style-type: none">• name and surname• email address• physical address <p>Any other personal data which may be provided by the enquirer regarding himself/herself or other individuals in the context of information exchanged such as company, organisational entity, description of concerns, personal case, circumstances, description of facts, opinions, assessments, etc.</p>
Retention period	<p>Your personal data will be kept only for the time necessary to achieve the purpose(s) for which they will be processed.</p> <p>Personal data related to records inserted in the EUIPO Data Protection Register will be stored as long as the processing is operational. After that date the record will be deleted from the Register but archived in the DP Tool and ShareDOX for the period of 5 years for reasons of possible legal appeal procedures.</p> <p>DPO Tool for storing files (consultations, complaints, and data breaches notifications/communications) and records: the DPO retention schedule will be manually implemented in the tool. In the future, it might be that an automated module for the implementation of the retention periods established per each category of files is available.</p> <p>The schedule, prepared in cooperation with all teams and the DPO, sets out the retention periods per case file type on the basis of the administrative, legal and financial usefulness.</p> <p>The retention period of the personal data contained in the documents is also defined in the records of the operational processes supported by those documents.</p> <p>The records' retention schedule also indicates the subsequent actions at the end of the administrative retention period on the basis of the potential historical value of documents and files.</p> <p>These actions include elimination of certain data, sampling or selection and long term preservation of the documents and cases identified as archives</p> <p>Personal data related with complaints are to be kept for one calendar year after closure of the complaint. In case of complaint to EDPS, the complaints and the personal data will be kept until the complete closure of the case (either before the EDPS or before the Court).</p> <p>Personal data processed in the scope of investigations will be kept up to five years for simple and non-substantiated cases and up to a maximum of 10 years for investigations where irregularities or breach of the DP Regulation was concluded.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.</p>



Recipients of the data	<p>Personal data will only be shared on a strictly need to know basis.</p> <p>In general, personal data are processed only by the DP Office staff and by the Data Protection Coordinators (taking into account the respective controller in each of the cases concerned and the sensitivity of the particular case).</p> <p>In some cases, such as breach of personal data, formal complaints, investigations, data are disclosed to the Litigation Service, the delegated controller (Director of Department or Head of Service) and other management, e.g. members and Head of Cabinet, the Executive Director, etc.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>DP Office staff members implement the appropriate technical and organisational measures in order to safeguard and protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>All personal data related to this processing is stored in secure IT applications according to the security standards of EUIPO.</p> <p>These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network;• Logical security hardening of systems, equipment and network;• Physical protection via secure Data Centre; <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the processing of personal data within the framework of the Data Protection Office tasks and duties:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/b72586bf-5bad-4c8e-84b4-1b8c8db98e0d</p>
EDPS Prior consultation	NO



Reference number	DPR-2018-112
Name of the processing operation	Management of contact details in Facility management service
Last Updated:	28/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Processors of the data in the Excel table with contact details of representatives/contact points involved in the implementation of construction projects- FM staff in IBD and the external provider of facility management IDOM; Processors of the data in the Excel table of contact details of external resources- IBD management and Facility management secretariat in IBD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	FM service in IBD maintains Excel tables with contact details of: - external resources whose contact details don't appear on the internal web page Insite; - Representatives/points of contact of companies and authorities involved in the implementation of construction projects of EUIPO. For the excel table with contact details of external resources, the personal data is collected upon the entry into service of the external resources and is deleted upon the completion of the service. For the excel table with contact details of representatives of companies/authorities involved in the implementation of construction projects the data is collected during the project start phase and is deleted after 10 years from the project implementation.
Purpose of the processing	Personal data of external resources is processed in order to ensure the communication with them and the successful provision of the service. Personal data of representatives/points of contact of companies and authorities involved in the implementation of construction projects of IBD is processed for the purpose of stakeholders' management, in order to ensure the successful implementation of the project and the post-implementation follow-up and in order to comply with the provisions of Ley 38/1999, de 5 de noviembre, de Ordenación de la Edificación.
Data Subjects	External resources whose contact details don't appear on the internal web page Insite; Representatives/points of contact of companies and authorities involved in the implementation of construction projects of EUIPO.
Description of categories of persons whose data EUIPO processes and list of data categories	The categories of persons whose data EUIPO processes are as follows: - external resources whose contact details don't appear on the internal web page Insite; - representatives/points of contact of companies and authorities involved in the implementation of construction projects of EUIPO. The processed personal data of external resources is the following: name, surname, company, function, telephone numbers, email address. The processed personal data of representatives/points of contact of companies and authorities involved in the implementation of construction projects of IBD is as follows: name, surname, company/authority/organisation, ,telephone number, email address.



Retention period	<p>The personal data of external resources is stored till the person works in EUIPO.</p> <p>The personal data of the representatives/ points of contact of companies and authorities involved in the implementation of construction projects of IBD is stored for the maximum period of 10 years after the implementation of the project that is the guarantee period established in the contract between EUIPO and the provider of services (on the basis of Ley 38/1999, de 5 de noviembre, de Ordenación de la Edificación).</p>
Recipients of the data	<p>The people who have access to the data are as follows:</p> <ul style="list-style-type: none">• to the Excel table with contact details of representatives/contact points involved in the implementation of construction projects- FM staff in IBD and the external provider of facility management IDOM;• to the Excel table of contact details of external resources- IBD management and Facility management secretariat in IBD.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this procedure is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Specific Privacy Statement on the processing of personal data in the procedure of management of contact details in Facility mana:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6f6df199-c20d-4d-d0-a1b4-8c2b6dce5c9f</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-001
Name of the processing operation	Processing personal data on the Prevention and Management of Conflict of Interests - Declaration of Interests for EUIPO staff and members of the Boards of Appeal
Last Updated:	03/04/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The management of the declaration of interests is necessary to encourage the highest standards of administration, professional ethics, integrity and independence.</p> <p>It serves to identify and disclose, in a transparent and consistent manner, the handling of situations where potential conflicts of interests may arise in order to avoid any conflict between the EUIPO public duties and any kind of private interest of staff.</p> <p>It deals with the following in particular:</p> <ul style="list-style-type: none">- assignment of staff to a Department/Service;- participation of staff in Selection Committees for recruitment procedures;- previous activities/current outside activities for staff in active employment or on personal leave/unpaid leave; professional activity during leave on personal grounds/unpaid leave;- activity of staff who have left EUIPO (on retirement/invalidity or at end of contract);- financial interests related to EUIPO activity;- permission to receive a decoration or award / to keep a gift/hospitality (lunches/dinners linked to the function of the staff);- spouse's/legally recognised partner's/dependant family member's current professional activity and financial interests that might entail a risk of conflict of interests;- publishing articles and speeches / participation in election campaigns;- holding an elected public office. <p>The Declaration of Interests does not contain an exhaustive list of potential interests. The processing of personal data includes any other element indicated by the data subjects that may affect their independence. The submission of the Declaration of Interests is compulsory.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>



Purpose of the processing	<p>Data are processed in compliance with rules of the Staff Regulations (SR) of officials and Conditions of Employment of Other Servants (CEOS) of the European Union, as well as with the Code of Good Administrative Behaviour and Guidelines on the Prevention and Management of Conflict of Interests.</p> <p>The purpose of the processing of data is to:</p> <ul style="list-style-type: none">- examine requests/declarations submitted periodically by internal, external and former staff with regard to their rights and obligations;- assess whether or not the requests/declarations are incompatible with their obligations under the SR and CEOS or constitute a risk for the EUIPO (real or potential impact in the EUIPO activities such as to impair the person's independence at EUIPO);- refuse requests (particularly where there is a potential conflict of interests, risk of breach of confidentiality, omission/breach of the rules, etc.);- or authorise requests, possibly with certain restrictions.
Data Subjects	<p>EUIPO's staff members, (officials, temporary agents and contract agents), members of the BOA, seconded national experts / trainees / consultants / interims. External staff are requested to declare conflict of interests through their employer before working at EUIPO.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <ul style="list-style-type: none">- full name, personal number, start/end data at EUIPO;- assignment (department and functions) of internal/external and former staff;- full name of spouse/legally recognised partner/dependent family member and his/her employer/professional current professional position and financial interests that might entail a risk of conflict of interests;- activities carried over the past 2 years / current activities, including outside activities;- gifts worth between 50€ and 150€/ financial interests (shares/stocks exceeding 50.000€ in the capital of companies having interests related to EUIPO activity and/or assets or any intellectual property rights that may have a potential impact in the person's activity at EUIPO;- any other relevant interests that may have a potential impact in the EUIPO activities.
Retention period	<p>Data will be kept during 5 years after the end of the employment / mandate / contract or activity.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Authorised staff of HRD giving an indicative level of real or potential conflict of interests regarding to a specific activity, the line manager and the Appointing Authority.</p> <p>The Ethic Committee is consulted on matters related to real or potential conflict of interests. This Committee is composed by Head of the Legal Service, the Director of HRD and the Line Manager or the Chairperson of the Management Board for staff appointed by the Council of the European Union or by the Management Board.</p> <p>EUIPO contractors and subcontractors might have access to data for maintenance and development of the applications supporting the "HR Database" under request and supervision of EUIPO.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	<p>NO</p>



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Paper documents (e.g.: request of outside activities, etc.) are kept in secured cupboards in the HRD (personal file) only accessible to authorised staff of HRD.</p> <p>Electronic working data are stored in secure IT applications (Sharedox, HR "Allegro" database and "SAP SuccessFactors" in the cloud) according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>A declaration of confidentiality is signed by the persons having access to the HR database.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on Prevention and Management of Conflict of Interests - DoI- EUIPO staff members and BOA members:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/255e063a-5eeb-4fcf-8d75-039276be7a2b</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-002
Name of the processing operation	Use of a Video- surveillance System in EUIPO
Last Updated:	31/01/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Security services in Infrastructures and Building Department External processor: security company Securitas and its subcontractor Nsecure B.V.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The European Union Intellectual Property Office (EUIPO) operates a Video-Surveillance System (VSS). EUIPO's video-surveillance system is an integrated CCVT system. The VSS has as an objective to ensure the safety and security of EUIPO buildings, assets, staff and visitors. The video-surveillance system is an integrated CCVT system that consists of detection and observation cameras with different settings/configuration depending on the area monitored. The cameras are placed in EUIPO's campus, composed of three buildings and the EUIPO perimeter, and at EUIPO premises outside the EUIPO campus, in Alicante and abroad. Cameras monitor and/or record all main buildings entrances, external emergency exits, secondary entrances, entrances to the car parks, common areas such as building's halls, parking areas' hallways giving access to the buildings, and data centers.</p> <p>Cameras do not monitor any areas under heightened expectations of privacy such as staff offices and leisure areas (restaurants, canteens, cafeterias, leisure rooms, EUIPOFit areas, lounge areas), waiting rooms, toilet facilities, etc. The only exception of this rule is the area that gives access to the Executive Director's Office, where cameras are installed for the purpose of protection of highly sensitive and confidential information.</p> <p>The location of all cameras is carefully scrutinized in order to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes. Detailed information regarding the cameras types, functions and specifications can be found in EUIPO's Video- surveillance Policy.</p>



Purpose of the processing	<p>The processing of personal data within this procedure has the purpose to prevent unauthorised physical access to premises and to ensure the security of EUIPO's staff, installations, facilities, information, systems and patrimony in general.</p> <p>The purposes of the processing operation are the following:</p> <ul style="list-style-type: none">• Detecting, deterring and preventing all kind of attacks, illegal entrees or other incidents (e.g. theft assets, vandalism, flood, fire) in EUIPO headquarters and external premises.• Detecting, deterring and preventing attacks or illegal entrees in the entrance and exit areas.• Detecting, deterring and preventing illegal entrees in the main buildings via the parking areas.• Detecting, deterring and preventing incidents in common areas such as hall and park areas.• Detection, deterring and prevention intrusions into the Data Protection Centres.• Investigating the facts after the occurrence of a physical security incident, and securing evidence to prosecute the perpetrator/s. The VVS is not an investigative tool. In exceptional cases the images may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation. <p>The processing of personal data collected from the VSS shall not be used for any other purpose. There shall be neither hidden cameras for ad-hoc investigations nor cover surveillance activities. There shall not be special video-surveillance for high-level events or demonstrations. The VSS shall not be used to monitor the work of employees or to monitor attendance.</p> <p>The footages shall be used for their original purpose and the video- surveillance system is neither installed nor designed for the internal investigations beyond physical security incidents or electronic incidents (for instance, theft of information stored in a PC).</p>
Data Subjects	<p>The categories of persons whose data EUIPO processes are EUIPO staff and external resources working in the EUIPO premises, visitors and external participants in events and meetings entering in the EUIPO premises and passing-by individuals at the sidewalk adjacent to the exterior part of the perimeter fence.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories of persons whose data EUIPO processes are EUIPO staff and external resources working in the EUIPO premises, visitors and external participants in events and meetings entering in the EUIPO premises and passing-by individuals at the sidewalk adjacent to the exterior part of the perimeter fence.</p> <p>The cameras record digital images with indication of time, date and location of:</p> <ul style="list-style-type: none">• Data subjects entering/leaving/walking in public areas of EUIPO's premises and passing-by individuals at the sidewalk adjacent to the exterior part of the perimeter fence;• Data subjects in Cars when accessing car park areas, docks areas and in the ramps of the car park and cars passing on the street close to the exterior part of the perimeter fence.• Data subjects inside of premises at the hallways of parking areas.• Data subjects at the ED's adjacent area.• Data subjects entering in highly restricted areas (data protection centers).
Retention period	<p>Camera images are stored for not more than 7 days. When this period expires, the data are automatically deleted. In case of a security incident, a backup of the corresponding video recording are stored for the period necessary to investigate and solve the incident. This period can be extended until the conclusion of an eventual complaint or appeal. Any additional retention period is documented, registered and its necessity is reviewed regularly. As soon as the purpose of the investigation and eventual complaint or appeal ends the images shall be deleted. In principle, when the person who has committed the security incident does not claim the opposite, the data will be retained for 1 year from the date of the incident.</p>
Recipients of the data	<p>The VSS, except from the cameras at the 5th floor, is monitored in real time by de security guards in the Security Room, 24 hours a day and 7 days a week. Access to recorded video- surveillance material is granted on a need- to-know basis only to authorised EUIPO staff and external providers. Details regarding the types of access to the VSS can be found in the link available in the Compliance check section of this record.</p> <p>Only in exceptional circumstances, the images are disclosed to investigatory bodies or enforcement authorities in the framework of a formal disciplinary or criminal investigation and prior consultation of the DPO, e.g. in the context of SEAT Agreement. The conditions under which the footage can be used in the investigations are specified in the Video-Surveillance Policy. Security service will keep a register in an electronic form of disclosures.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>No disclosure of data recorder by the surveillance camera system shall be made except by written authorization of the IBD Director, after consulting the DPO. Images or footages maybe disclosed to investigatory bodies in the framework of a formal disciplinary or criminal investigation, such as:</p> <ul style="list-style-type: none">• EU organisations such as Anti-Fraud Office (OLAF) or Commission's Investigation and Disciplinary Office (IDOC) in the framework of a disciplinary investigation, under the rules set forth in Annex IX if the Staff Regulations of Officials of the European communities.• Spanish law enforcement authorities, under the observance of the coordination on security matter established in the Agreement sign between Spain and EUIPO (SEAT Agreement).• Private entities such as insurance companies; upon consultation with the DPO and approval of ICLAD's Director and IBD Director.
General Description of security measures	<p>All personal data related to this procedure is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) Confidential declaration is signed by the external providers that have access to the CCTV.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Video- surveillance policy: https://euipo.europa.eu/ohimportal/en/euipo-video-surveillance-policy?inheritRedirect=true
EDPS Prior consultation	NO



Reference number	DPR-2019-003
Name of the processing operation	On processing personal data in the internal audit
Last Updated:	08/03/2019
Controller Organizational entity	Internal Audit
Controller contact details	Internal Audit Head of Service: InternalAudit@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The data subjects information is collected via the EUIPO directory and the organisation chart just before an audit starts. The information is used for any further communications between IAS and the audited area and to provide corresponding permission in the document management tool (ShareDox). It has to be noted that the reports spread to Top Management are anonymised; therefore, no data transfer has to be considered. All personal data related to the internal audit is stored in secure IT applications according to the Office's security standards. Data may be stored in IA's management tool 'AutoAudit', ShareDOX folders, and/or LimeSurvey, to which only IA staff have access, as well as in MS Outlook for correspondence management. Paper documents are kept locked in secure cupboards. The processing is automated.</p>
Purpose of the processing	<p>The purpose of processing data is to audit Office systems, process and procedures in order to issue the corresponding Audit Reports, having access to relevant documentations and contacting the concerned people. Moreover, it permits to send the satisfaction survey to those who have directly taken part to the audit.</p> <p>The need to establish the EUIPO Internal Audit Service is provided under Article 141 of the EUTMR. Title IV chapter 8 of the financial provisions applicable to the Office (Regulation No CB-1-15) and title IV chapter 7 of the rules for the implementation of the Regulation No CB-1-15 (Regulation No CB-2-15) further specify the responsibilities and independence of the Internal Audit Service.</p> <p>Anonymised reports are addressed to the Office's top management and governing bodies, and to bring information to the European Court of Auditors, to provide assurance and make recommendations regarding the quality of the Office's management and control systems.</p>
Data Subjects	EUIPO staff members : Internal auditors, auditees and audit observers.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following: Name, title, position, functions and department of the data subjects.</p> <p>For external assessment: Company contact details (internet and email address, business and mobile telephone number, official postal address).</p>
Retention period	<p>The documents are kept in line with the following:</p> <ul style="list-style-type: none">- 7 years since the publication of Audit Plan, in line with EUIPO FR No CB-1-15 (Article 42(5) and 107 FR)- 1 year after the publication of the Follow-Up Report for the related working documents.
Recipients of the data	All IAS members are authorised to access the data, namely: Head of Service, Auditors and Administrative support.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	General description of security measures (technical & organizational): All personal data are stored in secure IT applications (ShareDox, AutoAudit, LimeSurvey) according to the security standards of EUIPO. Data is stored only in EUIPO servers. The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement on processing personal data in the internal audit: http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/e5e6d5e0-e6cc-452e-b543-52cfd19a73ca/Data%20Protection_Privacy%20Statement%20-%20final.pdf
EDPS Prior consultation	NO



Reference number	DPR-2019-004
Name of the processing operation	Magister Lvcentinvs EUTM and RCD Intensive Modules
Last Updated:	27/03/2019
Controller Organizational entity	Academy
Controller contact details	DPOexternalusers@euipo.europa.eu
Joint Controller organizational entity	Other
Joint Controller contact details	magister.lvcentinvs@ua.es
Name and contact details of processor	EUIPO Infrastructure and Buildings Department as internal processor and Pomilio Blumm as external processor, providing services to IBD as described in DPR-2019-007.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Academy operates as the EUIPO's training and learning hub</p> <p>The Magister Lvcentinvs EUTM and RCD Intensive Modules is an event organized by the Academy, with the aim to provide specialised training on trade marks and designs to university students. To do so, the Academy receive from the University of Alicante an Excel file with the personal data of the participants attending the event (students and staff).</p> <p>This personal data is used to prepare the badges that will provide access to the participants to the EUIPO premises where the event takes place.</p>
Purpose of the processing	Processing the Magister Lvcentinvs EUTM and RCD Intensive Modules participants' personal data is necessary for: <ul style="list-style-type: none">• To allow entrance to EUIPO premises• To take a group photo of participants for promotion and communication purposes.
Data Subjects	Participants: students and university staff
Description of categories of persons whose data EUIPO processes and list of data categories	<p>EUIPO will process the following data:</p> <ul style="list-style-type: none">• Name, surname of participants (students, University staff)• ID number• In case of students: name of university they are studying at• Group photo of participants <p>During the event, the EUIPO (Communication Service) takes a group photo of all participants. Those data will be processed according to the Communication Service Record and Compliance checklist</p> <p>Participants will be informed that they can decline to be part of the group photo</p>



Retention period	<p>The personal data (names, passport/ID numbers) transmitted to the EUIPO by the University of Alicante will be deleted immediately after the event has ended.</p> <p>The information on how many students attended from the different universities will be used to draft an event report and will be deleted no later than one year after the event has ended.</p> <p>The group photo will be used solely for communication and promotional purposes. Retention will follow the standards set by the multimedia retention criteria of the Office: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/e8b04e7b-f4fb-4c1a-9a65-20082d996807</p>
Recipients of the data	<ol style="list-style-type: none">1. The Academy provides the data to IBD event provider Pomilio Blumm to arrange access to EUIPO premises.2. EUIPO Academy staff on the need to know basis has access to the MS Outlook archive folder where data are stored.3. Communication Service in relation to the group photo.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the Magister Lvcentinvs EUTM and RCD Intensive Modules is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/fa92a1f3-daa1-4e9d-8077-9aa92f29a9f4</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-005
Name of the processing operation	Statistics on individual production and timeliness, i.e. Board decision tracking table; Rapporteur Statistics; BoA Task Reports
Last Updated:	28/06/2019
Controller Organizational entity	Boards of Appeal
Controller contact details	President of the Boards of Appeal European Union Intellectual Property Office, Avenida de Europa 4, ES-03008 Alicante, Spain BoA-PresidencyOffice@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>MS Excel tables containing the following information for all appeal decisions and tasks (Production Data):</p> <ul style="list-style-type: none">• the identification of the file concerned;• the type of decision or task counted and measured;• the date when the decision or task was allocated to the Data Subject;• the date when the decision or task was executed;• the date when the decision or task was due;• if the decision or task was done in due time (timeliness);• the outcome of the decision or task;• the organisational unit (specific Board, Registry, KIS) where the decision was taken or the tasks performed;• the name and / or identifier of the Data Subject who produced the decision / performed the task. <p>All the Production Data will be extracted from the relevant databases (BoA Single Tool; Data-warehouse; Business Object) by the Boards of Appeal's Quality, Performance and Risk Officer (in case of the Rapporteur Statistics and BoA Task Reports) or collected by the Chairperson's secretary of the respective Board (in case of the Board decision tracking tables).</p> <p>The individual list of decisions or tasks measured is reviewed and communicated twice per year to the staff whose activities are to be monitored (before the mid-year review exercise and before the appraisal exercise).</p>
Purpose of the processing	<p>Measuring the quantity and timeliness of decisions drafted and tasks performed by the staff of the Boards of Appeal.</p> <p>The aim of this activity is, on the one hand, to monitor the global output of the Boards of Appeal in relation to the Boards of Appeal's service standards (including the timeliness service standards), and, on the other hand, to use this objective criteria - quantity and timeliness - as one of the elements taken into consideration for the appraisal of the Boards of Appeal staff subject to appraisals. Such production and timeliness management system must be carried out in order to measure the production and timeliness of the concerned staff taking into account all the other relevant factors.</p> <p>In case of the President, the Chairpersons and the further Members of the Boards of Appeal, the production data is also used to allow the Management Board to exercise its powers under Article 166 EUTMR and Article 153 EUTMR.</p>
Data Subjects	Staff members of the Boards of Appeal dealing with tasks (including proceedings tasks & decisions) which are subject to evaluation as well as the President, the Chairpersons and the further Members of the Boards of Appeal.



Description of categories of persons whose data EUIPO processes and list of data categories	Staff members of the Boards of Appeal dealing with tasks (including proceedings tasks & decisions) which are subject to evaluation as well as the President, the Chairpersons and the further Members of the Boards of Appeal.
Retention period	<p>The excel sheets containing the Board decision tracking table and the Boards of Appeal task reports shall be kept for no more than two years after the end of the appraisal period in order to allow the management to use the data for the appraisal of the staff members concerned, and the latter to exercise their rights as provided for in the internal rules on appraisals and/or in Article 90(2) SR. The excel sheets containing the Rapporteur statistics shall be kept for no more than five years. In case of the Rapporteur statistics a longer retention period is needed to allow the Management Board to evaluate the performance of the President, the Chairpersons and the further Members of the Boards of Appeal in accordance with Article 166(2), (3) and (5) EUTMR.</p> <p>After the above mentioned periods, the excel sheets shall either be deleted and no longer archived or anonymized, unless they need to be kept longer to establish, exercise or defend a right in a legal claim pending before the court.</p> <p>The Rapporteur statistics are made available to other BoA Members only if the concerned BoA Member has signed a written declaration of consent. The voluntary character of the Member's declaration of consent was reinforced in the following way: a) insertion of the word 'voluntary' in the title of the declaration; b) highlighting through underlining and bold face printing the elements 'free choice', 'can be withdrawn at any time', 'only valid for the period of one mandate', 'expires automatically'. The EDPSs recommendation of limiting the validity of the declaration of consent was implemented. The declaration of consent will be only valid for the period of one mandate (5 years) and expires automatically at the end of that mandate.</p>
Recipients of the data	<p>Access to the Business Object database allowing the extraction of Production Data with regard to staff working at the Boards of Appeal shall be granted to:</p> <ul style="list-style-type: none">• the Quality, Performance and Risk Officer of the Boards of Appeal;• Experts (database administrators) from the Digital Transformation Department (DTD) in case of technical problems that need to be solved. <p>Access to the excel sheets containing the Boards of Appeal statistics shall be granted to:</p> <ul style="list-style-type: none">• The Data Subject's hierarchy and their secretaries;• the Quality, Performance and Risk Officer of the Boards of Appeal to perform his tasks and to prepare anonymized Board of Appeal statistics. <p>In case of the Rapporteur Statistics, access is also provided to:</p> <ul style="list-style-type: none">• all Members of the Boards of Appeal with regard to the Production Data of other Members who have expressly consented in written form to their data being made available to other members of the Boards of Appeal. The consent can be freely revoked at any time by informing in writing the Quality, Performance and Risk Officer of the Boards of Appeal;• in the cases foreseen in the EUTMR, the Management Board of the EUIPO with regard to some of the data contained in the Rapporteur Statistics in order to allow the Management Board to exercise its rights, in particular Article 166 and Article 153 thereof. <p>The individual Boards of Appeal statistics are not disclosed to any person outside the Boards of Appeal with the exception of the Rapporteur Statistics which will be disclosed to the Management Board of EUIPO where necessary in order to allow the Management Board to exercise its rights.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to this processing is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network;• Logical security hardening of systems, equipment and network;• Physical protection via secure data centre. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC).</p> <p>Access to EUIPO systems and Databases shall only be accessible with an individual username and password. Pursuant to the security policy at EUIPO, user profiles shall be updated regularly.</p> <p>Access control systems with adjustable permissions are implemented. Only authorized persons have access to the documents.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Data Protection Statement on measuring individual production and timeliness:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3c284091-ada2-47b6-baf6-928be5d8c6d0</p>
EDPS Prior consultation	YES



Reference number	DPR-2019-006
Name of the processing operation	Security Verification of External Resources
Last Updated:	10/12/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal: Head of Common services, IBD, EUIPO H&Steam in IBD External: H&S services provider - 'PREVING Consultores S.L.U.' (https://www.preving.com/) and its subcontractor (Sistel which is official distributor of Google Cloud Platform licences)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The process of security verification consists of the following:</p> <ol style="list-style-type: none">1. One single security verification process will be applied to all external staff that will be granted the access card of external contractor (red access card);2. The process of security verification ensures that the companies have provided documentation that certifies that their employees, who will work in the Office premises, do not have pending criminal convictions and have provided authentic information regarding their professional and educational qualifications;3. The storage of the information is done within the Portal for security verification. The portal is integrated with the access management system that permits the automatic authorisation/non-authorisation/suspension of access on the basis of the result of the security verification.4. The accuracy and the authenticity of the information are declared by each company for its employees(external resources for EUIPO). In case of subcontracting, the contractor may be responsible for the submission of the data of the employees of the subcontractor. The completeness of the documentation is checked by external provider of EUIPO on EUIPO's behalf;5. EUIPO stores the information provided by the company for the external resource;6. The information stored in the portal is as follows: <ul style="list-style-type: none">• Declaration of confidentiality (EUIPO awareness agreement) signed by the external resource;• Educational and professional qualifications and references of the external resource (if applicable);• Declaration of the company that certifies to EUIPO that all of the above described documents are authentic. This accreditation shall be provided prior to the entrance of the external resources to EUIPO premises;• Declaration of the company that certifies to EUIPO that the external resource does not have pending criminal convictions. This accreditation shall be provided at the latest two weeks after the authorization of the access of the person to EUIPO installations. Extension of this period shall be authorized only in case the company duly justifies in advance the delay in the provision of the information. <p>In case the above documents have not been duly provided by the company in the portal, the access of the external resource to the EUIPO's premises will be denied/ cut .</p>



Purpose of the processing	<p>The process of security verification consists of ensuring that the companies have submitted in the Portal for security verification of external resources (hereafter the Portal) all documentation which has been requested by EUIPO. The control of this documentation is a prerequisite for the authorisation of the access to EUIPO premises of all external resources who receive the access card of an external contractor.</p> <p>The purposes of the processing of personal data are as follows:</p> <ul style="list-style-type: none">• to ensure that access to EUIPO premises is given only to the external resources for whom their companies have submitted all the documentation requested by EUIPO;• to ensure the security and safety of EUIPO staff, information, installations and patrimony. <p>In case the company has not submitted the required documentation for its employees in the Portal, thier access to EUIPO premises will not be authorised.</p>
Data Subjects	<p>It is compulsory for all external resources of the EUIPO required by their duties to access the Office premises on a regular basis (the ones who receive the access card of external contractor) to pass through the security verification process before the access is granted.</p>
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories of persons whose data EUIPO processes are employees of EUIPO's service providers (external resources for EUIPO) who will regularly enter the Office premises (will be assigned a red access card).</p> <p>The following personal data will be processed:</p> <ul style="list-style-type: none">• Name, surname, signature;• Educational and professional background and references (data in CV, diplomas and certificates, etc.) ;• Data in the declaration signed by the company for its employee (external resources for EUIPO) through which the company declares that the external resource does not have pending criminal convictions.
Retention period	<p>The data will be retained for a maximum period of 12 months from the day you have definitely stopped providing services to EUIPO.</p>
Recipients of the data	<p>Different users have access to data:</p> <ul style="list-style-type: none">• EUIPO internal administrators (Head of CSS; Health and Safety Officer) have access to all information for control purposes ;• H&S services provider - 'PREVING Consultores S.L.U.' has access to the information in order to check the completeness of the documentation provide by the companies. <p>Each company has access to the data of its employees in the Portal. In case of subcontracting, the contractor has access to the data of the subcontractor's employees and in some cases may be responsible for the submission of their data.</p> <p>Access to the data can be given to providers of Google for the purposes of Customer support, response, diagnosis and resolution services, incident tracking, responding to customer queries, and technical support.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?	<p>The data of the external resources (excluding the data of the external resources working in construction projects) is sent to the Security verification tool provider who stores it at Google Cloud Platform, Zone europe-west1-b (Ghlin, Hainaut, Belgium) European Economic Area (EEA). The data storage provider is certified in ISO 27001 and applies all necessary physical and IT security measures to protect the data. EUIPO has validated these security measures in the Security risk assessment linked below. It must also be noted that GCP does not have direct access to the information, however, even if not accessible by Google, it could still be transferred outside of the EU as part of the services provided by the subprocessors. Google employs subprocessors from the US, Europe, Asia and India for the purposes of Customer support, response, diagnosis and resolution services, incident tracking, responding to customer queries, and technical support. The full list of subprocessors is located here: https://cloud.google.com/terms/subprocessors. For transfers of data outside of the EU, and in particular for transfers to subprocessors, Google implements model contract clauses. The standard model is located here: https://cloud.google.com/terms/eu-model-contract-clause. Google is also registered in the Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active. -</p> <p>In case of transfer of personal data, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.</p>
General Description of security measures	<p>The security measure applied are as follows:</p> <ul style="list-style-type: none"> • The access to the data in the Portal will be secured through the use of security policy of passwords and users who will have different roles and levels of permissions. As user names are linked with an email address, then users can be a pool of people sharing an account, or single users. Different user profiles will be created, depending of the access to the data. • Access Control system implemented and roles defined to ensure that information can be accessed only by those required to access it. • Data stored at Google Cloud Platform, Zone europe-west1-b (Ghlin, Hainaut, Belgium) European Economic Area (EEA), certified in ISO 27001. • Physical Access control system compliant with CSA CCM v3.0, SSAE-16 / ISAE 3402, SOC 2 Type II. • Full protection at Core Switches with systems IPS and NGFW. Servers with ESET File Security antivirus, with centralized management and automated updates and scanners. • Encrypted communication channels (TLS v1.2 and VPNs) for secure communication of data. • Information is backed up to ensure integrity and availability of the data. • The Service provider carries out monitoring of the systems and periodic penetration tests to ensure that any vulnerability is promptly identified and fixed. • The service provider has an incident management protocol that includes communication of data breaches to EUIPO. <p>More information can be found in the Security Requirements and the Security risk assessment provided by EUIPO.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement security verification of external resources:</p> <p>http://sharedox.prod.oami.eu/share/page/repository?file=Security%20verification_%20PRIVACY%20STATEMENT.doc#x%3Ffilter=path%2FOffice_Docs%2FK%20INST%20AFFAIRS%2FK03%20DP%2FK0305%20DP%20Domains%2FDPC-IBD%2F3%20-%20Records%20IBD%2FRecords%20IBD%2FRecords%20IBD%2FSecurity%20Verification%20External%20Resources</p>
EDPS Prior consultation	YES



Reference number	DPR-2019-007
Name of the processing operation	Organisation and management of meetings and events by EUIPO
Last Updated:	08/06/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Hospitality, Security and Logistics teams (IBD) External processors: Events management service provider Pomilio Blumm and its sub provider for data storage DigitalOcean Security Other service providers involved in the management of events and meetings are as follows: Reprography services provider EULEN; Travel and accommodation services El Corte Ingles; Audio-visual services provider Vitelsa; Security services provider Securitas; The current list of the events management provider's providers can be obtained upon request.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

There are 3 main aspects in the process of support for the organisation of meetings/events, established by IBD:

- organisation and reservation of meetings through the use of Condeco application;
- support for the organisation of events;
- sound, video and audio-visual recording/streaming/photographing of events/meetings.

The processing of personal data in the scope of organising and conducting all types of meetings and events, e.g. meetings and working group meetings of the Management Board and of any networks, as well as all ad-hoc and regular internal and external meetings, in-house and external location meetings, workshops, conferences, seminars, webinars, stakeholder and press events, etc., is regulated by the Data Protection Internal Rules for the Organisation and Management of Meetings and Events.

Personal data processed during organisation of meetings:

All EUIPO staff and external resources who have an IT account (corporate email address) can organise meetings through the Condeco application that is integrated with their Outlook account. During this process the data stored in Condeco is as follows:

- personal data, coming directly from the Outlook active directory, regarding the requestor and the host of the meeting and the internal participants (if applicable);
- other data related to the corresponding meeting (date, duration of the meeting, meeting room, participants invited, additional services requested for the meeting such as tech conference services, catering services, other logistic services).

The information stored in Condeco is as well used for the elaboration of a monthly report regarding the cost of the catering services incurred in each service per person. The report is generated by Business Object (that consults two data bases: Condeco and Allegro) and enables management to provide control on the spending for catering services in meetings and to ensure sound financial management. Catering services send a mail to all heads of service/directors or the people authorised by them to consult the report, in order to inform them that the report is already accessible in Business object. For this purpose Catering services stores a table with personal data (name and email) of the people in all departments authorised to consult the report.

Personal data processed during the support for the organisation of events:

Usually EUIPO staff subscribes for an event organised by a concrete department through the use of the standard event participation form available on Insite (process managed by ICLAD). In the case of trainings organised by Academy, participants usually subscribe through the training module in Allegro. In both cases, once the events participants list is determined, the department requesting and hosting the event/training sends the list to IBD's Hospitality team and events management provider who process personal data as follows:

- in some events, when the events management provider is responsible for the invitation and registration of the participants;
- in all events/trainings, when the provider is responsible for the logistic coordination of the event.

The participation list for each event is:

- stored in Sharedox for the purpose of sound financial management and spending control;
- sent to the department that has initiated its organisation for the purpose of stakeholders management.

If the department initiating the organisation of the event decides that registration should be organised for this concrete event, the events management provider prepares a registration page through its events management platform Metis and sends the link to this registration page to the department or directly to the events participants (depending on the instructions of the department). The contact details of the participants are always provided by the department which initiates the organisation of the event. Apart from the purpose of registration, the Metis tool may be used for the purpose of reimbursements of DSA (daily subsistence allowance) and very rarely for the purpose of payment of paid events by the participants/attendees.

The logistics coordination of the events can include but is not limited to coordination activities before the event



(organisation of the enrolment of participants, coordination of the transport; catering; accommodation; reprography material, technical equipment, etc.), during the event (coordination of the participants' attendance, technical equipment functionality, etc.) and after the event (post event surveys, follow-up activities and keeping records).

Sometimes the logistics coordination of an event includes sending information regarding the event's participants to other services in EUIPO involved in the organisation of an event: security services for the purpose of accesses management; travel agency for the purpose of travel and accommodation arrangements; to the reprography services and to audio-visual services provider for the technical coordination of the event. When information is sent to an external provider, this provider should ensure that has adopted all organisational and technical measures necessary for the compliance with the Regulation (EC) N°1725/2018.

Personal data can be processed as well in the interactive events management application made available to the participants during the event where they can find details about the event and pose questions.

Personal data processed during sound, video and audio-visual recording/streaming/photographing:

Often meetings or events organised by EUIPO are sound-, video- or audio-video recorded and images are taken. The recordings/photographing/streaming can be done by IBD providers (events management provider or audio-visual services provider) or by Communication Services. If the recording/ photographing is done by Communication services, the personal data is processed according to CS DPO Notification - DPN-2018-092.



Purpose of the processing	Personal data are for the purposes of organising and managing the event/meeting, coordinating any required follow-up activities, financial management and communication/transparency purposes.
Data Subjects	Data subjects in this processing operations are: EUIPO staff and external resources who participate in events/meetings and external participants in events/meetings.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The categories of persons whose data EUIPO processes are as follows: EUIPO staff and external resources who participate in events/meetings and external participants in events/meetings.</p> <p>In the process of organisation and management of meetings, the personal data stored in Condeco is as follows:</p> <ul style="list-style-type: none">• for the requester and the host of the meeting: name, surname, email, telephone number, service/department, date and duration of the meeting, name of the meeting room, services requested and consumed/not consumed; incidents (not showing after booking) and in the case of special catering services requested- cost of the services incurred per person.• for the participants of the meeting:<ul style="list-style-type: none">in case of EUIPO staff: name, surname, email and telephone number;in case of external participants: email. <p>Additionally, Catering services stores a table with personal data (name and email) of the people in all departments authorised to consult the catering report in the report management system (heads of service, directors, other authorised staff).</p> <p>In the process of support for the organisation and management of events, the personal data collected could be as follows:</p> <ul style="list-style-type: none">• General Identification data: title, name, surname, Passport/ID information, email, position held, organisation/institution, country, city of departure, bank details, fiscal code and address for reimbursements purposes; mobile phone numbers for communication of key information in case of emergency/crisis situations.• Health- related needs/requirements (e.g. mobility and/or dietary needs), if indicated by the participant. <p>For the purpose of audio/video recording, the personal data collected is as follows: videos/photos, voice, statements, opinions, etc. When the recording, streaming, photographing are done by Communication services, the personal data is processed according to CS DPO Notification - DPN-2018-092.</p>
Retention period	<p>Personal data processed by the Data Controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they will be processed.</p> <p>In the process of organisation of meetings, the time limit for the storage of the personal data in Condeco is up to 5 years from the date of the discharge for the financial year to which the data relates (for the purpose of financial management).</p> <p>Personal data of the staff who consults the special catering services report are stored till they are authorised to access it.</p> <p>In the process of support for the organisation of events personal data (name, surname, bank details, address, titles, signature, email) can be stored for the maximum period of 5 years from the date of the discharge for the financial year to which the data relate (meaning maximum 7 years) for the purpose of financial accountability. The rest of the data is deleted at latest 6 months after the event. The health-related data in Metis is stored for 6 months only if the participants has not withdrawn his/her consent, in which case the data will be immediately deleted.</p> <p>The data in the hard disk of El Corte Ingles (name, surname, dates of stay, flight details) is stored for 5 years for accountability purposes.</p> <p>The data in Amadeus is deleted one week after the date of the flight back.</p> <p>Audio/video recordings and photos are retained till the completion of the requested service, after which they are sent to the department which has requested the service and deleted from the data base of the service provider. The audio/video recordings and photos can be retained by EUIPO for a longer period as described in CS's DPR-2018-092.</p> <p>In case a meeting is to be recorded solely for minute taking purposes, the recording should be accessible to the drafter of the minutes only and be permanently deleted once the final minutes have been adopted.</p>



Recipients of the data	<p>In the process of organisation of meetings, the parties that have access to the personal data stored in Condeco are global administrators (Event management service provider, IT service providers, Tech conference service provider) and group administrators (Tech conference service provider, Event management catering quality controller, Catering service provider manager, designated secretaries in relevant departments) and vendors (tech-conference service provider, catering service provider and event management provider).</p> <p>In the process of support for the organisation and management of events:</p> <ul style="list-style-type: none">• Event management provider (Pomilio Blumm team) and its subcontractors/suppliers, involved in the organisation and management of an event, have access to the personal data;• other services in EUIPO involved in the organisation of an event: security services for the purpose of accesses management; travel agency for the purpose of travel and accommodation arrangements; the reprography services and to audio-visual services provider for the technical coordination of the event.• the parties that have access to the personal data (participants list) stored in Sharedox are Hospitality management team, event management provider (Pomilio Blumm team), vendor management for financial control purposes;• department initiating the event has access to all the data (both in Metis and in Sharedox). <p>In the process of audio/video recording, in principle, the teams in charge of the recording are the only ones to have access to raw audio and video recordings/streaming/photographing processed under the responsibility of the Data Controller. Access to the raw data is restricted only to those that, with explicit permissions, can see the material. When the recordings, streaming, photographing are done by Communication services, the access to the personal data is managed as described in CS&#039;s DPR-2018-092.</p> <p>The service managers that receive the reports regarding the requested catering services are recipients of the data in the process of organisation of meetings through Condeco.</p> <p>All the departments, that have initiated the organisation of the event, are recipient of personal data collected during the event.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>Regarding transmission in EU:</p> <p>Data is transferred to the secure servers of the data storage provider of Pomilio. The data storage provider is ISO 27001 certified and applies all physical and IT security measures in order to protect the data.</p> <p>All suppliers/sub - providers of Pomilio in EU should comply with GDPR. Data protection clauses will be included in the requests for offers sent by Pomilio to its providers. In case of transfer of personal data, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.</p> <p>El Corte Inglés has signed a data protection agreement with Amadeus through which ECI has passed on Amadeus the same obligations as set out in the Contract between EUIPO and ECI. Amadues declares in its Privacy Policy that when personal data is transferred to another country it will continue to receive adequate protection through contractual or other arrangements put in place with affiliates and third party service providers.</p>



<p>General Description of security measures</p>	<p>In the process of organisation of meetings through the use of Condeco tool, the information will be stored in security hardened servers with access control measures and protected by Username and Password. Access to the Condeco tool is restricted by username and password. Authentication and authorisation are based on roles. Servers are physically protected at the Data Processing Centre. Network security is configured to prevent external threats from accessing the servers.</p> <p>In the process of event management through the use of Metis tool: The access to the tool is protected with passwords. The servers of the application are stored in Frankfurt, Germany. Systems are monitored, and information is backed up regularly to ensure that, in case of destruction or loss, data can be restored. Backups of the database and the software are performed weekly. Information is backed up regularly, to ensure recovery in the event of a disaster. Datacentre service provider has 24/7/365 monitoring of their systems, and a status page to verify if there is degraded performance or unavailability. All servers are protected by UPS to ensure continuity in the event of a power failure. There are several security measures applied in order to ensure the integrity of the information. Mainly, there are restricted access controls and centralised logging and monitoring to detect any potentially malicious activity. The database is encrypted using a symmetric key algorithm. Communications are encrypted using SSL3. There are several physical security measures applied in order to ensure that the servers that store personal data are protected: 24/7 Physical security guard services; Physical entry restrictions to the property and the facility; Physical entry restrictions to the co-located data centre within the facility; Biometric readers with two-factor authentication; Secure loading zones for delivery of equipment; Full CCTV coverage externally and internally. Data centre service provider's Security team utilises monitoring and analytics capabilities to identify potentially malicious activity within their infrastructure. User and system behaviours are monitored for suspicious activity, and investigations are performed following an incident reporting and response procedures. The event management provider has established a Personal data breach management procedure (please, consult the link at the end of this record). Data storage provider of Pomilio (DigitalOcean) is: ISO22301:2012, ISO/IEC27001:2005, and ISO9001:2008 certified.</p> <p>For more detail regarding the security measures implemented by the event management provider, please, consult the link provided in the last section of this record.</p> <p>In the process of sound, video and audio-visual recording/streaming/photographing, the access to the raw data is restricted only to those that, with explicit permissions, can see the material therein. For internal administrative meetings the legality, the need and the proportionality of recording (sound, visual and audio-visual), streaming and photographing should be analysed and demonstrated by the controller on a case-by-case basis. Recordings of internal meetings should remain an exception to the rule and the legitimacy, necessity and unavailability of alternative methods (to recording, streaming and photographing) to achieve the same purpose(s) should be properly examined and evidenced by the controller and moreover, prior consulted with the Data Protection Officer.</p> <p>If any of the aspects of the organisation of events and meetings is carried out by a service provider, the Infrastructures and Buildings Department, acting as the data controller for these aspects, will monitor and verify the implementation of the required organisational and technical security measures necessary to ensure compliance with the Regulation (EU) 2018/1725.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy statement for EUIPO staff and external resources working in EUIPO and Privacy statement for external participants :</p> <p>http://sharedox.prod.oami.eu/share/page/repository?file=Privacy%20Statement%20for%20EUIPO%20staff%20participating%20at%20Office%20B4s%20events%20and%20meetings%20_FINAL.docx#filter=path%7C%2FOffice_Docs%202FK%20INST%20AFFAIRS%202FK03%20DP%202FK0305%20DP%20Domains%20FDPC-IBD%202F3%20-%20Records%200IBD%202FRecords%20IBD%202FRecords%20IBD%202FEvents%20and%20meeting%20management</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-008
Name of the processing operation	Management of the Inventory of EUIPO's assets
Last Updated:	21/10/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processors: Head of Facility management Service Team leader of Inventory team Digital Transformation Department (for the purpose of maintenance and configuration of SAP, Inventory module) External processor: Severiano Servicio Móvil, S.A.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The Inventory officers, responsible for the management of the Inventory of EUIPO assets, receive the information regarding the update of EUIPO tangible and non-tangible assets from Remedy. EUIPO IT equipment and furniture dispose of labels that are scanned with a mobile phone application and automatically transferred to the facility management software Rosmiman and SAP. No personal data is stored in the mobile phone application. Only the EUIPO Inventory team and the external provider Severiano Servicio Móvil, S.A. have access to the mobile phone application that is password protected. Personal data is processed in case of: <ul style="list-style-type: none">• assignment of IT assets to EUIPO staff;• assignment of furniture to teleworkers.
Purpose of the processing	The personal data is processed for the following purposes: <ul style="list-style-type: none">• to ensure that the Office can identify the location of all the assets;• to comply with the provisions of EUIPO Financial Regulation concerning management of Inventory.
Data Subjects	EUIPO internal staff and external resources to whom assets have been assigned.
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data processes are as follows: name, surname, personal number, location and the assigned assets.
Retention period	Personal data is stored for as long as an asset is assigned to a concrete person. Only in the section History of the article per user in SAP, the name and surname of the last person to whom an article has been assigned, is stored for a longer period (for 12 months more than the period for which an asset is assigned to a concrete person).
Recipients of the data	Access to the data have the following user groups: <ul style="list-style-type: none">- Inventory team in Facility management , IBD, for control and inventory management purposes;- the external provider Severiano Servicio Móvil, S.A. for the purpose of management of the inventory;- staff of Finance Department who accesses the data in SAP for the purpose of accountability;- staff of DTD who accesses the data in SAP for the purpose of maintenance and configuration of the Inventory module.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data in SAP is stored according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2). <p>The data in the facility management system Rosmiman is stored in secure cloud system that complies with the recognized standard ISO 27001. The data is protected with access control measures and Firewall system. Servers are physically protected at the Data Processing Centre in Madrid, Spain.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement Inventory:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/e9745330-81d0-41d6-bc7d-d5027339e624</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-009
Name of the processing operation	uniFLOW Printing management in EUIPO
Last Updated:	27/02/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Joint Controller organizational entity	Digital Transformation
Joint Controller contact details	Director of Digital Transformation Department EUIPO, Avenida de Europa 4, 03008 Alicante, Spain,
Name and contact details of processor	Internal processors: Digital Transformation Department External processor: Service provider - CANON
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The uniFLOW tool allows EUIPO staff and external resources to use any printer in the Office premises by using their employee access card.</p> <p>The application collects user data, analyses the information on printer usage and generates reports/statistics. Information on the individual printer usage is accessible to all users and enables them to assess their environmental impact.</p> <p>A report regarding the paper consumption at department, service and team level will be sent to EUIPO management and will be as well published on Insite. This report will not contain any personal data.</p>
Purpose of the processing	The purposes of this processing operation are as follows: - keeping track of printer usage statistics; - raise awareness on the environmental impact of the usage of Office printers.
Data Subjects	EUIPO printers users
Description of categories of persons whose data EUIPO processes and list of data categories	Name, Surname, User Login, e-mail, ID Number, Service or Area, Department, Name and Type/Format of File printed (for instance "Excel file", "Picture file" and so on), Volume of pages/sheets printed including Duplex printing, Colour or B&W impressions, Date of printing, Printer ID.
Retention period	Personal data collected will remain in the database and will be deleted no later than 1 year after the anonymised results have been delivered. The anonymous statistic data will be kept according to the EUIPO retention policy.
Recipients of the data	1st Line Canon Technician. Staff member responsible for the project in DTD during the project deployment.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<ul style="list-style-type: none">• Tool will be connected to EUIPO's authentication systems in order to verify the person that is trying to access the information.• Tool includes access control measures to grant or deny access based on the profile of the user that is connecting.• Client-server communication of sensitive data is conducted over an SSL link.• Access to the tool installation is limited to system administrators.• Servers are implemented at EUIPO's CPD so there is no external interaction; personal information is only reachable after authentication.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement UniFLOW printing management: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/21496bd2-8fcf-485a-b59b-0b27145de650
EDPS Prior consultation	NO



Reference number	DPR-2019-010
Name of the processing operation	Data processing in the context of the application form of the Blockathon Forum
Last Updated:	10/03/2020
Controller Organizational entity	Observatory
Controller contact details	Observatory @euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>As a follow-up action of the Blockathon, EUIPO will orchestrate the collaboration of a community of stakeholders from EU institutions, enforcement authorities, industry and academia in the form of a FORUM that will focus on the creation of a definition and a pilot for anti-counterfeiting solutions.</p> <p>Any member of the public can express their interest to join this FORUM through the Observatory website by means of an online application form.</p> <p>EUIPO will collect and store personal data of the website users, including their contributions.</p> <p>The processing is automated as the information is obtained through the online application form.</p>
Purpose of the processing	<p>EUIPO processes personal data in order to allow the users of the new website to raise their awareness on IP and blockchain technology through an interactive platform where they can exchange ideas about the Blockathon event.</p> <p>The overall goal is to create an EU anti-counterfeiting infrastructure based on Blockchain. To implement a step-by-step strategy first forming the Anti-counterfeiting Blockathon Forum to bring together all the relevant public and private stakeholders. Secondly the Anti-counterfeiting Blockathon Forum will work on the development and implementation of an anti-counterfeiting use case and software to achieve interoperability, standardisation and proof of authenticity, both through electronic channels such as e-mail exchange and feedback to questionnaires or physical meetings such as workshops, events and meetings, and other means of follow up on the topic of the use case and the pilot.</p>
Data Subjects	Participants to the Blockathon Forum
Description of categories of persons whose data EUIPO processes and list of data categories	<p>We process the following data completed by the interested user in the FORUM online application form:</p> <ul style="list-style-type: none">• First name & last name• Job title and company name• Introduction line• Industry• E-mail address• Nationality• Industry• Contributions• Credentials



Retention period	<p>Personal data will be kept only for the time needed to achieve the purpose(s) for which it is processed.</p> <p>The documents containing information about the members of the Forum are living documents that are constantly updated. Whenever a person does not wish to continue being part of this network, the data is automatically deleted from the lists.</p> <p>In any case, EUIPO will keep the personal data for the FORUM for a maximum of 2 years.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	The members of the Observatory staff responsible for the administration of the FORUM webpage and the management of the FORUM.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the network members is stored in secure IT applications (e.g. ShareDOX (the document management system) and the HR Portal database) according to the Office's security standards, as well as in specific electronic folders and mailboxes.</p> <p>The database and mailboxes are password protected under a single sign-on system and connected automatically to the user's ID. E-records are held securely to safeguard the confidentiality and privacy of the data therein.</p> <p>Regardless of the stage, everybody dealing with personal data in the context of the networking activities must sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/44960d24-8918-402e-b778-9170ddaf5c3d</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-012
Name of the processing operation	Processing of personal data in the context of the IP Enforcement Forum 2019
Last Updated:	14/03/2019
Controller Organizational entity	Observatory
Controller contact details	Observatory@euipo.europa.eu
Name and contact details of processor	EU Commission and the OECD for access and security purposes.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO is co-organising with the EU commission and the OECD the third International Forum on IP enforcement will bring together key European and international decision makers, enforcement agencies, multinational companies, and other private actors as well as relevant stakeholders to discuss, trends and alternative enforcement techniques for intellectual property both at EU and international level in a prospective and dynamic setting.</p> <p>The participants will register as using the Pomelio webpage used for the registration of participants to EUIPO events.</p> <p>For the post-event communication and information, EUIPO will also take some pictures and make some audio-visual recordings during the Forum.</p> <p>The event will take place at the Organisation for Economic Co-operation and Development (OECD) headquarters in Paris. Personal data of the participants collected by EUIPO, will be transmitted to the OECD for access and security purposes.</p>
Purpose of the processing	The purpose is to collect the details of the participants of the event and speakers needed for the event logistics (dinner, traveling and accommodation of speakers, the access to the OECD building. etc)
Data Subjects	Participants invited to the event.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>We process the following data completed by the interested user in the Forum online application form:</p> <ul style="list-style-type: none">• First name & last name• Organisation or company• E-mail address• ID number (only for speakers)• Representing country (only for government officials) <p>In addition, audio-visual recordings will be made during the event, including while participating in interviews/workshops. If that is the case, images/photos, statements, opinions, etc. may be processed depending on the type of recording and the purpose(s) of the recording.</p>



Retention period	<p>Personal data will be kept only for the time needed to achieve the purpose(s) for which it is processed.</p> <p>In any case, EUIPO will keep the personal data for the Forum for a maximum of 2 years, as the event takes place on a biannual basis.</p> <p>In what refers to photos or audio-visual records, they might be kept for educational, institutional, historic, informational and/or promotional (internally and externally) reasons for a longer period of time if they have been published on the EUIPO intranet, the EUIPO website, or made available via the Office's other social media channels or the learning portal of the Academy. If this is the case, personal data will be limited as much as possible, for example, by keeping only the name, surname, and photographs.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>EUIPO:</p> <p>The members of the Observatory staff responsible for the organisation of the Forum</p> <p>The external providers involved in the event management, such as the registration and the travel agency.</p> <p>EU Commission and the OECD:</p> <p>The team members and providers involved in the event management.</p> <p>In all the scenarios, access to the information is given on a strict need to know basis.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	To the OECD which is a co-organiser of the event. The personal data transferred will only consist of name, surname, organisation or company and -mail address and only for government officials, the representing country.
General Description of security measures	<p>All personal data related to the network members is stored in secure IT applications (e.g. ShareDOX (the document management system) and the HR Portal database) according to the Office's security standards, as well as in specific electronic folders and mailboxes.</p> <p>The database and mailboxes are password protected under a single sign-on system and connected automatically to the user's ID. E-records are held securely to safeguard the confidentiality and privacy of the data therein.</p> <p>Regardless of the stage, everybody dealing with personal data in the context of the networking activities must sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/22bfc177-de33-4d8b-8175-bde271b19404</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-013
Name of the processing operation	Processing personal data within the framework of the renewal of temporary and contract agent's contracts at EUIPO
Last Updated:	16/01/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the renewal of temporary and contract agent's contracts at EUIPO.</p> <p>There is a need for EUIPO to provide flexibility in the workforce due to the variations in terms of increase or decrease in the activities of EUIPO generated by the market situation and the behaviour of industry towards Intellectual Property, while ensuring a balanced budget to which the Office as a self-financed agency is fully committed.</p> <p>Data processing operations for renewal of staff member's contracts are conducted by authorised staff of Human Resources Department (HRD) who proceeds to an individual assessment of each particular case.</p> <p>For the first renewal procedure, HRD performs an analysis of the file and of the recommendation sent by the jobholder's Director (or delegated person). For the second renewal procedure for temporary agents, HRD establishes a list of staff members proposed for renewal or non-renewal.</p> <p>Data mentioned in point 2, as well as supporting documents (such as expression of interest of the jobholder, the recommendation of his/her Director or delegated person), are presented to the Authority Authorised to Conclude Contracts of employment (AACC) and/or subdelegated authorities for preliminary analysis. The AACC then informs the jobholder about its envisaged decision, send him/her all the documents at its disposal, and invites him/her for comments within a deadline. The final assessment and decision is taken after that deadline, upon reception or not of comments.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>



Purpose of the processing	<p>The purpose of processing data is to enable EUIPO to take decisions about renewal of working contracts for temporary and contract agents within the framework of the workforce management in EUIPO.</p> <p>The personal data are collected and processed in accordance with:</p> <p>Temporary agent contract</p> <p>Article 2(f) of the Conditions of Employment of Other Servants of the European Union (CEOS) provides a type of engagement for temporary agent specific to agencies of the European Union. Article 8 CEOS constitutes the relevant provision for the renewal of temporary agents referred to in Article 2(f):</p> <ul style="list-style-type: none">- First renewal: based on Article 8 CEOS, EUIPO's staff policy establishes the standard term of contract for temporary agents under type of contract Article 2(f) CEOS as fixed period of 5 years. The contract may be renewed for a further period of 5 years;- Second renewal for indefinite period: Article 8 CEOS stipulates that any further renewal of a temporary agent contract concluded under Article 2(f) CEOS shall be for an indefinite period. On that basis, EUIPO has established a procedure for the second renewal of those contracts. <p>Contract agent contract:</p> <p>Article 3(a) CEOS foresees the engagement of contract staff. Article 85 CEOS constitutes the relevant provision for the renewal of contract agents referred to in Article 3(a). Based on Article 85 CEOS, the Office employs contract staff to address a variety of needs, including temporary needs related to specific projects. The Office applies the policy of a 5 year fixed term contract renewable for a further period of 5 years.</p> <p>The procedure which applies to the first renewal of contracts is detailed in the QSD-0060 Work instruction (First Renewal or Non-Renewal of Contracts of Temporary or Contract Agents, published in Insite). This Work Instruction is referred to in the Guidelines for the renewal of temporary agent contracts at EUIPO, also published on Insite.</p> <p>The procedure which applies to the second renewal of temporary agent's contracts is detailed in these Guidelines.</p>
Data Subjects	EUIPO staff members : Temporary and Contract agents
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <ul style="list-style-type: none">- Identification of the data subject (full name, personal number);- Type of contract, duration, job title, function group, grade, statutory link, job assignments (current and past, including in other Institutions/Agencies);- Performance of the jobholder (appraisal reports by the jobholder's Director (or delegated) and HRD authorized staff for first renewal procedure and only by HRD authorized staff for second renewal procedure);- The talent and competency profile of the jobholder which could be compared with the needs identified in the Office;- For the assessment of the first renewal of contract: the recommendation of the jobholder's Director or delegated person with the reasons for renewal or non-renewal of the contract and its supporting documents (e.g.: appraisal reports, emails, letters and notes);- The specific situation and interests of the jobholder; for the second renewal procedure, it is put forward on his/her expression of interest.



Retention period	<p>Working documents in electronic and paper data (emails, letters, notes) used for the assessment of each individual case, as well as all letters/notes exchanged between the Authority Authorised to Conclude Contracts of employment (AACC) and the staff member concerned by a renewal of contract are kept up to a maximum of 5 years after decision of the AACC about the renewal or non-renewal of the contract.</p> <p>Working documents may be kept beyond 5 years in case of complaint and further judicial procedure. In that case, all documents are kept until the end of the judicial procedure.</p> <p>The renewed contract is kept in the staff member's individual file for the same duration as these files (8 years after the expiry of all rights of the person concerned and of any dependents and for at least 120 years after the date of the birth of the person concerned).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Authorised staff of HRD working with these files and the AACC. The data is also accessible to the HRD management, authorised staff of the Cabinet and the jobholder's Director or delegated person.</p> <p>Other recipients on a strict need to know basis: Authorised staff of Finance Department and PMO (only to the extent necessary to process remunerations/or sickness insurance).</p> <p>External staff (IT administrators) could have access to the data, if necessary for technical reasons. EUIPO's contractors and subcontractors might also have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>Paper files: The storage is done only in locked cupboards kept by HRD. Access is limited to authorised HRD staff members working with these files.</p> <p>Electronic files: Personal data are stored in secure IT applications (ShareDox, HR "Allegro" and "SAP SuccessFactors") according to the security standards of EUIPO as well as in specific electronic folders accessible only to authorized persons working in the files.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein. Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data for the renewal of temporary and contract agent's contracts at EUIPO: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/fcd7e271-176b-47bd-9af2-9f9c91c9aa8c
EDPS Prior consultation	NO



Reference number	DPR-2019-016
Name of the processing operation	School and University Visits
Last Updated:	13/03/2019
Controller Organizational entity	Academy
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	EUIPO Infrastructure and Buildings Department as internal processor. ibddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Once the visit requested is approved, Academy contacts the teacher by email to organise the details of the visit. Academy requests that the teacher sends an email containing: Name of the school or university Full name and ID number of the students Full name, ID number and e-mail address of the teacher This list is sent by email to Security Services (IBD) with copy to Academy. This list is an MS Excel file; this list is used with the sole purpose of granting access to the EUIPO premises where the visit takes place in accordance with DPR-2019-007.
Purpose of the processing	Processing the participants' personal data is necessary to <ul style="list-style-type: none">• allow entrance to EUIPO premises• to keep track of how many people are in the building for evacuation purposes• to report on the number of university/school visitors
Data Subjects	School and university students and teachers
Description of categories of persons whose data EUIPO processes and list of data categories	EUIPO receives the following personal data from the schools /Universities: Name, surname, ID number of students and teachers from school /University attending the event. In addition, the e-mail address of the teacher. The name of the school or university is also gathered.
Retention period	The personal data transmitted to the EUIPO by the teachers will be deleted immediately after the event has ended. The information regarding: name of the school, name and address of the teacher, and how many students attended from the different schools/universities will be kept in an excel sheet in Sharedox for each calendar year. Personal data will be deleted yearly (every September). The excel sheet without personal data will be deleted every two years (every September).
Recipients of the data	1. EUIPO Academy receives personal data from school / University. 2. Selected EUIPO Academy staff has access to Excel table in Office's tool Sharedox. 3. Infrastructures and Buildings Department Security receives data to allow access to EUIPO premises.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	All personal data related to the school/ University visit is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Schools and Universities Visits Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/c54b27a0-0ac1-44f5-825d-54b88bd6283b
EDPS Prior consultation	NO



Reference number	DPR-2019-017
Name of the processing operation	Organisation of the access of IBD staff/resources to the installations of other organisations/authorities/companies.
Last Updated:	01/03/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: IBD secretariat (FM secretariat for visits of FM teams and CSS secretariat for the visits of CSS teams).
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	For the purpose of exchange good practices and knowledge sharing, in the framework of the department's projects and activities, IBD secretariat may organise the access to installations of other organisations/authorities/companies. The collection of the data is via email or by telephone. The data is stored in the personal computer of the FM/CSS secretary or in Sharedox and is sent to the organisation/authority/company where the visit will take place via email.
Purpose of the processing	The purpose of the processing operation is to organise the physical access to premises of organisations/companies/authorities which IBD staff will visit in order to exchange best practices and knowledge/know-how.
Data Subjects	IBD staff and external resources
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data processed is as follows: Name, surname, Passport/DNI number.
Retention period	The data is retained till the visit (or the last visit of the series of visits organised for the concrete purpose) has finished.
Recipients of the data	IBD secretariat (FM secretariat for visits of FM teams and CSS secretariat for the visits of CSS teams). The data is received by the corresponding organisation/authority/company where the visit is foreseen.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	Data is transferred to companies in Spain which comply with GDPR. In the mail with with the data is sent, the company is reminded to delete the data after the end of the visit.
General Description of security measures	All personal data related to this process is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/412d75b0-12d9-4550-8237-ba26d9a1fbff
EDPS Prior consultation	NO



Reference number	DPR-2019-018
Name of the processing operation	Processing of personal data in the procedure of management of office material requests
Last Updated:	21/02/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Contact: Director of Infrastructures and Buildings Department, EUIPO ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processor: Logistics team, IBD All EUIPO staff and external resources External processor: SPI ALICANTE S.L.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Only authorised people in EUIPO can request office material through the use of a dedicated web portal: http://www.spi.com.es . No personal data will be saved on the servers of this web portal . Each person authorised to request material will be given a reference number that will be saved in the web site for requests. This reference number will be associated in the management portal of the service provider with the EUIPO location number and the department of the people authorised to request material. The processing of the location number is necessary in order to ensure that the person will receive the requested material at his/her office. The name of the department is necessary for the purpose of elaboration of statistics and reports with aggregate (anonymous) data. EUIPO logistics team will maintain a list of the people authorised to request office materials that contains their name, office phone number and email address. The list will be published on Iniste at the Logistics page dedicated to Office materials´ in order to be visible for all EUIPO staff.
Purpose of the processing	Personal data is processed in order to ensure the timely delivery of the material to the corresponding authorised person in each EUIPO department.
Data Subjects	All EUIPO staff authorised to request office material
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data processed is name, surname, location number, email address, office phone number and the department of all people authorised to request office materials. IBD logistics and EUIPO staff and external resources with EUIPO IT account process all personal data listed above. The external provider of office material processes only the location number and the name of the department of the people authorised to request office material.
Retention period	Personal data (location number) in the system of the provider will be kept for the period of the contract between the provider and EUIPO. Personal data in the document management system of EUIPO will be kept only for the period for which the person is authorised to request office materials.
Recipients of the data	IBD logistics and EUIPO staff and external resources with EUIPO IT account have access to all personal data listed above. The external provider of office material has access only to the location number and the name of the department of the people authorised to request office material.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the requests for office material is stored in secure program of the provider as follows:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• On spot Physical protection measures ensured. <p>Part of the data is as well stored in a EUIPO IT application according to the security standards of the Office. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre:• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/381b1e5c-fe58-4088-8a6c-a404bd02d322</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-019
Name of the processing operation	Maintenance management in Rosmiman
Last Updated:	25/05/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Head of Facility management service, IBD Maintenance team leader in Facility management service (FM), IBD External processors: Maintenance service provider (Ferrovial Servicios S.A.) Cleaning service provider (Ferroser Servicios Auxiliares S.A.) IDASA sistemas (provider of ROSMIMAN® IWMS Global Site) and its subcontractor Acens Technologies, S.L.U. Facility management service provider (IDOM)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The management of incidents in EUIPO is done through the Remedy09 tool. The information about the incidents/requests related to the maintenance of EUIPO installations (including cleaning) is automatically passed from Remedy09 (My service desk) to the maintenance management tool (currently Rosmiman). These incidents/requests are treated by Infrastructures and Buildings department´ service providers: <ul style="list-style-type: none">• Maintenance service provider for incidents related to maintenance of EUIPO installations;• Cleaning service provider for incidents related to cleaning of EUIPO installations.
Purpose of the processing	The personal data of My service desk users (EUIPO staff and resources) is collected and processed in the ROSMIMAN® IWMS tool for the following purposes: <ul style="list-style-type: none">• in order for the maintenance operators to be able to locate the incident and resolve it in due time thus ensuring the quality of the service provided and the staff satisfaction with the workplace;• to ensure the follow-up on the maintenance requests;• to maintain a history of resolutions implemented in order to improve/correct the solution in the event of reoccurrence of the incident;• to keep the historical data of every location, independently of the occupant.
Data Subjects	The users of the maintenance/cleaning products in My service desk.
Description of categories of persons whose data EUIPO processes and list of data categories	Identification data of My service desk users (EUIPO staff and external resources) as follows: name, surname, technical location, office email and telephone number.
Retention period	The personal data (except for the technical location) is kept for the maximum period of 5 years (the time in which a staff member usually remains at the same location) as it is required for operational purposes to maintain the information related to the requester in order to improve/correct the solution proposed to him/her when the incident reoccurs. The technical location and the incident´s details will be deleted from the tool at the end of the contract with the tool provider but will be kept by EUIPO because the controller needs to keep the historical data of every location, independently of the occupant.



Recipients of the data	<p>The following users have access to the personal data:</p> <p>1) For control and supervision purposes: Facility management internal team in IBD and the external provider IDOM have access as follows:</p> <p>Operator profile Access right type Maintenance Management operator Read Space Management operator Read Inventory operator Read Administrator Full Access</p> <p>2) In order to resolve the incidents/requests: Maintenance service provider Ferrovial Servicios S.A. and Cleaning service provider Ferroser Servicios Auxiliares S.A.</p> <p>The application administrators will be EUIPO staff. ROSMIMAN tool provider (IDASA sistemas) can access the data only under previous authorisation of EUIPO.</p> <p>When external audit companies are auditing the maintenance process in EUIPO, they are given as well access to the data.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>Information is sent to the Rosmiman platform of the Service provider, located in Madrid. The service provider is ISO 27001 certified in order to ensure the secure management of personal data.</p> <p>The security safeguards implemented are included in section 3 of the document "Rosmiman - DTD Security Requirements"</p>
General Description of security measures	<p>All personal data related to the procedure of management of the maintenance/cleaning services in EUIPO is stored in secure cloud system that complies with the recognized standard ISO 27001.</p> <p>The data is protected with access control measures and Firewall system. Servers are physically protected at the Data Processing Centre in Madrid, Spain.</p> <p>For more information, please, consult Acens Infrastructure Annex and Security requirements Rosmiman.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/dc76a0d8-922b-4479-b807-e2be7e45e99b</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-020
Name of the processing operation	Statistics, publications and communication of user's data
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Generation and public communication of statistics in relation to (electronic and non-) e-business relating to Trademarks and Designs owners and representatives (users) for internal use and external communication, including users' suggestions. The above statistics are to be generated in respect to the following users: <ul style="list-style-type: none">• TOP 100 representatives (only representatives, no direct filers) with more than 20 EUTMs e-filed (>20) in the past quarter including their classification performance;• TOP 25 e-users (only representatives or groups of representatives) using e-filing for 99% or more for their overall EUTM/RCD direct applications and oppositions + e-communication activated + a cumulative volume of e-filings. However, just TOP 25 (volume) are presented in the ranking;• Statistics on paper filings (only representatives or groups of representatives) using paper filing (non e-filing) for more than 12% of their overall EUTM/RCD direct applications and oppositions + a cumulative volume of paper filings. However, just TOP 25 (volume) are presented in the ranking.
Purpose of the processing	The purposes of the processing are: <ul style="list-style-type: none">• production of communications and publications of statistics for internal and external reporting• promotion of e-communication strategy, increase of e-communication and further reduction of paper share.
Data Subjects	Users of EUTM/RCD systems, applicants/owners and/or representatives, being natural persons identified or identifiable.
Description of categories of persons whose data EUIPO processes and list of data categories	Data subjects: Users of EUTM/RCD systems, applicants/owners and/or representatives, being natural persons identified or identifiable. Data categories: <ul style="list-style-type: none">• First name• Last name• Company name• Country• Number, type and means (electronically or not) of EUTM/RCD related proceedings filed• % of EUTM/RCD fast track applications• % of EUTM/RCD applications auto classified• % of HDBs expressions used• Timings on classification handling• User area usage (User e-com status)• User (natural persons) suggestions/feedback• E-mail address of the suggestion/feedback contributor (natural person)



Retention period	<p>Personal data are kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>The data will be only retained for a maximum period of 5 years in accordance with EUIPO Strategic Plan time framework.</p>
Recipients of the data	<p>Outside the Office: All internet users connecting to Office's or ETMDN webpages, be individuals or public and private entities, as for example, IP rights owners, representatives, IP information providers, National IP Offices, etc., both EU, as well as non EU sited.</p> <p>Inside the Office: Office's responsible staff from CD and CGS.</p> <p>Internal processor: Name, position: Head of Service Organizational entity: Customer Management Service</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to Statistics, publications and communication of user's data is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/Statistics_publications_communication_of_users_data_en.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-021
Name of the processing operation	EUIPO User Area
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euiipo.europa.eu
Joint Controller organizational entity	Digital Transformation
Joint Controller contact details	1. EUIPO, Director of the Operations Department ODDPC@euiipo.europa.eu 2. EUIPO, Director of the Digital Transformation Department DTD-EUS@euiipo.europa.eu
Name and contact details of processor	External processor: Name, position: IECISA-ALTIA Organizational entity: DTD Operations service provider
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The User Area is the Office's principal means of electronic communication as defined in Decision EX-17-4 of the Executive Director of the Office of 16 August 2017 concerning communication by electronic means. It can be accessed exclusively through the Office's Website.</p> <p>The User Area enables users to:</p> <ul style="list-style-type: none">• submit applications and perform other actions related to EUTMs and RCDs;• upload, view, print, save and send electronic documents and notifications to the Office;• receive, view, download, print and save electronically generated documents and notifications sent to them by the Office;• view a list of all their past and present files with the Office;• manage all their personal information (address, phone, etc.);• manage a personalised alert system;• manage their current accounts with the Office. <p>To access the User Area and the services thereof, users need to create an online account on the Office's website and submit a certain number of details, some of which constitute personal information insofar as they relate to individuals. If the user has already applied for a European Union trade mark or a registered Community design before and provide his/her owner ID upon registration, some of the required information will be directly imported from the PER database. Information submitted by the user is processed by the EUIPO Portal (of which the User Area is a part of) and its associated Back Office. In addition, any information that will be made available through eSearch will be indexed by this tool.</p> <p>Details of the users (in particular, email addresses and phone numbers) will also be used to send IP-related information (e.g. news on trade marks or designs, invitations to seminars, workshops, etc.), promote EUIPO initiatives and conduct survey campaigns.</p> <p>More information about the User Area can be found here: https://euipo.europa.eu/ohimportal/en/user-area</p>
Purpose of the processing	<ul style="list-style-type: none">• To identify the holder of the account and provide him/her with the above-mentioned services through the EUIPO User Area.• To promote the European Union trade mark and the European Union design systems
Data Subjects	<ul style="list-style-type: none">• EUTM/ RCD applicants and owners• Representatives• Website users



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects:</p> <ul style="list-style-type: none">• EUTM/ RCD applicants and owners• Representatives• Website users <p>The categories of the data processed are:</p> <p>Identification data:</p> <ul style="list-style-type: none">• username• owner ID• email address• first name and last name• nationality• address• correspondence address• post code• town/city• country• telephone number• fax number <p>Others:</p> <ul style="list-style-type: none">• login history• communications with the Office
Retention period	<p>Personal data is only kept for the time necessary to achieve the purpose for which it is processed.</p> <p>The time limits for storing data are indefinite (for reasons of legal certainty), as foreseen by Article 111(9) EUTMR and Article 7(1) of Decision No EX-14-3 of the President of the Office.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process</p>
Recipients of the data	<ul style="list-style-type: none">• The DTD Operations service provider for the administration and management of EUIPO systems• EUIPO IP examiners from OD in charge of updating users' data through back office tools such as the PER Database <p>User Area is not available to general public and access to it is restricted. Only EUIPO staff dealing with IT maintenance and management of user interactions might have</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>The User area is protected by the following security measures:</p> <ul style="list-style-type: none">• Access is restricted by username and password, with password complexity requirements.• Authorization mechanisms implemented to ensure that information is only visible to the specifically authorized users.• Security measures at the network perimeter to prevent unauthorized access.• All information transmitted via the internet is encrypted <p>Information stored in EUIPO systems is protected by the following Security measures:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access all EUIPO systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Center.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy statement: https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/User_Area_en.pdf</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-022
Name of the processing operation	Acknowledgement of receipt of fines related to traffic infringements
Last Updated:	01/03/2019
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Contact: Director of Infraestructuras and Buildings Department, EUIPO ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Head of Common services, Logistics team leader in IBD, Security officer in IBD, ED Secretariat External processors: Mail Distribution and Internal mail services provider (EULEN) Only in case the data subject is an external driver (an employee of the external transport services provider), data is as well processed by the external transport services provider Serranica.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Human Resources Department sends to the Head of Common services in Infrastructures and Buildings Department (IBD) all letters of the Spanish authorities related to infringements done with the official vehicles of EUIPO. The Head of Common services controls the whole procedure of acknowledgement of receipt of fines related to traffic infringements done with EUIPO official vehicles. For this reason, the Head of Common services sends the letter to the responsible in the Logistics team who checks who has driven the vehicle at the time of the infringement using the available information in his Outlook. In case the offender is an internal driver of EUIPO or an external driver authorised to drive the official EUIPO vehicle, he is informed about his/her obligation to sign the acknowledgement of receipt and to send it to Mailroom. In case there is any contradiction between the information found in Outlook and the information given by an internal driver who has received the acknowledgement of receipt, the Logistics team leader should request from the Security officer who has access to the key management software to check the information stored there regarding the keys to EUIPO vehicles (who has taken the keys on the concrete date). All the necessary measures are taken in order to ensure that the personal data of the offender is kept confidential: • the acknowledgement of receipt should be in a sealed envelope; • only the subject of the letter (acknowledgement of receipt of a fine) and the reference number of the acknowledgement of receipt will be written on the envelope; • it is recommendable to use the Internal distribution services to send the letter back to Mail room. In case the vehicle is assigned to the Office top management and the controls in Outlook prove that the official driver was not driving the vehicle at the time of infringement, the fines are forwarded to ED Secretariat who furtherly sends the acknowledgement of receipt to the Mailroom in a sealed envelope as described above. In special occasions and only after previous authorisation of the Logistics team leader or directly IBD management, an external driver can be given the permission to drive an official vehicle of EUIPO. In such cases, the Logistics team leader sends the letter of the Spanish authorities to the transport services provider which is responsible to: • check who has driven the vehicle at the time of the infringement and • send to the Logistics team leader the signed acknowledgement of receipt in a sealed envelope on which only the subject of the letter and the reference number of the receipt is written.



Purpose of the processing	The purpose of the processing operation is to ensure the compliance with the Spanish Traffic Code and more in concrete with the obligation of the titular of the vehicle to provide to the responsible authorities the data of the person who has committed the infringement.
Data Subjects	The data subjects are all EUIPO staff members authorised to drive Office vehicles and only in special occasions and after previous authorisation- the external drivers employees of the transport services provider.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data subjects are all EUIPO staff members authorised to drive Office vehicles and the external drivers authorised to drive EUIPO official cars.</p> <p>The data processed is name of the person, vehicle model and plate number, details of the transport (date, hour, route), details of the infringement.</p>
Retention period	<p>The data is processed only for the time necessary for the completion of the purpose of the processing operation- in order to identify the person who has committed the infringement and ensure its data is sent to the Spanish authorities.</p> <p>The data in the key management system is stored for 3 months.</p>
Recipients of the data	<p>The following people have access to the data of the internal drivers of EUIPO:</p> <ul style="list-style-type: none">• Head of service of CSS;• IBD Logistics team leader in order to check in Outlook who has driven the vehicle at the moment of the infringement;• Security officer in order to check in the keys management system who has taken the keys of the vehicle from the key cabinet;• representatives of the Spanish authorities who have issued the fine. <p>The following people have access to the data of EUIPO top management:</p> <ul style="list-style-type: none">• ED Secretariat in some limited cases as described in the previous section;• representatives of the Spanish authorities who have issued the fine. <p>The following people have access to the data of external drivers:</p> <ul style="list-style-type: none">• the external transport services provider Serranica only in case the data subject is an external driver;• representatives of the Spanish authorities who have issued the fine.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>Data is transferred to the competent Spanish authorities which have issued the fine. The following necessary measures are taken in order to ensure that the personal data of the offender is kept confidential:</p> <ul style="list-style-type: none">• the acknowledgement of receipt sent to the Mailroom of EUIPO should be in a sealed envelope;• only the subject of the letter (acknowledgement of receipt of a fine) and the reference number of the acknowledgement of receipt will be written on the envelope;• it is recommendable to use the Internal distribution services to send the letter back to Mail room. Mailroom sends it to the Spanish authorities.



General Description of security measures	<p>The personal data regarding the infringement is stored on paper in the acknowledgement of receipt that is sent to the Mailroom in sealed envelope through Internal Mail by the person who has committed the infringement or by the Logistics team leader (in case the infringement has been committed by an external driver).</p> <p>All personal data in the key management software is stored according to the security standards of the Office as follows:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2). <p>The following necessary measures are taken in order to ensure that the personal data of the offender is kept confidential:</p> <ul style="list-style-type: none">• the acknowledgement of receipt sent to the Mailroom of EUIPO should be in a sealed envelope;• only the subject of the letter (acknowledgement of receipt of a fine) and the reference number of the acknowledgement of receipt will be written on the envelope;• it is recommendable to use the Internal distribution services to send the letter back to Mail room.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/12d7e2c0-5e02-40c9-b6f9-d2247f650a81
EDPS Prior consultation	NO



Reference number	DPR-2019-023
Name of the processing operation	Recruitment of officials by transfers or available reserve lists established by EPSO (paragraph 3.1 of the Framework for the Workforce Management in the Office)
Last Updated:	15/05/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of the Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the scope of the recruitment of officials by transfers or available reserve lists established by EPSO (paragraph 3.1 of the Framework for the Workforce Management in the Office).</p> <p>The Office reserves a number of permanent posts for the recruitment of officials in area of support where there is a need to benefit from the specific expertise of EU officials. These recruitments will be done either by way of transfers or by making use of available reserve lists established by EPSO.</p> <p>Following the paragraph 3.1 of the Framework for the Workforce Management in the Office on recruitment of officials for needs related to support functions, the data processing is used to examine the information received from the EUIPO temporary and contract staff with regard to:</p> <ul style="list-style-type: none">- their administrative status in other Institutions/Agencies;- their participation in EPSO competitions <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	Any personal data supplied by the temporary and contract staff members is processed solely for administrative purposes and for the efficient implementation of the procedure described in paragraph 3.1 of the Framework for the Workforce Management in the Office in accordance with the rules of the Staff Regulation (SR), the Conditions of Employment of other servants (CEOS) and with EUIPO administrative decisions.
Data Subjects	EUIPO's temporary and contract agents having the administrative status of officials in another Institution / or whose name is on an available reserve list for officials established by EPSO.
Description of categories of persons whose data EUIPO processes and list of data categories	The following data are processed only on need to know basis and by authorized staff of HRD: <ul style="list-style-type: none">- full name, personal number, reference of the EPSO reserve list and its date of validity;- administrative status in another Institution/ Agency, function group and grade.
Retention period	Data will be kept for a period no longer than 5 years. In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.



Recipients of the data	<p>Access to this data is determined by strict rules and is based on the needs of the procedure.</p> <p>Other than the concerned person's access to his/her own file, access to data is given to the Appointing Authority/Authority Authorised to Conclude contracts and the authorised staff of the Human Resources Department in charge of processing the data.</p> <p>External staff (IT administrators) could also have access to the data, if necessary for technical reasons.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member; line manager, director, reporting officer or IT-technician.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement on processing of personal data within the scope of the recruitment of officials by transfers or available here:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/77c1b39a-3410-40b3-ad96-893f550f01b5</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-025
Name of the processing operation	Follow-up of individual production and timeliness
Last Updated:	10/09/2019
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Joint Controller organizational entity	Customer
Joint Controller contact details	CDLegalDPO&FraudCoordination@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Measuring the quantity and timeliness of decisions drafted and tasks performed by the staff members of the operational departments.</p> <p>The summaries of production data by individual are made available through a system console ("Kibana") that will be accessible to each examiner at all times. The list of decisions or tasks measured is reviewed before the beginning of every appraisal exercise and is duly communicated to the staff whose activities are to be monitored. The console allows for:</p> <ul style="list-style-type: none">• individual examiners to follow-up on their own production (number of tasks closed or decisions notified);• team leaders to monitor the production of their team (number of tasks closed or decisions notified) as a whole and of individual examiners;• heads of service to monitor the production of the entire Service (number of tasks closed or decisions notified)• director to monitor the production of the entire department (number of tasks closed or decisions notified) <p>All the production data used for measurements are extracted from the relevant IT application. The data processed using the EUIPO applications are currently stored in different production databases such as the EUIPO Website and eBusiness systems, IP Tool, Madrid Protocol System (MPS), RCD (Eurodesign), Euroclass, EuroNice, Common Payment System (CPS), Classification, Template Manager (COR), SEARCH, Madrid Protocol Communication (MPC), Person Module (PER), Publications (PUB), Language Checker (LCT), QFMan, FileNet, Document Access Service (DAS), UQCT, e-Platform, SAP and Allegro.</p>
Purpose of the processing	<p>The purpose of this activity is, on one hand, to monitor the global outputs of the Office in relation to the Office's service standards (including the timeliness service standards), and, on the other hand, to use these objective criteria - quantity and timeliness – as one of the elements taken into consideration for the appraisal report of the data subject concerned, as well as of the respective management responsible.</p> <p>Information collected will be compared with established reference numbers and established procedures for the appraisal.</p> <p>Such production and timeliness management system must be carried out in order to measure the production and timeliness of the concerned staff taking into account all the other relevant factors.</p> <p style="text-align: right;">In addition, the summarised data will be provided to the Performance Experts to be used to guarantee the production of the Office corporate tools.</p>
Data Subjects	Examiners from the operational departments



Description of categories of persons whose data EUIPO processes and list of data categories	<p>We process the following data related to tasks and decisions taken by examiners in the operational departments:</p> <ul style="list-style-type: none">• the identification of the file concerned• the type of decision or task counted and measured• the date when the decision or task was allocated to the data subject• the date when the decision or task was executed in the system• the date when the decision or task was due• if the decision or task was completed in due time (timeliness)• the outcome of the decision or task• the organisational unit (service/team) where the decision was taken or the tasks performed• the name, user name and/or other identifier of the data subject who produced the decision/performed the task.
Retention period	<p>All production data and the personal data relating to trade marks and designs examination is stored in the back office tools for an indefinite period.</p> <p>The summaries of production data by data subject shall be kept for no more than two years after the end of the appraisal period in order to allow the management to use the data for the appraisal of the staff members concerned, and the latter to exercise their rights as provided for in the internal rules on appraisals and/or in Article 90(2) SR. After this period, all individual data extracted in electronic form shall be deleted and no longer archived, and all other copies in any form shall be destroyed, unless they need to be kept longer to establish, exercise or defend a right in a legal claim pending before the court.</p>
Recipients of the data	<p>Access to the relevant EUIPO databases will be granted to:</p> <ul style="list-style-type: none">• Director, deputy director/s, Heads of Service and Team Leaders• Quality, Performance and Risk Officers and Internal Control Correspondents from the concerned Departments;• duly authorised Governance and Performance experts from the Corporate Governance Service and experts (database administrators, data mining) from the Digital Transformation Department. <p>The summaries of production data per data subject will be accessible to:</p> <ul style="list-style-type: none">• the data Subject's Director, Deputy Director, Head of Service and Team Leader;• the Head of Service in charge of Corporate Governance• the Quality, Performance and Risk Officers and Internal Control Correspondents/Data Miners responsible for preparing the data for the hierarchy of the Departments. <p>The information concerning individual production and timeliness will only be shared with people necessary for the implementation of such measures on a need to know basis. The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The standard security measures of the EUIPO Information Systems are applied:</p> <ul style="list-style-type: none">- EUIPO username and password required in order to access EUIPO network and systems.- Authentication and authorization based on roles.- Authentication and authorization at server level, no anonymous access allowed.- Server is physically protected at the Data Processing Centre.- Logical security hardening of the servers.- Network security configured to prevent external threats from accessing the mail servers.



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on follow-up on individual production (volumes and timeliness): http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/7c0cbc41-ac95-41e3-8f46-95feb2bb437e
EDPS Prior consultation	YES



Reference number	DPR-2019-027
Name of the processing operation	STAKEHOLDER QUALITY ASSURANCE PANEL AUDITORS ("SQAP")
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euiipo.europa.eu.
Name and contact details of processor	<p>External processors (external service providers):</p> <ul style="list-style-type: none">- Pomilio Blumm Ideas Company which provides event organisation/coordination services. The SQAP carries out several audit events a year.- Viajes El Corte Inglés S.A. for the travel agency services ("El Corte Inglés") which provides event services and travel/accommodation arrangements. <p>There are 2 framework agreements in place between EUIPO and Pomilio Blumm , and El Corte Inglés which contain the Office's standard data protection clauses in accordance with Article 23(2).</p> <p>The data processing (or any part of it) is not further subcontracted to any other third party by the Office or by our external service providers.</p> <p>Please note that Pomilio Blumm and El Cortes Inglés may work with airline and hotel companies for travel and accommodation arrangements, but these third parties will not be considered as Processors under current applicable legislation and for the purposes of this notification. The event application Metis is owned and managed by Pomilio Blumm.</p> <p>In principle, the processing carried out by the Controller and the Processor takes place in EU only. However, if the data subjects are located outside of the EU, there might be a processing taking place outside of the EU. However, this transfer would be covered under one of the derogations set out in article 50 of Regulation (EU) 2018/1725, in particular in its point (c): "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject".</p> <p>Nevertheless, the above are to be exceptional cases related mainly to travel arrangements for the data subjects, which will be consulted case by case with the DPO and the data subjects are to be duly informed on the said.</p>
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

The Office strives for the highest quality of its products. A solid quality assurance framework has been implemented by President's decision No ADM-14-51, which is the basis for introducing external ex post quality audits, bearing in mind the objectives for continual improvement ("Office Product Quality Framework").

This quality assurance architecture is dependent on both the current ex post and ex ante quality audits, complementing each other and working harmoniously with all the relevant participants (currently Corporate Governance Service (CGS), Customer Department (CD), Operations Department (OD), International Cooperation and Legal Affairs Department (ICLAD) and Boards of Appeal (BoA)). As defined in President's decision No ADM-14-51, the Office Product Quality Framework (in which Stakeholder Quality Assurance Panels is included) will be governed by the following bodies: the Knowledge Circle on Quality (KCQ), who will report to the Quality Board, the top management board responsible for quality matters.

SQAP project is part of the line of action 5 "Enhance customer-driven quality services" of the SP 2020. SQAP will allow integrating the perspective of the Office's user into our quality system, and ultimately in the way we work. SQAP is about our users and their perception of our products' quality. It is an opportunity to close the perception gap and to prove the Office's commitment to continuous improvement.

The data processing is partially automated and described as follows:

Collection of data:

- At first stage, a request for expression of interest is sent to the user associations (UAs). The UAs express interest and appoint auditors who will represent them in the SQAP project. The SQAP team gathers all the data and sends an invitation letter to the nominated auditors with UAs in copy.
- The quality data, such as opinions/comments & evaluation statements of the external auditors together with name and surname are collected via the Lime-survey tool and they can be manually collected by the SQAP team during the live audit sessions.
- Identification data (name, surname and ID/passport number) and health data (only dietary requirements, allergens or intolerances) are collected in by means of the standard EUIPO event on-line registration form (Metis platform).

Please see in Annexes 1 and 2 the standard forms used to collect the personal data.

Use of data:

- The SQAP team extracts the auditor's response to the SQAP audit questionnaire (check list) from Lime Survey tool, number of the case, the relevant evaluation, including the identification data, to support the discussions between the external auditors and the SQAP team.
- The auditors' feedback (Quality Data – see section: "Description of categories of persons whose data [EUIPO] processes and list of data categories") is analysed in an excel table and updated once revised after discussions with auditors. Then the auditor's feedback is anonymised for analysis purposes and it is copied into ShareDox in a Word/PDF document accessible to limited people.
- The auditors' feedback (Quality Data – see section: "Description of categories of persons whose data [EUIPO] processes and list of data categories") is used for external reporting including the name and surname of the auditors. The reports obtained after the analysis contain analysed and aggregated data. External auditors are permitted to share the reports with relevant persons in their user associations, but they are not permitted to use it for professional purposes and to distribute it to third parties other than the relevant persons in their use associations without the prior



approval of the EUIPO.

- The Identification Data (see section: "Description of categories of persons whose data [EUIPO] processes and list of data categories") is also used for travel and accommodation arrangements purposes.
- The Health Data (see section: "Description of categories of persons whose data [EUIPO] processes and list of data categories") is used for obvious dietary purposes.

Disclosure:

- Reports containing aggregated feedback data as well as identification data (name and surname) of the auditors are sent to some EUIPO internal departments and services, linked to the KCQ report, and externally to the auditors and UAs to which the auditors belong (further description in section "Recipients of the data").
- There is also a possibility that UAs might receive information on number of decisions checked by each auditor from their UAs and some feedback on their auditors' performance.

Personal data is also processed for the purposes of organising and managing SQAP events, coordinating any required follow-up activities and for communication purposes. This may include registration and accommodation for SQAP participants; minute-taking and distribution of minutes; web publication, publication in the in-house magazine or through other media channels such as social media platforms; providing participants with further information on future SQAP events, etc.

SQAP events may be recorded via photographs, audio-visual and/or audio recordings, or other methods.



Purpose of the processing	<p>The processing of the personal data aims to get feedback regarding the quality of EUIPO's core business products and to have an insight which will allow for a better understanding of the users' perception.</p> <p>Personal data are also processed for the purposes of organising and managing the SQAP events, coordinating any required follow-up activities and for communication purposes. This may include registration and accommodation for SQAP participants; minute-taking and distribution of minutes; web-publication, publication on the in-house magazine or other media channels such as social media platforms or external media; to enable EUIPO to provide participants with further information on the particular SQAP events in the future, etc.</p> <p>There is a possibility that recordings (audio-visual, audio, photographs or more) will be carried out during the SQAP events.</p> <p>If participants do not wish their image to be photographed/recorded/web-published for compelling and legitimate grounds relating to their particular situation, they can leave and/or not be present in the place where the photographing/recording occurs or contact the SQAP team who will accommodate their needs, if possible.</p>
Data Subjects	<p>Data subjects are external auditors, members of the below Users Associations (UAs)</p> <p>Users Associations:</p> <p>APRAM, CITMA, ECTA, GRUR, INTA, INTERNATIONAL CHAMBER OF COMMERCE, MARQUES, AIM, AIPPI, ASIPI, BMM, BEDA, BUSINESSEUROPE (before: UNICE), CNIPA, EFPIA, EURATEX, FICPI, LES/LESI, UNION – IP</p> <p>In future SQAP audits, there will be a new request for expression of interest to the UAs to participate in the audits, thus this list of UAs may change.</p> <p>All personal data processed as described in this notification is related to the external auditors participating in the SQAP project.</p>



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>Data subjects are external auditors, members of the below Users Associations (UAs)</p> <p>Users Associations:</p> <p>APRAM, CITMA, ECTA, GRUR, INTA, INTERNATIONAL CHAMBER OF COMMERCE, MARQUES, AIM, AIPPI, ASIPI, BMM, BEDA, BUSINESSEUROPE (before: UNICE), CNIPA, EFPIA, EURATEX, FICPI, LES/LESI, UNION – IP</p> <p>In future SQAP audits, there will be a new request for expression of interest to the UAs to participate in the audits, thus this list of UAs may change.</p> <p>All personal data processed as described in this notification is related to the external auditors participating in the SQAP project.</p> <p>Identification Data:</p> <ul style="list-style-type: none">• Name and surname• User Association they are member of• Email and mobile phone number• CV• ID/Passport• Company they work for• Image and voice recorded during audit events; <p>Quality Data:</p> <ul style="list-style-type: none">• Quality and general evaluations of the EUIPO's core business products and activities - opinions/suggestions/comments• General feedback regarding the event, Office and project <p>Health Data:</p> <ul style="list-style-type: none">• Dietary requirements, allergens or intolerances <p>In addition, SQAP events may be recorded via photographs, audio-visual and/or audio recordings, or other methods, and participants may take part in interviews, workshops, etc. In this case, the resulting images, audio, statements and/or opinions, etc. may be subject to additional processing depending on the type of content and the purpose(s) for which it was recorded.</p>
<p>Retention period</p>	<p>Personal data processed by the Data Controller(s) or the service providers under their supervision are generally stored for the period of time necessary to achieve the purpose for which they will be processed.</p> <p>Personal data associated with SQAP must be erased after 2 years from the end of the last SQAP event in which data subject has participated. Nevertheless, some personal data might be kept for educational, institutional, historic, informational and/or promotional (internally and externally) for longer period of time if they have been published on the EUIPO intranet, EUIPO learning portal, EUIPO website, and/or made available via other Office's social media channels. If this is the case, the personal data will be limited as much as possible, for example, keeping only the name, surname, user association and photos.</p>



Recipients of the data	<p>Personal data will be disclosed to internal and external EUIPO staff working on the SQAP project, particularly staff from the Customer Department. External providers for the events at the Office will have access only to data strictly necessary for the organisation of the event and travel/accommodation for the participants.</p> <p>Participants' names and surnames, and, photos/videos of the event and any other personal data set out in the record may be accessible through internal and external communication tools, such as the Office intranet 'Insite' and the in house magazine 'Backstage', or published on the EUIPO website (such as in Alicante News), or in any other external press/media.</p> <p>Information concerning quality evaluations will be shared only with those required for the analysis and reporting, and strictly on a need-to-know basis. Personal data is not used for any other purposes or disclosed to any other recipient(s). Nevertheless, the User Association(s) you belong to may receive the number of decisions checked by you and some feedback on your performance as an auditor during the SQAP event.</p> <p>If any processing of personal data is carried out by a service provider, the data controller(s) will monitor and verify the implementation of the required organisational and technical measures necessary to ensure compliance with Regulation (EU) 2018/1725.</p> <p>In total, the data recipients are the following:</p> <p>For raw data:</p> <ul style="list-style-type: none">- Several EUIPO departments: CGS, OD and ICLAD and any other staff members on a need to know basis.- External auditors have actually the access to all the Quality Data (i.e. feedback of their colleagues) as well as to Identification Data (limited to the name/surname of their peers).- For the Lime Survey tool, the ones acting as "super administrators" and "administrators". <p>For aggregated results (including identification data of auditors):</p> <ul style="list-style-type: none">- EUIPO departments which may be interested.- EUIPO management.- EUIPO Quality Board service.- The staff/members of the UAs.- The auditors and their user association in case they forward the results to them.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?	<p>The data might be transferred to third parties, namely to:</p> <ul style="list-style-type: none">- Airline and Hotel companies for travel and accommodation arrangements purposes only.- Pomilio Blumm for the events platform purposes. <p>For the safeguards see below, section "General description of security measures (technical & organizational)" .</p>
General Description of security measures	<p>Personal data associated with the organisation, coordination and follow-up of the SQAP is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p> <p>The Confidentiality agreement and the Privacy Statement can be found enclosed in Annex 3 and Annex 2 respectively).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/c5e84e47-a3a1-4187-857a-46db12b6a5b9</p>
EDPS Prior consultation	YES



Reference number	DPR-2019-028
Name of the processing operation	Key User Programme
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euiipo.europa.eu.
Name and contact details of processor	External providers: 1. IECISA ALTIA - external service provider for DTD Informatica Corte Ingles SA. HEAD OFFICE Informaticá El Corte Inglés 4 Travesía de Costa Brava, (Mirasierra) 28034 Madrid, Spain, tel. +34 91 387 47 00 https://www.iecisa.com 2. LivePerson - external service provider for online chat LivePerson, Inc. T: 212.609.4200 475 Tenth Avenue F: 212.609.4233 5th Floor info@liveperson.com New York, NY 10018 www.liveperson.com
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The Key User Programme (KUP) is a package of services provided to all key users with the aim in guiding them towards increased use of online solutions, filing more straight-through files (mainly EUTM and RCD applications) and increasing use of current account.</p> <p>The package of services provided to users includes:</p> <ul style="list-style-type: none">• an online chat offered for guiding users and responding to their queries in the EUTM and RCD e-filings;• an improved User Area with monitoring statistics and dedicated news;• a dedicated Key User Management team (staff members of CD) who provide personalised support to the users;• a dedicated communication channel to receive IP-related information, such as news on trade marks or designs, invitations to seminars, workshops, and any other communications related to EUIPO goods and services. Certificates of attendance may be issued to the participants. <p>To participate to the key users programme, users must sign up on line (via the EUIPO User Area) and accept the terms and conditions of the Key User Programme. Terms and conditions are here. The Office is collecting personal data of the users who are signing up to the Key User Programme.</p> <p>Place where data is stored:</p> <p>Data is stored in the following EUIPO systems:</p> <ul style="list-style-type: none">• Office Website• PER• SAP CRM• BO Warehouse• Kibana• Access Database• Excel• Power BI <p>Upon activation by the user of the online chat the above specified data is transferred to the Online chat system: LivePerson.</p> <p>This information is stored along with chat session information to be used for statistical purposes and for linking the chat information with the user.</p>
Purpose of the processing	<p>The personal data is collected and stored in the corresponding EUIPO IT systems with the purpose of providing the services specified in the record. The data may also be used to produce internal statistics to monitor performance and quality of the Key User Programme which are necessary to improve the services.</p>
Data Subjects	<p>Data subjects are Key Users who are individuals participating in the Key User Programme</p>



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects are Key Users who are individuals participating in the Key User Programme</p> <p>Data collected from the users signing up to the key users programme and stored in the EUIPO systems:</p> <ul style="list-style-type: none">• PER ID and Name/Surname of the users as existing in the EUIPO PER database of the Office• Address of the user as existing in EUIPO PER database• Administrative email address provided for the administration of the user area• Key User Contact name• Key User Contact e-mail address• Key User Communication Language• Subscription to receive key user notifications to the email specified above.• Testimonials• photos, sounds, videos and audio-visual recordings, in the context of visits (e.g. IPforYou) <p>(Users will be informed of the processing of such data at the beginning of each event and a notice will appear in screens of the place of the event).</p> <p>Data of users having signed up to the key users and being transferred to the Online chat system only when user activates the online chat:</p> <ul style="list-style-type: none">• PER ID• Web User ID• Company name or Name• Name of Key User contact and Organization• Administrative e-mail address
Retention period	<p>The personal data will be kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>As long as the users remain in the Key User Programme the information collected for the purpose of the programme is maintained in EUIPO systems. Information coming from PER database is part of the register of the Office and the above-mentioned retention period does not apply.</p> <p>Testimonials, photos, sounds, videos and audio-visual recordings, will be kept 2 years after the Key-user visit.</p> <p>Information transferred to Live Person is retained in Live Person's infrastructure for a period of 13 months.</p> <p>Personal data contained in the certificates of attendance issued for the users who participated in events will be stored in Sharebox for a period of 2 years after the event (closing date).</p>
Recipients of the data	<p>1. EUIPO authorised staff and employees of the EUIPO providers in the framework of the provision of a service to the EUIPO necessary for the purpose of the data processing or the maintenance of the EUIPO systems on which the data is stored and according the specific contract.</p> <p>EUIPO authorised staff are :</p> <ul style="list-style-type: none">• CD staff dealing with customers: second line agents key user managers and teams leaders and line managers• External provider in charge of provision of First Line service• Management of the Office• Staff involved in the maintenance and support of IT systems specified above (internal/external providers). <p>2. Employees of the LivePerson provider for the on-line chat offered to the KUs. External Provider who acts as a Data Processor strictly to provide the software needed to manage the on-line chat service.</p> <p>3. In the context of visits (e.g. IPforYou): testimonials, photos, sounds, videos and audio-visual recordings can be published on EUIPO communication channels, or Newsflash sent to all Key Users.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>EUIPO's data centres are located in the EU</p> <p>LivePerson has primary and backup data centres in the United States, Europe and Australia.</p> <p>Moreover, some accesses and third-party sub-processors are located outside of the EU: Australia, Canada, Dominican Republic, USA, Israel, India, Singapore and Japan.</p> <p>The LivePerson third-party sub-processors are:</p> <ul style="list-style-type: none">• Sixty K Ltd, Bulgaria• Talk2Rep, Dominican Republic• Amazon Web Services, Inc., USA• Equinix, Inc., USA, UK, Netherlands and Australia• AllCloud Platforms Ltd, Israel• Google Inc., USA• Infocepts Inc, India• Marketo, Inc., USA <p>All of LivePerson's Affiliates (USA, Italy, Germany, UK, France, Australia, Japan, Singapore, USA, Canada, Israel).</p> <p>In the majority of the cases the subprocessors located outside of the EU are either registered in the Privacy Shield or indicate compliance with GDPR in terms of international transfers. In any case, LivePerson indicates that any transfer outside of the EU that is not subject to the Privacy Shield is also implemented via standard contractual clauses.</p> <p>The adequate mechanisms for the international data transfers are:</p> <ul style="list-style-type: none">• European Commission-approved standard contractual clauses related to transfers of personal information (available at http://ec.europa.eu/justice/dataprotection/internationaltransfers/transfer/index_en.html) <p>Privacy Shield certification (for Swiss and US) https://www.privacyshield.gov/welcome</p> <p>The EUIPO may provide, upon decision of the Executive Director or the Data Controller, the personal data collected for the purpose of the Key User programme to other EU institutions or bodies in the framework of administrative cooperation. The personal data transferred may be used for statistical and information purposes.</p>



<p>General Description of security measures</p>	<p>All personal data related to Statistics, publications and communication of user's data is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• When transferred to LivePerson, personal data will be encrypted and in a secure storage. Encryption is implemented using AES algorithm and a 192 binary digit key.• Encryption keys are unique per customer.• Access to client information is restricted.• Access to the chat client is protected by username and password. Chat agents are provided with an individual, nominal username and password.• Communications during the chat are encrypted using HTTPS.• Live Person infrastructure includes Access Control measures, patch management, server hardening and security incident monitoring. <p>Further details on Live Person configuration is available here.</p> <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/a971d5e9-467a-4ae7-a4d3-4fd69b1d19bf</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-032
Name of the processing operation	User Satisfaction Surveys
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euipo.europa.eu.
Name and contact details of processor	External processor: Name: BERENT Deutschland GmbH as the external service provider ("Berent") Organizational entity: CMS + BERENT Contact details: BERENT Deutschland GmbH Carl-Ludwig-Strasse 16 D-37213 Witzenhausen Germany Tel: +49 5542 9119-01 E-mail: info@berent.com
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Satisfaction surveys are sent via an e-mail invitation to an active population of users of EUIPO services (i.e. users having used EUIPO services within the year before the survey). Replies to the questions included in the online surveys are totally voluntary. The responses are collected in order to perform statistical processing to explore cause-effect relationships related to satisfaction with the services covered by the survey. As a result of the processing, a statistical report is produced.</p> <p>This report contains the answers in an anonymous and aggregated form that are available to EUIPO top management. This report is reported only in a manner that does not allow individual responses to be identified.</p> <p>An external service provider (Berent) has been appointed to conduct this survey and produce statistical reports under the instructions of EUIPO.</p> <p>Neither EUIPO nor the service provider use the personal data for any other purpose than carrying out the survey and collecting, aggregating and further analysing the results thereof.</p>
Purpose of the processing	The objective of this processing activity is to gather the feedback from the users in order to identify the follow up measures and actions to be taken to improve the quality of the services provided by EUIPO and to measure the level of users' satisfaction by type of users (i.e. country, segments and EUTM/RCD services used).
Data Subjects	EUIPO users: active users having used EUIPO services within the year before the survey.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects: EUIPO users: active users having used EUIPO services within the year before the survey.</p> <p>Data categories: - Existing demographic data on users of EUIPO services: EUTM/RCD, country, segments (owners, key users and representatives) gathered from PER, CRM, OWS and other existing systems. - Identification data (name and email address of users) - Responses to the questions. - Other data: position / function, number of employees, duration of business relationship with the Office.</p>
Retention period	<p>Personal data are kept only for the time necessary to achieve the purposes for which they will be processed.</p> <p>Excel tables on ShareDOX: 2 years from the survey starting date because users may be contacted for follow up (in case a user has made a suggestion for example the time limit to contact him back on the final status of the suggestion is 2 years).</p> <p>Reports on ShareDOX: indefinite since the reports are presented in aggregated way without personal data.</p> <p>Excel table without personal data: indefinite since the table are anonymous and it is not possible to track down a user.</p>
Recipients of the data	<ul style="list-style-type: none">• Internal EUIPO authorised staff from CD (Customer Feedback Team) in charge of analysing the results of the survey.• The external service provider staff involved in performing the survey will collect the results of the survey and analyse the raw data in order to perform statistics and figures in collaboration with Customer Feedback Team
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to User Satisfaction Surveys is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Standard IT access controls are implemented to ShareDox and the Survey System. <p>Confidentiality and data protection clauses are signed-off by the service provider participating in the survey exercises (see point 25).</p> <p>The service provider complies with the guidelines described in ISO 20252:2012, and the ESOMAR, MRS and BVM codes. BERENT's Managers are members of these aforementioned research associations and, as such, are obliged to conduct all business in accordance with the rules and regulations of these codes.</p> <p>Please see section "Other linked documentation", the documents "EUIPO-Data protection web-server" and "Berent security measures" for a description of Berent security measures.</p> <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/User_Satisfaction_Survey_en.pdf
EDPS Prior consultation	NO



Reference number	DPR-2019-034
Name of the processing operation	Language Check Tool (LCT)
Last Updated:	29/03/2019
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The LCT allows for the identification of possible meanings of the trade mark in any EU language in order to examine the trade marks regarding Absolute Grounds requirements. The language check is performed by native speakers in their respective languages, belonging to EUIPO (internal language checkers) or European Cooperation Project 4 – Collaborative Network (ECP4-CN) implementing National Offices (external language checkers); the result is captured in the LCT.</p> <p>The LCT captures personal data – the name of the responsible internal or external examiner and his/her language (performing the language check); the number of checks completed by the individual examiner (internal or external); the result/status of the check and his/her comments if the case.</p>
Purpose of the processing	<p>To identify if a trade mark has any meaning in any EU language helping to examine the trade marks regarding Absolute Grounds requirements.</p> <p>The production of the individual examiners (internal and external) form part of the appraisal report.</p>
Data Subjects	The language checkers (internal and external)
Description of categories of persons whose data EUIPO processes and list of data categories	<ul style="list-style-type: none">• LC Request Date: date of entering in the LCT• Status of each Language Check: “Not Done”, “Done with remark” & “Done without remark”• Remark (comment, if any)• Name of the language checker• Language of the language checker• Production (number of language checks performed) done by a language checker in a given period included in two years after the end of the appraisal period. <p>The “List of EUIPO Language Checkers” can be found in Insite, under “Operations” contact data. The list contains the names of the language checkers, their language and the organisational assignment.</p>
Retention period	<p>Indefinite for the data linked through the LCT to the EUTM application in the IP Tool.</p> <p>Two years after the end of the appraisal period for the summaries provided by data miners to the reporting officer (on demand) for appraisal purposes.</p>
Recipients of the data	<p>The Language Checkers (data subjects), both internal and external, only have access to their own production numbers.</p> <p>The Coordinators, backup coordinators and data miners in EUIPO have access to the detailed information and to the above personal data, including the production.</p> <p>The Director, Deputy directors, Team Leaders of the involved departments in EUIPO have the access rights in the directory containing the production requesting the said from the data miners, mainly used at the end of the appraisal periods.</p> <p>Coordinators and management of ECP4-CN implementing National Offices (NO) are able to request the Language Check coordinators in EUIPO to provide production data/statistics of the language checkers in their NO, for a specific period of time.</p> <p>All EUIPO staff can see the names of the language checkers, the respective language and the total number of pending cases (unassigned to a specific examiner) in a certain language.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the Language Check tool is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>PS Language Check Tool:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/5b4ec27b-d07f-488c-b832-52b051c010ef</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-035
Name of the processing operation	Mapping of the experience and competencies of OD inter partes decision takers
Last Updated:	28/03/2019
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Spreadsheet(s) reflecting the languages in which examiners work, the types of decisions they can take according to their training and experience, as well as their competencies as co-signers, coaches and ex ante checkers The information will be compiled by OD Team Leaders and will be periodically updated by them to reflect the acquisition of new competencies.
Purpose of the processing	The information processed will serve two main purposes: <ul style="list-style-type: none">• To facilitate the correct allocation of files, in particular taking into account the automatic allocation capabilities of the new IT back office tools (files to be pulled by examiners following a set of criteria). The data in the spreadsheet might be eventually integrated for this purpose in the future IT tools.• To assist the Team Leaders and Heads of Service in the definition of optimal co-signing groups in accordance with Articles 132(2) and 134(2) EUTMR, as well as in the organization of coaching and ex ante checking activities. The information on the spreadsheet will not be used for appraisal purposes. Although the competencies and experience of each examiner might be relevant in the context of an appraisal, they will be assessed individually by their reporting officers and not extracted from these spreadsheets.
Data Subjects	OD inter partes decision takers
Description of categories of persons whose data EUIPO processes and list of data categories	The following data related to all inter partes decision takers in OD is processed: <ul style="list-style-type: none">• Team number;• Staff member name;• Legally qualified status (for the purposes of Articles 132(2) and 134(2) EUTMR);• Languages (for drafting and for co-signing);• Types of decisions that can be taken by each examiner classified by difficulty (e.g. A, B1, B2, C);• Experience as co-signer (e.g. average, intermediate, co-signer/coach);• Ex-ante checker (yes or no);• Time dedication to decision drafting (in %).
Retention period	The spreadsheet will be periodically updated (at least once every three months) and previous versions will not be stored. Personal data that is no longer needed (e.g. data about staff who have left the department or no longer draft inter partes decisions) will only be kept until the next update. The spreadsheet will be in use until it serves the purpose of facilitating the allocation of files by the IP tool and/or the formation of the co-signing groups.
Recipients of the data	OD Management; OD QPROs; OD Team Leaders; OD Secretariat; IT administrators managing work allocation tools for the back office
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	The spreadsheet is protected through the system of ShareDox permissions (access groups) to ensure they can only be accessed by the above-mentioned recipients. The automatic versioning of the file (that is activated by default for every EUIPO document in ShareDox) has been disabled. The document has only one live version so that no historical data is kept.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	PS mapping of experience/competencies of OD inter partes decision takers : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/15bb05ac-fe24-4a4d-9e2e-d616ffa6847a
EDPS Prior consultation	NO



Reference number	DPR-2019-037
Name of the processing operation	Processing personal data within the framework of EUIPO Mobile Telecommunications Services Policy
Last Updated:	29/03/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The Human Resources Department (HRD) is responsible for monitoring and implementing the EUIPO's policy and guidelines concerning the use, in the interest of the service, of mobile telecommunication services by internal/external staff members.</p> <p>Staff members who have been selected by the Department's management to use mobile telecommunications services/devices are requested to give previous acceptance to the conditions laid down in the EUIPO's established policy for mobile telecommunications, as well as those stated in the Personal Security Policy (Information Security & You) .</p> <p>EUIPO offers the following – not limited – possibilities of mobile telecommunication devices to staff members: Basic Mobile Phone, Smart Phone, SIM card, Portable modem, Tablet, Laptop.</p> <p>The telecommunications services provided are: Voice (Internal 4-digit numbers, National, Europe or International) and Data (Wi-Fi only, National, Europe or International).</p> <p>Mobiles and iPads are pre-loaded with the applications necessary for normal professional use. Staff members shall not carry out Office business on any other application than those provided. The user is responsible for covering any costs related to subscription/purchase for any applications that they download from an online store.</p> <p>The staff member will be informed by the Service Desk of the Digital Telecommunications Department (DTD) about the above mentioned services, as regards Voice and Data consumption to device's they have in use, as well as about any change to said limits. Users may request their Voice and Data consumption details for a certain period (within a limit of one year) by sending an e-mail to the mailbox euipomobiletelecomexpense@euipo.europa.eu</p> <p>Cellular data consumption throughout the Office will be monitored on a monthly basis by DTD and FD.</p> <p>When the user reaches the maximum consumption of National allocated data, access to data will be slow down; in this case the user is required to raise an incident through the Service Desk and provide justification from the Director /Head of Service to obtain an additional data allowance.</p> <p>In case of excessive use of Voice and/or Data services, the Service Desk (DTD) shall inform the staff member's Director /Head of Service who may request a written justification to the user.</p> <p>Users may be requested by HRD to provide a written justification when additional data use has been made. . If necessary, the user will be asked to modify their use within the following month.</p> <p>In case of misuse or non-justified excessive use, appropriate measures will be taken, such as the withdrawal of all mobile devices.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The processing of personal data by HRD is used to:</p> <ul style="list-style-type: none">- examine requests (if the mobile telecommunications service/device required for a staff member is duly justified and approved by the Department management of the staff member concerned;- approve / reject / cancel requests;- revise the approved requests every 12 months at Office's level;- take the appropriate corrective measures in case of inappropriate or excessive use of the telecommunication's services/devices, such us withdrawal and/or modification of their use.
Data Subjects	EUIPO staff members (internal and external staff)



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed are the following:</p> <p>Full name, personal number, phone number, address (building, floor, office), start/end date at EUIPO, assignment (Department and functions) for internal/external staff.</p> <p>Information in the dashboard: calling number, called number, country, date and time of call, duration of the call and cost.</p>
Retention period	<p>Data of individuals shall be erased or made anonymous as soon as possible after the months of collection, no longer than up to the end of the period during which the bill may lawfully be challenged or payment pursued.</p> <p>The list of staff members that have exceeded the monthly threshold amount for the use of mobile phones have a history of 12 months maximum (kept by FD-VMEF) – i.e. records of over 12 months will be deleted.</p> <p>The data relating to billing (only aggregated data) are retained for a period of 5 years from the data of decision granting discharge in respect of implementation of the EUIPO's budget.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process or a disciplinary procedure.</p>
Recipients of the data	<p>Access to the data is determined by strict rules and is based on the needs of the procedure. Access is given to the following persons/services:</p> <ul style="list-style-type: none">- Staff member concerned and his/her Department management (Line manager /Director) for the justification of requests;- HRD for approval of all requests, monitoring and implementation of EUIPO telecommunications policy;- A restricted number of staff authorized by the Department management of the staff member concerned;- A restricted number of staff authorized by HRD for monitoring EUIPO's mobile telecommunication services policy;- One staff member of FD-VMEF for reasons of verification of the bills provided on a monthly basis by the telecom provider;- Two staff members of DTD (Line manager and the manager of the mobile telecommunications) have access to the dashboard where all data are available. Depending on the situation, information collected through the mobile device management tool may need to be sent by DTD to the external service provider and any subcontractor, after duly notification to EUIPO and its acceptance;- Data accessible to DTD when processing Data Migration: device username and password, as well as all personal data stored and maintained by the user on the device (e.g.: photographs, bank and credit card information / passwords to any application or website);- The Data Controller and the Director of the staff member concerned will receive a monthly report from DTD / FD-VMEF informing about the total cost attributed individually to staff members who have exceeded the given threshold. This information only contains the total expense per telecommunication services line number (no indication is given to the telephone numbers dialled);- In case of complaints, data may be disclosed to the Legal Service and /or to the EU Court of Justice;- Data may also be sent by DTD to the police in case of theft or robbery of the device.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Electronic documents are stored according to the Security measures of the EUIPO Information Systems (IT), as well as in specific electronic folders accessible only to authorized persons working in these files. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. SAP SuccessFactors” is also certified in ISO 27001.</p> <p>A limited number of authorized staff (internal or external) administrating the IT Systems has access to the electronic data.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on EUIPO Mobile telecommunications :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/cdd9e409-ec07-4df3-a17c-5dcd01514205</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-038
Name of the processing operation	Management of Incidents and Changes
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	IECISA ALTIA DTD Operations external service provider KIO NETWORKS ESPAÑA S.A. (Murcia)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The processing consists in collecting incidents and/or change requests from individual users through a web based application. Incidents and changes may concern: • Desktop & Accessories • EUIPO Applications • Workplace • Health, Safety and Security • Logistics • Purchasing • IT Technical Requests • Telecommunications • Staffing Internal users (staff) file these incidents and/or change requests in accordance with their daily needs directly in the system. External users' incidents and/or change requests are filed in the system by DTD's Service Desk as a consequence of a phone call. Incidents and change requests are then subject to a series of validations and/or authorizations by DTD support services or other EUIPO's services depending on the nature of the product requested. These validations and/or authorizations are supported by a workflow mechanism implemented in Remedy. In accordance with their respective validations, authorizers perform the appropriate actions to address the incidents and/or change requests management. Finally, incidents and change requests management may be subject to statistical analysis, in principle fully anonymous.
Purpose of the processing	The first purpose is to provide EUIPO's users with user friendly tool and procedure to request any items or services needed to ensure the daily and efficient functioning of EUIPO and its services. Since part of the incidents and change requests management is outsourced and entrusted to external providers, contractual SLAs have been established to ensure the appropriate fulfilment of the service. The statistics that can be gathered during the usage of the tool can also be used to measure the service provider compliance with these SLAs.
Data Subjects	All EUIPO Staff and external providers staff working in EUIPO Premises.
Description of categories of persons whose data EUIPO processes and list of data categories	The following information is collected from the user, regardless of whether the user is internal or external: • Login • first name, last name • Company • EUIPO personal number • ID Card number • department, service • administrative address • phone extension • mobile phone • email • list of user's IT inventory Depending on the request type, the system can ask for information like contract type, card plate number or user location.
Retention period	The information from requests, incidents, surveys and authorizations is kept for a maximum of 10 years from the closure of the request, as it is required for operational purposes to maintain the information related to asset requests in order to have evidence of the requested, the authorizer, and the type of request. Information may be kept further in an anonymous form for statistical purposes.
Recipients of the data	All actors involved in the validation and management of incidents and/or change requests: - DTD Service Desk - Authorizers - Service providers from DTD and IBD in charge of providing the services required by the user.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO



If so, to which ones and with which safeguards?	KIO NETWORKS ESPAÑA S.A. (Murcia)
General Description of security measures	<p>For information managed by My Service Desk (Incidents and Changes) the service provider has security measures implemented such as:</p> <ul style="list-style-type: none">• EUIPO data is separated/partitioned from other service provider clients.• For this reason the service provider put in place the necessary technical and organisational measures to assure the data controller (EUIPO) that he (and all his sub-contractors) protect the EUIPO's data against destruction, loss, modification, publication, without authorisation, during the treatment and its transmission over a network but also against any other illicit treatment.• Communications between the service provider and the EUIPO as well between data centres are encrypted.• The location of the servers and data store are in IECISA –ALTIA premises in Spain• Server is physically protected at the Data Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. <p>More information about security measures implemented by the service provider: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/e0a2c271-2fc2-4762-9168-53a39725780d</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement: http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/7f01b4b2-5ee2-4ac7-b1f6-35e926779c11/Terms%20of%20Use%20-%20My%20Service%20Desk.pdf?a=true</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-039
Name of the processing operation	RCD-Download
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	RCDDOWNLOAD is the EUIPO's data provision service of the particulars of RCD applications or registrations submitted to it which may be accessed by the authorized users by bulk download. The RCD-Download system is used to extract information about the RCDs from RCD Online and provide services to subscribers that will allow them to download the RCDs in XML format under TM-XML standard. General users without registration are allowed to access only to the Anonymised Dataset through OpenData platform (https://euipo.europa.eu/ohimportal/en/open-data).
Purpose of the processing	Provide third parties and public authorities with the information they need to enable them to exercise the rights conferred on them by the RCD and to determine the existence of priori rights belonging to third parties.
Data Subjects	Individuals whose data have been entered as RCD particulars



Description of categories of persons whose data EUIPO processes and list of data categories	With regard to persons information, the service supplies the following data if available with regard to a particular RCD: <ul style="list-style-type: none">- Designer:<ul style="list-style-type: none">o Nameo Identifier- Applicants/Owners:<ul style="list-style-type: none">o Applicant Identifiero First Nameo Middle Nameo Last Nameo Organization Nameo Name Synonymo Typeo Address Country Codeo Address Countyo Address Stateo Address Streeto Address Cityo Address Postcodeo Postal Address- Representative:<ul style="list-style-type: none">o Representative Identifiero Representative Type Code (Professional Representative, Lawyer, Association, Employee, Other)o First Nameo Middle Nameo Last Nameo Organization Nameo Name Synonymo Typeo Address Country Codeo Address Countyo Address Stateo Address Streeto Address Cityo Address Postcodeo Postal Address- Appeals:<ul style="list-style-type: none">o Appellant IDo "Appellant's representative ID"o Respondent IDo Respondent's representative ID- Recordals related:<ul style="list-style-type: none">o Claimant IDo "Claimant's Representative ID"
Retention period	<p>The data are kept for an indefinite period of time for legal, historical and statistical purposes according to the Article 111(8)(9) of Regulation (EU) 2017/1001 of the European Parliament and of the Council.</p> <p>Other personal data stored in the database will also be kept indefinitely, but its removal from the database can be requested 18 months from the expiry of the related Community Design or the closure of the relevant inter partes procedure. This does not apply to personal data stored in the Register.</p> <p>In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	DTD Operations and their service provider IECISA – ALTIA (as EUIPO external service provider for IT operations) can access the tool (and related data) for technical reasons such as maintenance, updating and improvement of the tool. The Office will not make available to the public any personal data other than that available in the Register.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	Due to the nature of the tool (available to general users) data could be seen by anybody around the world.
General Description of security measures	<p>For information stored in RCDDOWNLOAD, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. <p>To have access to non-anonymized data, it is necessary to go through a user validation process.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://euiipo.europa.eu/ohimportal/en/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-040
Name of the processing operation	EUTM-Download
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUTM DOWNLOAD is the EUIPO's data provision service of the particulars of EUTM applications or registrations submitted to it which may be accessed by the authorized users by bulk download.</p> <p>The EUTM Download system is used to extract information about the EUTMs from EUTM Online and provide services to subscribers that will allow them to download the EUTMs in XML format under TM-XML standard.</p> <p>General users without registration are allowed to access only to the Anonymised Dataset through OpenData platform (https://euipo.europa.eu/ohimportal/en/open-data)</p>
Purpose of the processing	Provide third parties and public authorities with the information they need to enable them to exercise the rights conferred on them by the EUTM and to determine the existence of priori rights belonging to third parties.
Data Subjects	Individuals whose data have been entered as EUTM particulars



Description of categories of persons whose data EUIPO processes and list of data categories	With regard to persons information, the service supplies the following data if available with regard to a particular EUTM: - Applicants/Owners: o Applicant Identifier o First Name o Middle Name o Last Name o Organization Name o Name Synonym o Type o Address Country Code o Address County o Address State o Address Street o Address City o Address Postcode o Postal Address - Representative: o Representative Identifier o Representative Type Code (Professional Representative, Lawyer, Association, Employee, Other) o First Name o Middle Name o Last Name o Organization Name o Name Synonym o Type o Address Country Code o Address County o Address State o Address Street o Address City o Address Postcode o Postal Address - Oppositions: o Opponent ID o Representative ID - Appeals: o Appellant ID o "Appellant's representative ID" o Respondent ID o Respondent's representative ID - Recordals related: o Claimant ID o "Claimant's Representative ID"
Retention period	The data is kept for an indefinite period of time for legal, historical and statistical purposes according to the Article 111(8)(9) of Regulation (EU) 2017/1001 of the European Parliament and of the Council. In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal process.



Recipients of the data	<p>EUTM Download allows the bulk download of information which is considered to be of public interest, which the Office has a legal obligation to make accessible to any third party (Register data). By default, the information that can be downloaded is from EUTM data files that do not contain any personal data of owners or representatives. However, after registration and proper validation of the requester, a more complete EUTM dataset can be accessed, which does contain said personal data.</p> <p>All the extracted EUTMs are accessible by all the subscribers with a personal username/password.</p> <p>DTD Operations and their service provider IECISA – ALTIA (as EUIPO external service provider for IT operations) can access the tool (and related data) for technical reasons such as maintenance, updating and improvement of the tool.</p> <p>The Office will not make available to the public any personal data other than that available in the Register.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	Due to the nature of the tool (available to general users) data could be seen by anybody around the world.
General Description of security measures	<p>For information stored in EUTM DOWNLOAD, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. <p>To have access to non-anonymized data, it is necessary to go through a user validation process.</p> <p>Regardless of stage, everybody dealing with personal data in the context of EUTM Download must sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://euiipo.europa.eu/ohimportal/en/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-041
Name of the processing operation	CESTO
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	CESTO is an automated and harmonized search tool which will perform searches for any given trade mark application and in turn provides information in relation to similar trade marks from an array of IP offices (who have their trade marks in TMview), similar trade marks from the same or similar owners from the same array of offices, emblems and other heraldic devices held by WIPO, Geographical Indications at EU and national level, International Non-Proprietary Names for active pharmaceutical ingredients from WHO (MedNet), as well as any specific information as provided by the IP offices and the EUIPO (on a dashboard). Some of the most commonly used webpages containing English language and specialized dictionaries will also be included.
Purpose of the processing	<ul style="list-style-type: none">- Creation of user accounts- Management of the user accounts- Communication with the users- Statistics
Data Subjects	Individuals whose data have been entered as EUTM particulars.
Description of categories of persons whose data EUIPO processes and list of data categories	<ul style="list-style-type: none">- Name and surname- Username- Password- Email- Country of the IP office- Account's role (e.g. administrator, IP office...) <p>It must be noted that when a data subject performs a search in CESTO, personal data of the right owners might be shown in the results, though this information is not managed or stored by CESTO, it is obtained from the data sources of the tool (such as IP Offices or WIPO)</p>
Retention period	User account information is kept for as long as there is a contractual relationship with the Office (in case of staff) or the IP Office's staff is involved in the process. Once the contractual relationship ends, or the account is not necessary anymore, it is deactivated. EUTM information, as long as EUTMs are not removed or not deleted through the daily update procedure.
Recipients of the data	Outside EUIPO: All internet users connecting to https://www.tmdn.org/network/ Inside EUIPO: - EUIPO examiners. - DTD responsible staff.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?	Due to the nature of the tool (available to general users) data could be seen by anybody around the world.
General Description of security measures	<p>For information stored in CESTO, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. <p>The registration process is “on-request”. Only EUIPO’s staff can generate new accounts.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://tmdn.org/network/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-042
Name of the processing operation	TMC
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu for internal users DPOexternalusers@euipo.europa.eu for external users
Name and contact details of processor	IT security team and network/system administrators' team from IECISA ALTIA. IT security team consists of internal staff members. IECISA ALTIA is an external service provider for the DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The Terminology Maintenance Console (TMC) (https://euipo.europa.eu/tmc/login) is the business administration tool for TMclass and Similarity. It is an online platform whose principal function is to allow participating offices maintain their harmonised database of goods and services (HDB). The TMC also enables Participating Offices to maintain pairs stemming from their oppositions where specific goods and services are in debate.
Purpose of the processing	<ul style="list-style-type: none">- Creation of user accounts- Management of the user accounts- Communication with the users- Add comments and modify terminology- Statistics
Data Subjects	EUIPO Staff; EUIPO external service providers; IP National Offices staff
Description of categories of persons whose data EUIPO processes and list of data categories	<ul style="list-style-type: none">- Name and surname- Username- Password- Email- Country of the IP office- Telephone number- Account's role (e.g. administrator, IP office...)
Retention period	User account information is kept for as long as there is a contractual relationship with the Office (in case of staff) or the IP Office's staff is involved in the process. Once the contractual relationship ends, or the account is not necessary anymore, it is deactivated.
Recipients of the data	The user's data are available within the platform to all registered users. IECISA – ALTIA, as EUIPO external service provider for IT operations, can access the tool (and related data) for technical reasons such as maintenance, updating and improvement of the tool.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	IP National Offices



General Description of security measures	For information stored in TMC, the standard security measures of the EUIPO Information Systems is applied: <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the servers. The registration process is “on-request”. Only EUIPO’s staff can generate new accounts.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://tmdn.org/network/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-043
Name of the processing operation	e-Search Plus
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	eSearch Plus is an EUIPO online tool which allows external and internal users to access, free of charge, EUIPO's data related to CTM (Trade marks) and RCD (designs), applications and registrations. eSearch Plus disseminates, through an automated process, all publicly available EUTM and RCD related information, including information on owners, representatives and, if present, appellants and respondent.
Purpose of the processing	The Office is required to maintain a public register with all the information regarding EUTM and RCD, including the personal data of owners and representatives, to allow third parties and public authorities to exercise the rights conferred on them by the EUTM and the RCD. This information is considered to be of public interest.
Data Subjects	Individuals whose data have been entered as EUTM and RCD particulars



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>With regard to persons information, the service supplies the following data if available with regard to a particular EUTM and/or RCD as well as regard to a singular Owner and/or Representative:</p> <ul style="list-style-type: none">* Trademarks:<ul style="list-style-type: none">- Owner information<ul style="list-style-type: none">o ID numbero First name/ Middle name/ Last nameo Organisationo Address Countryo Address State/countryo Address Towno Address Post codeo Addresso Correspondence address- Representative information<ul style="list-style-type: none">o ID numbero First name/ Middle name/ Last nameo Organisationo Typeo Address Country Codeo Address State/countryo Address Towno Address Post codeo Addresso Correspondence addresso Telephoneo Faxo Email- Appeal<ul style="list-style-type: none">o Appellant IDo Appellant Representative IDo Respondent IDo Respondent Representative ID- Recordals<ul style="list-style-type: none">o Claimant IDo Claimant Representative ID- Oppositions<ul style="list-style-type: none">o Opponent IDo Opponent Representative ID* Designs:<ul style="list-style-type: none">- Owner information<ul style="list-style-type: none">o ID numbero First name/ Middle name/ Last nameo Organisationo Address Countryo Address State/countryo Address Towno Address Post codeo Addresso Correspondence address- Representative information<ul style="list-style-type: none">o ID number
--	---



- o First name/ Middle name/ Last name
- o Organisation
- o Type
- o Address Country Code
- o Address State/country
- o Address Town
- o Address Post code
- o Address
- o Correspondence address
- o Telephone
- o Fax
- o Email
- Appeal
- o Appellant ID
- o Appellant Representative ID
- o Respondent ID
- o Respondent Representative ID
- * Owners:
 - ID number
 - First name/ Middle name/ Last name
 - Organisation
 - Address Country
 - Address State/country
 - Address Town
 - Address Post code
 - Address
 - Correspondence address
- * Representatives:
 - ID number
 - First name/ Middle name/ Last name
 - Organisation
 - Type
 - Address Country Code
 - Address State/country
 - Address Town
 - Address Post code
 - Address
 - Correspondence address
 - Telephone
 - Fax
 - Email



Retention period	<p>All the personal data included in the EUTM or RCD register are kept indefinitely for legal, historical and statistical purposes according to Article 7(1) of Decision No EX-14-3 of the President of OHIM and to the Article 111(8)(9) of Regulation (EU) 2017/1001 of the European Parliament and of the Council.</p> <p>Other personal data stored in the database will also be kept indefinitely, though its removal from the database can be requested 18 months from the expiry of the related EU trade mark or the closure of the relevant inter partes procedure. This does not apply to personal data stored in the Register.</p>
Recipients of the data	<p>DTD Operations and their service provider IECISA – ALTIA (as EUIPO external service provider for IT operations) can access the tool (and related data) for technical reasons such as maintenance, updating and improvement of the tool.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>Due to the nature of the tool (available to general users) data could be seen by anybody around the world.</p>
General Description of security measures	<p>All personal data available via eSearch Plus is stored in secure IT applications according to the Office's security standards. Appropriate levels of access are granted individually only to authorised recipients.</p> <p>Regardless of stage, everybody dealing with personal data in the context of eSearch Plus must sign a confidentiality declaration.</p> <p>For this process, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement: https://euipo.europa.eu/ohimportal/en/data-protection</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-044
Name of the processing operation	e-Search Case Law
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	eSearch Case Law is an EUIPO online tool which allows external and internal users to search, free of charge, decisions taken by the Office and judgements of national and Union courts eSearch Case Law disseminates, through an automated process, all public information related to proceedings for EUTMs and RCDs, including information on owners, representatives and, if present, appellants and respondent. The tool provides users with the possibility of having free, automatic translations of decisions taken by the Office and judgments of the national and European Union courts.
Purpose of the processing	The Office is required to maintain a public register with all the information regarding proceedings for EUTMs and RCDs to enable third parties and public authorities to exercise the rights conferred on them by the EUTM and the RCD and to create a channel of communications with applicants and other parties. This information is considered to be of public interest.
Data Subjects	Individuals whose data have been entered as EUTM and RCD particulars



Description of categories of persons whose data EUIPO processes and list of data categories	<p>With regard to persons information, the service supplies the following data if available with regard to a particular EUTM and/or RCD:</p> <ul style="list-style-type: none">* Trade mark decisions:<ul style="list-style-type: none">- Application Information<ul style="list-style-type: none">o Owner ID numbero Owner nameo Representative ID numbero Representative name- Opposition<ul style="list-style-type: none">o Opponent IDo Opponent nameo Opponent representative IDo Opponent's representative's name- Cancellation<ul style="list-style-type: none">o Cancellation applicant's IDo Cancellation applicant's nameo Cancellation applicant's representative IDo Cancellation applicant's representative's name* Design decisions:<ul style="list-style-type: none">- Application Information<ul style="list-style-type: none">o Owner ID numbero Owner nameo Representative ID numbero Representative name- Invalidity<ul style="list-style-type: none">o Invalidity applicants IDo Invalidity applicant's nameo Invalidity applicant's representative IDo Invalidity applicant's representative name* Preliminary rulings:<ul style="list-style-type: none">- Parties<ul style="list-style-type: none">o Nameo Representativeso Correspondence addresso Name of the Officials involved in the Decisions* National court judgments National court judgments are published as they are received, as described in the Practice Note – Online publication and access to judgements. Please, note that national and EU court judgments are made available as they were initially published by the respective court.
Retention period	All the personal data included in the EUTM or RCD register are kept indefinitely for legal, historical and statistical purposes according to Article 7(1) of Decision No EX-14-3 of the President of OHIM and to the Article 111(8)(9) of Regulation (EU) 2017/1001 of the European Parliament and of the Council.



Recipients of the data	DTD Operations and their service provider IECISA – ALTIA (as EUIPO external service provider for IT operations) can access the tool (and related data) for technical reasons such as maintenance, updating and improvement of the tool. For the purposes of automatic translations, personal data is processed internally by the Advance Linguistic Solutions team in the Customer Department.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	Due to the nature of the tool (available to general users) data could be seen by anybody around the world.
General Description of security measures	<p>All personal data available via eSearch Case Law is stored in secure IT applications according to the Office's security standards. The automatic translations are produced using eTranslation, a service provided by the European Commission. The connection between the EUIPO and eTranslation is set using the sTESTA secure network. Appropriate levels of access are granted individually only to authorised recipients.</p> <p>The databases are password-protected under a single sign-on system and connected automatically to the user's ID. E-records are held securely to safeguard the confidentiality and privacy of the data therein.</p> <p>Regardless of stage, everybody dealing with personal data in the context of eSearch Case Law must sign a confidentiality declaration.</p> <p>For this process, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://euiipo.europa.eu/ohimportal/en/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-045
Name of the processing operation	Email Usage
Last Updated:	29/03/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	IT security team and network/system administrators' team from IECISA ALTIA. IT security team consists of internal staff members. IECISA ALTIA is an external service provider for the DTD. MICROSOFT (the service provider)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of the email traffic from and to the mailboxes of EUIPO staff, as well as any service provider that has been assigned an EUIPO email address (from herein after referred to as "EUIPO email system users"). This Notification is linked to the DPO Notification - DPR-2018-003 Office 365.
Purpose of the processing	-To enable electronic communication and exchange of electronic messages and attachments amongst EUIPO staff and with external users, such as service providers, stakeholders and any other recipient of EUIPO emails. -To offer to EUIPO email system user the email access to addresses of all EUIPO email system users, EUIPO inboxes, and of main external partners (other Institutions and bodies, Member states, and other EU organizations included in the email address book) -To have a trail of emails in the event that an incident requires investigating emails sent or received by EUIPO email system users. -To have a backup in case that a EUIPO email system user requests the recovery of a deleted email.
Data Subjects	All EUIPO Staff, External Providers Staff, and anyone that has been assigned an EUIPO email address.
Description of categories of persons whose data EUIPO processes and list of data categories	All information included in the emails and in the personal address book: • First name and surname of the EUIPO email system users. • Email addresses of both the sender and the recipient, and any address book references • Email subject • Email contents • Email attachments All personal information included in the Global Address book: • First name and Surname • Email alias • Department • Office location • Office phone number • Office mobile phone number • Company • Email group memberships.
Retention period	• Email information as well as any personal address book implemented by the EUIPO email system user is stored for as long as the user wishes to maintain the email and has a contractual obligation with the Office. • The personal information included in the Global address book is stored for as long as the user has a contractual obligation with the Office. Once a contract expires, information is retained for 90 days for the purposes of collection from the Office or possible renewal. After this period, information is deleted. • In the case of a legal claim or an administrative investigation, be it a disciplinary or criminal offense, information could be stored longer than the time limits indicated above. These measures are treated on a case by case basis.
Recipients of the data	In the processing of email traffic and for the management of exchange server backups, the only recipient is the service provider of DTD Operations for the management of the tool (Processor). Any other access to email information would require authorization by the EUIPO DPO. That said, all EUIPO email system users will have access to the Address book information, as well as staff of other European institutions with access to the Address Book.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES



Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	In the processing of email traffic and for the management of exchange server backups, the information managed is not shared with anyone that is not the data subject, data controller, the processor or any recipient indicated above. That said, by definition of an e-mail system, e-mail messages and attachments could be sent out to and received from anybody around the world. This includes EUIPO email system users willingly or unknowingly sharing personal data of other EUIPO email system users (for example, by having the email address of other EUIPO email system users in copy of an email sent to a third party).
General Description of security measures	<ul style="list-style-type: none">• EUIPO username and password required in order to access the email inbox.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Center.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail server Office 365 Security Measures applies (DPR-2018-003)
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: http://sharedox.prod.oami.eu/share/proxy/alfresco/slingshot/node/content/workspace/SpacesStore/98834903-68c8-43f5-8776-883394f03f39/Privacy%20Statement%20EMAIL%20USAGE%20-%20FINAL.pdf?a=true
EDPS Prior consultation	NO



Reference number	DPR-2019-046
Name of the processing operation	Collection of misleading invoices addressed to the users of the IP systems
Last Updated:	29/05/2019
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain
Joint Controller organizational entity	ICLAD
Joint Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain
Name and contact details of processor	External processor: external service provider eXTEL Contact Centre which acts on behalf of the EUIPO as data processor
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The Customer Department of the Office (Information Centre) provides the Office's customers with information services. In this context, it receives emails and/or phone calls by which misleading invoices for unsolicited IP services sent to the users are reported to EUIPO, and collects such misleading invoices centrally. It collects all relevant data in one single document which is further shared with Europol on a regular basis. The International Cooperation and Legal Affairs Department (Litigation Service) processes personal data of users included in reported misleading invoices for the purposes of legal advice and representation in legal proceedings in relation to the reported misleading invoices.
Purpose of the processing	The purposes of the processing operation are to: <ul style="list-style-type: none">• facilitate interactions with the EUIPO when users, user associations and national or international IP offices report misleading invoices to EUIPO;• allow the centralised collection of all misleading invoices reported to EUIPO and compilation of a common list/database of anonymised misleading invoice samples;• allow sharing of reported misleading invoices with Europol in a secure and structured manner for the purpose of providing comprehensive evidence to assist any future criminal legal actions;• where it proves necessary, allow reporting of instances of suspected fraud to national law enforcement and/or judicial authorities of EU Member States;• produce statistical reports with the aim of obtaining metrics regarding user interactions and fraud cases. The personal data is not intended to be used for any automated decision making, including profiling.
Data Subjects	Users reporting misleading invoices for unsolicited IP services



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>Data subjects:</p> <p>Users reporting misleading invoices for unsolicited IP services</p> <p>The data processed is:</p> <ul style="list-style-type: none">• contact data: first name, last name, username, company name, address, country, phone number, fax number, email address, bank account details;• interaction data: interaction record ID, time, date, language, country, status, channel, subject, content or description of the interaction, categorisation, file number, group responsible, responsible for reply, employee responsible, previous interaction;• identification data: PER ID, country, languages;• content of the emails received from the user;• copies of misleading invoices sent to EUIPO. <p>All misleading invoice examples published by the Communication Service on the EUIPO website in the common list/database are anonymised and do not include any personal data.</p>
<p>Retention period</p>	<p>Personal data will only be kept for the time necessary to achieve the purposes for which it is processed. Where applicable, it will be kept for a period corresponding to 10 years or the closure of legal proceedings on the basis of misleading invoices reported to EUIPO.</p>



Recipients of the data	<p>Personal data is disclosed to the following recipients.</p> <ul style="list-style-type: none">• Authorised staff of the Customer Department, and in particular, the Information Centre for interaction with users, and for collection and storage of misleading invoice samples.• Authorised staff of the Digital Transformation Department and external contractors for the technical maintenance of the IT tools.• Authorised staff of the International Cooperation and Legal Affairs Department (Litigation Service) and, where appropriate, authorised external lawyers, for the purposes of legal advice and representation in legal proceedings in relation to the reported misleading invoices. <p>Information concerning the data processing will only be shared with those persons necessary for the implementation of such measures on a strictly need-to-know basis.</p> <p>Personal data such as name and address of the user reporting a misleading invoice and any other identification data contained in the referred invoice, where such data of a victim are essential part of evidence of reported suspected offences of fraud, may be transferred by the Customer Department of EUIPO to Europol in a secure and structured manner.</p> <p>Europol may receive and process personal data from Union bodies, such as EUIPO, insofar as necessary and proportionate for the legitimate performance of its tasks (Article 23(5) of Regulation (EU) 2016/794 ('Europol Regulation')). Processing of such data of victims by Europol is allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives (Article 30(1) of the Europol Regulation).</p> <p>Where it proves necessary, such data may be transferred to national law enforcement and/or judicial authorities of EU Member States. Further processing of personal data will be based on the Europol Regulation and the data protection legislation applicable to the competent national authorities.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	Where it proves necessary, such data may be transferred to national law enforcement and/or judicial authorities of EU Member States.
General Description of security measures	<p>All personal data related to the collection of misleading invoices addressed to the users of the IP systems is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Confidentiality and data protection clauses are signed-off by the service provider. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on the processing of personal data in relation to the collection of misleading invoices addressed to the users: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/2049e269-42a2-46e7-89e3-7c8d220081d9
EDPS Prior consultation	NO



Reference number	DPR-2019-047 (Update of DPN-2015-002)
Name of the processing operation	Processing personal data for the prevention and management of conflicts of interests - EUIPO Management Board (MB) / Budget Committee (BC) - Members, experts and advisers
Last Updated:	30/05/2019
Controller Organizational entity	Other
Controller contact details	Chairperson of the MB/BC under the following mailbox: MBBCSecretariat@euipo.europa.eu EUIPO, Avenida de Europa 4, 03008 Alicante, Spain
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The management of the declaration of interests is necessary to encourage the highest standards of administration, professional ethics, integrity and independence.</p> <p>It deals in particular with the following :</p> <ul style="list-style-type: none">- participation of the MB/BC Members in a Preparatory Subcommittee (PSC), to carry out the preparatory work to submit a proposal to the MB to decide on the appointment of the members of the Boards of Appeal, and to carry out the preparatory work to submit a proposal to the MB to decide on a list of candidates to be sent to the Council for the appointment of the Executive Director, the Deputy Executive Director and of the President and the Chairpersons of the Boards of Appeal;- previous activities /current activities of the MB/BC Members, experts or advisers;- financial interests related to EUIPO activity;- spouse's/legally recognised partner's/dependant family member's current professional activity and financial interests that might entail a risk of conflict of interests. <p>The Declaration of Interests does not contain an exhaustive list of potential interests. The processing of personal data includes any other element indicated by the data subjects that may affect their independence.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>Data are processed in compliance with EUIPO's MB/BC Guidelines on Conflict of Interests.</p> <p>The purpose of the processing of data is to examine declarations provided by MBBC Members, experts and advisers when they consider relevant to declare specific interest of the data subject.</p> <p>It serves to:</p> <ul style="list-style-type: none">- identify and disclose, in a transparent and consistent manner, the handling of situations where potential conflicts of interests may arise in order to avoid any conflict between the EUIPO public duties and any kind of private interest;- assess whether or not the declarations are incompatible with their obligations or constitute a risk for the EUIPO (real or potential impact in the EUIPO activities such as to impair the person's independence at EUIPO).
Data Subjects	EUIPO Management Board (MB) / Budget Committee (BC) members, experts and advisers



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed:</p> <ul style="list-style-type: none">- Forename/surname of MB/BC Members, experts or advisors;- Forename/surname of spouse/legally recognised partner/dependent family member and his/her employer/professional position. <p>Interests that are or could be related to the activity of EUIPO and which may have a potential impact such as to impair the person's independence as MB/BC Member, expert or adviser:</p> <ul style="list-style-type: none">- Past activities: posts held and professional activities held over the past 2 years (nature of the post, dates, name of the employer, foundation, institution or other organization);- Current activities: posts and professional activities held (the same data as those required for past activities);- Financial interests: shares/stocks exceeding 50 000€ or equivalent in the capital of companies having an interest related to the EUIPO activity and/or any assets or any intellectual property rights;- Spouse's/legally recognized partner's/ dependent family member's current professional activity and financial interests that might entail a risk of conflict of interests;- Any other relevant interests that may have a potential impact in the EUIPO activities.
Retention period	<p>Data will be kept during a period of 5 years after the end of the mandate/contract or activity.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Access is given to:</p> <ul style="list-style-type: none">- the Chairperson of the MB/BC;- the Deputy Chairperson or the longest serving member or the oldest one (only in the situations foreseen in point 6 of the Guidelines on Conflict of Interests);- the authorised persons working in the secretariat of the MB/BC. <p>Access to this data which is of a personal nature is determined by strict rules and is based on the needs of the procedure.</p> <p>Accessibility to the public:</p> <p>The Office will publish in its website the Guidelines on the prevention and management of conflict of interests together with:</p> <ul style="list-style-type: none">- the names of the MB/BC Members, experts and advisers, together with the names of the organisation they are representing;- the minutes of the MB/BC meetings along with the list of participants. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>The IT applications are password protected under single-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data herein.</p> <p>EUIPO Information Systems (IT) have a limited number of authorized staff (internal or external) administrating the IT Systems and having thus access to all electronic data of the Office.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>A declaration of confidentiality is signed by the persons having access to the data.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on Prevention and Management of Conflict of Interests - Declaration of Interests (MBBC):</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/5e13cc8e-7d4e-41d4-8228-299cd39c1804</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-049
Name of the processing operation	OD FTE Table and Smart Display
Last Updated:	11/06/2019
Controller Organizational entity	Operations
Controller contact details	ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>1</p> <p>Privacy Statement on the processing of personal data in the context of the OD FTE Table and “Smart Display”</p> <p>The protection of your privacy is of high importance to the European Union Intellectual Property Office (‘EUIPO’ or ‘us’ or ‘the controller’) and we feel responsible for the personal data that we process on your behalf. Therefore, we are committed to respecting and protecting your personal data and ensuring the efficient exercising of your data subject’s rights. All the data of personal nature, namely data that can identify you directly or indirectly, will be handled fairly and lawfully with the necessary due care.</p> <p>This processing operation is subject to the Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. The information in this communication is given pursuant to Articles 15 and 16 of the Regulation (EU) 2018/1725.</p> <p>1. What are the nature and the purposes of the processing operation?</p> <p>This processing operation consists of compiling data that are already available in different EUIPO applications, and are covered by specific Data Protection Records and Privacy Statements.</p> <p>The data processed is:</p> <ul style="list-style-type: none">• production data (volumes) of Operations Department (OD) examiners, as available in Kibana• time dedication to different areas of activity for OD Staff, available in the Task Allocation module in Allegro (updated only once per quarter) collected in an Excel table, as established by the Head of Service. It can vary monthly. <p>The “Smart Display” is an Excel sheet with formulas that combines all of that information with the help of an Access database into a user-friendly read-out clearly indicating the absolute numbers and the proportional percentages of completion of all areas of production activity of the examiner. The “Smart Display” was developed following a recommendation of the Working Group set up in the OD after the Staff Satisfaction Survey in 2018. Examiners had wished for a tool that would allow each examiner to look at his/her achievements in relation to the individual objectives (i.e. reference numbers) at any given point in time. Following this suggestion, the “Smart Display” will be available to all OD examiners to quickly follow-up on their production in terms of absolute numbers of decisions taken and/or tasks executed, considering their weighting and putting them into relation to the time dedicated to these tasks and the yearly reference numbers set for the Department in the “Note on Objectives”. The “Smart Display” does not take into consideration non-production activities, i.e. so-called “horizontal tasks”. No other factors (e.g. experience, quality, timeliness) that might be of relevance when looking at the individual performance as a whole are taken into consideration.</p> <p>The information will also be available for the Team leader (TL) and the Head of Service (HoS) and will significantly ease the cumbersome calculations done today.</p>



Purpose of the processing	<p>The purpose of this activity is to:</p> <ul style="list-style-type: none">a) Provide examiners with a quick reference to their production volumes on a daily basis that takes their dedication to the respective area of activity into account.b) Harmonise the way examiners and reporting officers calculate the completion of the reference numbers taking the relative dedication to different areas of activity into account;c) Provide TLs with the same reference for all their team membersd) Provide the HoS with the same reference for all the jobholders in the service. <p>The processing is not intended to be used for any automated decision making, including profiling.</p>
Data Subjects	OD examiners
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Staff member's first name, last name, login, team, statutory link, the areas of activity (same as in the Task allocation section of Allegro)</p> <ul style="list-style-type: none">• Staff member's time dedication (in percentages of Full Time Equivalent (FTE)) to the various areas of work, e.g. 20% in EUTM Examination, 30% Opposition Proceedings, 20% in KC, 30% in coaching, etc.• Staff member production data (same as in the Kibana individual report). <p>All of the production data used for measurements are extracted from the relevant IT application (Kibana). The data processed using the EUIPO applications are currently stored in different production databases such as the EUIPO Website and eBusiness systems, IP Tool, Madrid Protocol System (MPS), RCD (Eurodesign), Euroclass, EuroNice, Common Payment System (CPS), Classification, Template Manager (COR), SEARCH, Madrid Protocol Communication (MPC), Person Module (PER), Publications (PUB), Language Checker (LCT), QFMan, FileNet, Document Access Service (DAS), UQCT, e-Platform, SAP and Allegro.</p>
Retention period	<p>All production data and the personal data relating to trade marks and designs examination is stored in the back office tools for an indefinite period.</p> <p>The Smart Display shows snapshots of the current production of the examiners and will not keep any record.</p> <p>The Access database back-up and historical copies shall be kept for no more than two years after the end of the appraisal period in order to allow the management to use the data for the appraisal of the staff members concerned, and the latter to exercise their rights as provided for in the internal rules on appraisals and/or in Article 90(2) SR. After this period, all individual data extracted in electronic form shall be deleted and no longer archived, and all other copies in any form shall be destroyed, unless they need to be kept longer to establish, exercise or defend a right in a legal claim pending before the court.</p>
Recipients of the data	<p>Access to the excel sheets and Access database will be granted as follows:</p> <ul style="list-style-type: none">• Smart Display: each examiner has access only to the calculation concerning her/his own production; access is given with their Windows credentials. The TL has access to the calculation for each member of the team, and the HoS – to the entire service;• FTE Table: OD Secretariat have modify access, OD Management and TLs have read only access (access is set in a restricted ShareDox folder).• Access database: OD Secretariat and three duly authorised OD Quality, Performance and Risk Officers have modify access with a password only. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	The standard security measures of the EUIPO Information Systems are applied: <ul style="list-style-type: none">- EUIPO username and password required in order to access EUIPO network and systems.- Authentication and authorization based on roles.- Authentication and authorization at server level, no anonymous access allowed.- Server is physically protected at the Data Processing Centre.- Logical security hardening of the servers.- Network security configured to prevent external threats from accessing the mail servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement FTE TABLE and SMART DISPLAY: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/d404bb1b-cb17-4db1-b3b0-893582bf34c3
EDPS Prior consultation	NO



Reference number	DPR-2019-050
Name of the processing operation	Processing operations of personal data on EUIPO Directories - Insite "My Portal" / "Who is Who" / "Who to Contact" (Photo publication)
Last Updated:	20/02/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Head of the Entitlements and Staff Welfare Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing of data consists of making available the photo of EUIPO's staff members (officials/ temporary agents/contract agents) on the directories of the Office "myPortal" / "Who is Who" / "Who to Contact", only for the data subjects who have given their prior consent. It also concerns Seconded National Experts (SNE's), Trainees and Agency staff (interims).</p> <p>In "myPortal", the persons concerned can give consent for the publication of their photo. The revocation of consent can also be expressed at any time.</p> <p>Personal data of EUIPO staff is actually processed on HR database "Allegro" / Alfresco (Sharedox), Open Text, Excel/ Access and "SAP SuccessFactors" in the cloud .</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purposes of publishing your photo on the Office's directories is facilitating the search of the EUIPO staff, enabling a collaborative culture and promoting the internal communication and the staff engagement according to the Line of Action 1 of the Strategic Plan 2020.
Data Subjects	- EUIPO's staff members (officials / temporary agents / contract agents); - Seconded National Experts (SNE's) / trainees / agency staff (interims).
Description of categories of persons whose data EUIPO processes and list of data categories	The photo of EUIPO staff members, SNE's, Trainees and Interims having given consent for its publication on the Directories of the Office "myPortal" / "Who is Who" / "Who to Contact".
Retention period	<p>For data subjects having given consent for the publication of the photo on the directories of the Office appearing in Insite, data will be kept until the end of service of the person concerned.</p> <p>In case of revocation of consent, the photo will be withdrawn from the directories in the maximum period of 15 days.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Access to the data subject's photo taken by the Security Service is given to:</p> <ul style="list-style-type: none">- EUIPO's Internal staff (officials, temporary and contract agents);- EUIPO's external staff (only those who have been granted access to Insite on a need to know basis (e.g.: seconded national experts/ trainees /agency staff/ consultant/ expert). <p>Access may be allowed on a temporary and restricted basis to IT-technicians for customization, development, updating, technical tests, repair, support and improvement of the directories.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The access to the directories of the Office appearing in Insite ("myPortal" / Who is Who"/ Who to Contact") and to the HR database "Allegro" and "SAP SuccessFactors" are given individually to each profile following the type of job at EUIPO, HRD, staff member, line manager, Director, AIPN/ AACC or IT-technician.</p> <p>The Office's directories and HR database are password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited.</p> <p>Cloud systems "SAP SuccessFactors" have 24/ 7 security monitoring and alerting, security incident and threat response procedures, and automated security measures to prevent unauthorised access.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing of data on EUIPO Directories-"My Portal"/"Who is Who"/"Who to Contact"- Photo Publication:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/56583eee-30a7-4dda-8650-be6274445e29</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-051
Name of the processing operation	Record of the data processing in the IP Enforcement Portal
Last Updated:	26/05/2020
Controller Organizational entity	Observatory
Controller contact details	observatory@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>For the exchange of information function (EDB):</p> <p>The tool holds data on registered IP rights, contact information, supplementary product information and logistics entered by the rights holders. This information can be used by EU enforcement authorities in order to detect counterfeit products.</p> <p>The mentioned information is introduced by companies or their representatives. Companies (rights holders) are the owners of the information and therefore they are the ones in charge of controlling the quality of the information that they introduce.</p> <p>The work of the EUIPO, whenever a new company joins the system, is to validate the request, create the company and the master user of this company. The rest of users will be managed by the company master user.</p> <p>E-filing of Customs Applications for Action (AFAs):</p> <p>Personal data contained in the AFAs that rights holders can file electronically through the EDB to the European Commission's central IP database COPIS (as per Regulation (EU) No 608/2013 on Customs enforcement of IPR), is transferred to said central database.</p> <p>The EUIPO, through the Observatory, only acts as a processor of the data contained in the AFA on behalf of the controllers of COPIS (the national Custom authorities). No AFA personal data on possible infringers is stored in the Enforcement Database</p> <p>For the recording of IP enforcement cases in non-EU countries (ACRIS), the information is used by the EU Commission (DG Trade) for statistical purposes. Users report, in a structured format, all data relating to cases of intellectual property rights' infringements affecting EU companies in countries outside the EU and the corresponding enforcement actions with local authorities.</p>



Purpose of the processing

The purpose of the exchange of information function of the IP Enforcement Portal is to help enforcement agencies to better identify counterfeit goods with the help of the IPR, product and contact information entered by the rights holders (companies).

In addition, the e-mail addresses of the master users are used

- to circulate internal information about the EDB, such as new functionalities or any updates in the current ones, or to provide new use instructions;
- for automatically generated notifications from the system to users, such as when a new user account has been created;
- to inform users about other services or products provided by the Observatory within its legal mandate (knowledge building, awareness events, publication of studies on IPR);
- to circulate invitations to periodical enforcement Fora;
- to carry on surveys aiming at measuring the performance of the system and/or fine-tuning its applications.
- to share with enforcement authorities of the EU Member States, Europol and OLAF for enforcement operations carried out by these authorities. (See related

Record:

<http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/360fd21d-25a2-456d-b657-2511f51f9cbf>

and Privacy Statement:

<http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/d07b1332-c58d-4fab-ad5f-82d5cb64555f>

The purpose of the record of non-EU cases function is

- to produce relevant statistical information to assess the level of infringements of intellectual property rights (IPR) in third countries;
- to provide the Commission with information about concrete IP problems faced by EU companies outside the EU and make use of this information in the context of the 'IP Dialogues';
- to measure the efficiency of actions taken by enforcement authorities against counterfeiting;
- to allow rights holders to share information on infringements of IPR and related enforcement actions in third countries ('cases'), by making anonymised statistics from the tool available to all users. This provides users an overview of infringement business models and trends in enforcement, without having access to specific case details or information on which companies loaded the cases in the IP Enforcement Portal.



Data Subjects

For the exchange of information function:

- Rights holders, or their legal representatives, in possession of the security code assigned by the EUIPO; name, surname, e-mail address and telephone number;
- Individual contact persons authorized by the above IPR holders; name, middle name and surname, employee's company, language, professional e-mail address and telephone number;
- For the creation of the profiles of the authorities not accessing using the CCN network, name, surname, the professional e-mail address and the static IP addresses of the enforcement authorities they work for.
- Officers of law enforcement authorities, national IP Offices and other institutions and agencies active on protection of IP, can, voluntarily, share their individual contact details with specific rights holders through the tool.

For the record of non-EU cases function:

IPR holders (and IPR helpdesks) can enter the details of points of contact, specifically the name, surname and email address of the person within the company in charge of the file, even though this information is not mandatory. This personal data can be loaded by different types of users as defined in the 'IP Enforcement Portal Legal Notice', and it is stored and processed when they log in to the database with the appropriate credentials.

As stated in the legal notice, the Office is not responsible for information uploaded by the users. In particular, users should take all reasonable steps to ensure that personal data which is inaccurate, incomplete or no longer up to date is not entered into the database.

Users can search for their own cases and edit the information at any time. However a user cannot access cases uploaded by other users if they have not been authorised to do so by an administrator or company master user.



<p>Description of categories of persons whose data EUIPO processes and list of data categories</p>	<p>For the exchange of information function:</p> <ul style="list-style-type: none">- Rights holders, or their legal representatives, in possession of the security code assigned by the EUIPO; name, surname, e-mail address and telephone number;- Individual contact persons authorized by the above IPR holders; name, middle name and surname, employee's company, language, professional e-mail address and telephone number;- For the creation of the profiles of the authorities not accessing using the CCN network, name, surname, the professional e-mail address and the static IP addresses of the enforcement authorities they work for.- Officers of law enforcement authorities, national IP Offices and other institutions and agencies active on protection of IP, can, voluntarily, share their individual contact details with specific rights holders through the tool. <p>For the record of non-EU cases function:</p> <p>IPR holders (and IPR helpdesks) can enter the details of points of contact, specifically the name, surname and email address of the person within the company in charge of the file, even though this information is not mandatory. This personal data can be loaded by different types of users as defined in the 'IP Enforcement Portal Legal Notice', and it is stored and processed when they log in to the database with the appropriate credentials.</p> <p>As stated in the legal notice, the Office is not responsible for information uploaded by the users. In particular, users should take all reasonable steps to ensure that personal data which is inaccurate, incomplete or no longer up to date is not entered into the database.</p> <p>Users can search for their own cases and edit the information at any time. However a user cannot access cases uploaded by other users if they have not been authorised to do so by an administrator or company master user.</p>
<p>Retention period</p>	<p>Taking into account the purpose of the IP Enforcement Portal, the fact that registration in the database is made by users on a voluntary basis, and that the information stored can be used by enforcement authorities for the purpose of detection of counterfeited goods, the personal data will be stored in the database as long as it is not deleted by the master user or sub-account user, or by the system administrators on their behalf.</p> <p>When it comes to the record of Non-EU cases, no personal data is used for the statistics used by DG Trade. Any personal data entered by the user, will be stored in the database as long as it is not deleted by the master user or sub-account user, or by the system administrators on their behalf.</p>



Recipients of the data	<p>For the exchange of information function:</p> <p>The following have access to data:</p> <p>Within EUIPO:</p> <ul style="list-style-type: none">- for the purpose of creation and maintenance of the accounts, the Enforcement Portal Team, a reduced number of Customer Department staff and the system administrators, on a strict need to know basis- With regards to the rights holder accounts and the information included, EUIPO has access only to the product information of products shared by the rights holder with the EUIPO IP Enforcement Portal team for the purpose of training enforcement authorities.- Apart from the above, EUIPO only has access to the information of master users and subaccount holders (name, surname and e-mail address). <p>Outside EUIPO:</p> <ul style="list-style-type: none">- right holders' master users and sub-account users, and right holder's authorised representatives, for data related to their respective company only; <p>The enforcement authorities that are registered in the Portal.</p> <ul style="list-style-type: none">- officers within law enforcement authorities and other institutions, with a profile to access the system, for contact data of all companies registered in the Portal (name, surname, address, e-mail address, telephone and fax numbers, countries covered, products covered, languages, if the contact can answer technical or legal questions and the type of contact for the company – main or secondary) <p>For the record of non-EU cases:</p> <p>Personal data is disclosed to the following recipients:</p> <p>Within EUIPO:</p> <ul style="list-style-type: none">- EUIPO IT operators and the system administrator, only for the purposes of resolving technical or functionality issues, or performing technical maintenance.- Neither master users nor sub-account users can create, modify or delete contact point data. Observatory users can access, in read-only mode, the personal data of companies' points of contact for cases that have been uploaded in the IP Enforcement Portal. <p>Outside the EUIPO:</p> <ul style="list-style-type: none">- IPR holders and IPR helpdesks: Master users can create, modify and delete their own companies' contact point. Sub-account users can create their own companies' contact point, but are not allowed to modify or delete existing ones.- EU delegations: Neither master users nor sub-account users can create, modify or delete points of contact. EU delegation users can access, in read-only mode, the personal data of companies' points of contact for cases that have been uploaded in the tool. However, they can only access cases from the regions where they operate.- Directorate General for Trade: Neither master users nor sub-account users can create, modify or delete points of contact. Directorate General for Trade users can access, in read-only mode, the personal data of companies' points of contact for cases that have been uploaded in the tool.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Security is ensured by the EUIPO's general security policy. In the framework of its Information Security Management Policy, EUIPO is certified to ISO 27001 standards.</p> <p>All personal data are stored in EUIPO's servers.</p> <p>The IP enforcement Portal is password protected and the creation of an account is based upon a security code assigned by EUIPO.</p> <p>Additionally, for the exchange of information between rights holders and enforcers, security is ensured as follows:</p> <ul style="list-style-type: none">- enforcers' profiles are created in the secure Customs Communication Network (CCN) of the European Commission. Communication via the CCN is based on identification, authentication and authorisation under the control of a national responsible;- enforcement authorities not able to connect using CCN, access via a static IP address. In such a case, profiles are created by the system administrators of EUIPO under the control of a single point of contact in the enforcement authority.- for companies, the system has a 2 level protection: password and pin-safe.- Rights holders/users do not see the information of the other account. They only have access to their own account. <p>Moreover, in order to ensure the highest level of security to its IT systems including the IP Enforcement Portal (former EDB), EUIPO is certified with Service Organization Control (SOC)-2 standards. The SOC2 report focuses on a business's non-financial reporting control, based upon the internationally recognized "Trust Service Principles" of security, availability, processing integrity, confidentiality and privacy, ensuring in particular that systems:</p> <ul style="list-style-type: none">- are logically and physically protected from unauthorized accesses;- are available for committed or agreed use;- are complete, accurate, timely and authorized in processing;- protect information that is designated "confidential" as committed or agreed;- collect, use, retain and disclose personal information in conformity with the commitments of the entity's privacy notice and with privacy international standards. <p>SOC-2 certification is a recurrent process, being EUIPO subject to yearly independent audit.</p> <p>Therefore, EUIPO ensures the highest standard of security be applied to the IP Enforcement Portal.</p> <p>See link to a summary of the report</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/4b09d773-c27a-4077-9d74-37aaa7f640c6</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Data Protection Statement on the processing of personal data in the context of the EUIPO's IP Enforcement Portal: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/2261f8dc-4186-4e4cb-82c5-6e4a6e8266c2
EDPS Prior consultation	NO



Reference number	DPR-2019-052
Name of the processing operation	RECORD IP Enforcement Portal user list for operations by enforcements authorities
Last Updated:	03/06/2019
Controller Organizational entity	Observatory
Controller contact details	Observatory@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Enforcement authorities of the Member States, Europol and OLAF approach the Observatory, to use its networks to reach out to rights holders of a certain sector for their support in enforcement operations.</p> <p>The Observatory provides the enforcers with the name and e-mail addresses of the companies/rights holders, or their Legal Representatives, in possession of the security code assigned by the EUIPO (master users), which will be asked if they are willing to provide intelligence for the particular enforcement operations. This list is sent in the form of an encrypted excel file.</p> <p>This does not include the information on the contact points included in the IP Enforcement Portal, as EUIPO has no access to this information.</p>
Purpose of the processing	One of the mandates of the Observatory is to support the communication between enforcements authorities and rights holders. This process helps enforcers to get hold of the rights holders, to facilitate the enforcement operations.
Data Subjects	Rights holders, or their legal representatives, in possession of the security code assigned by the EUIPO; company, name and e-mail address.
Description of categories of persons whose data EUIPO processes and list of data categories	Rights holders, or their legal representatives, in possession of the security code assigned by the EUIPO; company, name and e-mail address.
Retention period	The list of emails of master users of companies from a certain sector of industry that are forwarded to the enforcement authorities to support their operations, are created ad hoc, extracted from the accounts register of the IP Enforcement Portal and not stored in the EUIPO archives, but just forwarded per e-mail to the official in charge of the enforcement operation.
Recipients of the data	The enforcement officials of the Member States, Europol and OLAF that are in charge of the operations.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	All personal data related this process is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Data protection statement on processing personal data in the context of the EUIPO's IP Enforcement Portal user list for operatio: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/d07b1332-c58d-4fab-ad5f-82d5cb64555f
EDPS Prior consultation	NO



Reference number	DPR-2019-053
Name of the processing operation	Processing personal data within the framework of the agreement between EUIPO and the European School of Alicante (After School Children's Nursery)
Last Updated:	06/06/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service (HRD) . European School of Alicante (After School Children's Nursery El Faro) – EULEN
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In the framework of the EUIPO's social policy, the after-school nursery has been set up collaboratively by the EUIPO and the European School of Alicante in order to provide parents working at the Office alternative care of their children aged up to 12 years during working hours, when the schedule school has finished.</p> <p>According to the European Commission grid for nursery costs (from group I / up to group XII), the monthly amount to be paid by EUIPO's statutory staff members to the European School for the after school nursery of their children depends on the composition of their family and their monthly net income.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The processing of data by the Human Resources Department (HRD) is necessary to verify the situation of EUIPO's statutory staff members with dependent children attending the nursery (composition of family / net income) in order to send a confirmation to the European School regarding the monthly amount that shall be paid by the parents relevant to the school nursery.
Data Subjects	EUIPO staff members (officials / temporary agents and contract agents)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data are processed only on a need to know basis:</p> <p>Staff member and other family members:</p> <ul style="list-style-type: none">- Name, surname and personal number;- Composition of the family (number of dependent children/persons);- Income (salary slips) of the children's father / mother working at EUIPO;spouse (children's father / mother) not working at EUIPO;- Unemployment certificate of the children's father/ mother (if applicable);- Proof of payment / absence of payment of allowances received by the children's father / mother (if applicable). <p>Staff member's children enrolled at the after school nursery:</p> <ul style="list-style-type: none">- Name / surname;- Option of attendance at the after school nursery (full time/part time).
Retention period	<p>Data processed and stored in Outlook and paper files are kept during a period of time not longer than 1 school year (from beginning of September (Y) / up to the end of September (Y + 1).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Data are disclosed to authorised staff of HRD working on these files. Data can also be disclosed to the management of HRD, the Appointing Authority (AA)/ Authority Authorized to Conclude Contracts (AACC) and the Social Assistant (HRD).</p> <p>EUIPO contractors and subcontractors might have access to data for maintenance and development of the applications supporting “HR Allegro” and “SAP SuccessFactors” under request and supervision of EUIPO.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Personal data are stored in secure cupboards (HRD) and IT applications (Outlook, HR “Allegro” database and “SAP SuccessFactors” in the cloud (e.g.: names, composition of the family / number of dependent children /relatives) according to the security standards of EUIPO, as well as in specific electronic folders.</p> <p>Data are accessible only to authorised persons working in these files. Appropriate levels of access are granted individually only to the above recipients.</p> <p>The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. “SAP SuccessFactors” is also certified in ISO 27001.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing personal data in the framework of the agreement between EUIPO and the European School (After School Nursery):</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/0150894f-cba4-4571-b462-821a8bb05554</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-057
Name of the processing operation	Register of recommended Training DTD
Last Updated:	20/06/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The process aims to facilitate the learning on different training courses that are recommended. The persons that did the training will leave an opinion or feedback about it. This will help the rest of the staff to choose better between the different courses.</p> <p>The exercise is voluntary; DTD staff is not required to mandatorily provide this information.</p>
Purpose of the processing	-Identify reference persons within the learning course. -Have feedback on the different learning courses.
Data Subjects	DTD Internal Staff
Description of categories of persons whose data EUIPO processes and list of data categories	With regard to persons information, the process supplies the following data: o First name/ Middle name/ Last name o Opinion/feedback on the training
Retention period	All the personal data will be kept for five (5) years.
Recipients of the data	DTD Internal Staff will have access to the entire register of information.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	For this process, the standard security measures of the EUIPO Information Systems is applied: <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/9dd14406-2aa6-4c83-b179-0b683070bce0
EDPS Prior consultation	NO



Reference number	DPR-2019-058 EUIPO Trade Mark and Design Education Programme
Name of the processing operation	Management of personal data for the EUIPO Trade Mark and Design Education Programme
Last Updated:	10/06/2019
Controller Organizational entity	Academy
Controller contact details	DPOexternalusers@euipo.europa.eu
Name and contact details of processor	<ul style="list-style-type: none">• EUIPO Trade Mark and Design Education Programme project team, and the Members of the Steering Committee and the Examination Board (some of them are EUIPO staff and others are not).• EUIPO Academy Department for activities related to the administrative functioning of the ETMD Education Programme and for the administration of the e-Learning course in the Academy Learning Portal (Moodle) in accordance with DPR-2018-004.• Deloitte, as an external processor providing services to Human Resources Department (consultancy services related to the EUIPO ALP), for project support to the ETMD Education Programme may have access to the data.• EUIPO Infrastructure and Buildings Department as internal processor and Pomilio Blumm as external processor, providing services to IBD as described in DPR-2019-007.• EUIPO Digital Transformation Department for the management of IT systems involved.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

The EUIPO Trade Mark and Design Education Programme is a new training activity addressed to legal practitioners qualified in one of the Member States of the European Economic Area or professional representatives admitted and entered on the lists maintained by the EUIPO, in accordance with Art. 120 (1)(b) EUTMR and Art. 78 (1)(b) CDR.

The processing of the data will be automated.

I. Candidates (Participants after the enrolment)

- Candidates will submit the application for inscription electronically through the section created specifically for this purpose. The personal data provided by the Candidates in the application form, including the financial data revealed as a consequence of the payment of the course fees, will be processed as described in DPR-2019-007.
- The Candidates that will be accepted to the Education Programme, hereafter the Participants, will be instructed to provide their EUIPO website user accounts (to create an account in the case of new users) in order to be enrolled in the Education Programme e-learning course in the Academy Learning Portal.
- The activities in the scope of the eLearning course such as: results of electronic self-assessment tests; participation in forums or discussions; submission of written assignments will fall under the scope of the EUIPO Academy Learning Portal DPO Notification DPR-2018-004.
- Final examination, consisting of written and oral exam, will be conducted at the end of the course. The examination papers of the written exam will be submitted anonymously by using a reference code that each Participant will be assigned by the Project team. The correlation between the codes and participant's names will not be revealed to the Examination Board.
- The successful Participants will be granted a Certificate. The Steering Committee may decide to publish the list of the successful Participants in the Official Journal of the EUIPO or in another section of the EUIPO's corporate website. Nevertheless should this be the case, the successful Participants will be asked to give their explicit consent prior to the publication.
- Possibility to be part of an Alumni scheme is envisaged for the successful Participants. The Alumni will be asked to give their consent prior to the inclusion in the Alumni scheme after the end of the final examination. However, the possibility to request inclusion in the Alumni scheme at their convenience, at a later stage, will remain open upon provision of their consent.

II. External teachers

- External teachers for the purposes of the ETMD Education Programme will be proposed by the Steering Committee.
- Personal data, including financial data will be processed by Pomilio Blumm, as per DPR-2019-007, in order to manage the travel arrangements, access to EUIPO premises and payment of the fee for the lectures.
- Consent to be recorded, to live stream the lecture and to use the recording and the lecture material in the framework of the Academy Learning Portal will be requested from the external teachers when the offer to participate in the Education Programme will be placed.
- Opinions or feedback provided as evaluation of the Participants' activities in forums or workshops.

III. Members of the Steering Committee and the Examination Board

- Personal data, including financial data will be processed by Pomilio Blumm, as per DPR-2019-007, in order to



manage the travel arrangements, access to EUIPO premises and payment of the DSAs for their participation in meetings or eventually payment of fees for revision of exam papers and conduct of oral examination.

- Opinions of the Examination Board members expressed as part of the assessment of exam papers and the aural examination.



Purpose of the processing	<p>I. The processing of the candidates' (participants after the enrolment) data is necessary for</p> <ul style="list-style-type: none">• Inscription and identification of the participants in the course,• Payment of the course fees,• Enrolment in the e-Learning course on the Academy Learning Portal,• Admission to final examination• Records of successful participants for the purpose of inclusion in the Alumni scheme or issuance of Duplicate of a Certificate. <p>II. The processing of the external teachers' data is necessary for:</p> <ul style="list-style-type: none">• Organisation of travel arrangements and access to EUIPO premises,• Payment of the fees for the lecture,• Recording and/or live streaming of the lecture, preparation of e-Learning content for the purposes of the Academy Learning Portal. <p>III. The processing of the Members of the Steering Committee's and the Examination Board's data is necessary for</p> <ul style="list-style-type: none">• Organisation of travel arrangements and access to EUIPO premises,• Payment of the DSAs or fees for revision of exam papers and conduct of oral examination,• Use of opinions expressed in the scope of examination in order to assess the exam mark.
Data Subjects	<p>I. Candidates (Participants after the enrolment)</p> <p>II. External teachers</p> <p>III. Members of the Steering Committee and the Examination Board</p>



Description of categories of persons whose data EUIPO processes and list of data categories

I. Candidates (Participants after the enrolment)

- Identification data

- Name and surname,
- Date of birth,
- Nationality,
- Address,
- EUIPO Representative ID number,
- Valid copy of passport or ID,
- Telephone number,
- E-mail address and EUIPO user account,
- Diploma for finished Law studies or Certificate of membership in a Bar association (in exceptional cases).

- Financial data

- Bank account details / credit card details

- Health data

- Medical certificate proving inability to follow the course (only in exceptional cases).

II. External teachers

- Identification data

- Name and surname,
- Valid passport or ID number,
- Telephone number,
- E-mail address.

- Financial data

- Bank account details.

- Specific data

- Personal image (recording of the lecture),
- Opinions expressed as evaluation of the Participants.

III. Members of the Steering Committee and the Examination Board

- Identification data

- Name and surname,
- Valid passport or ID number,
- Telephone number,
- E-mail address.

- Financial data

- Bank account details.

- Specific data

- Opinions expressed as part of the assessment of exam papers and the aural examination.



Retention period	<p>I. Candidates (Participants after the enrolment)</p> <ul style="list-style-type: none">• Personal data of Candidates whose applications will not be accepted will be deleted within 1 month after the end of the registration phase.• The activities in the scope of the eLearning course such as: results of electronic self-assessment tests; participation in forums or discussions; submission of written assignments etc. will be governed by the EUIPO Academy Learning Portal DPO Notification and Privacy Statement and the retention policy applicable to the Academy Learning Portal. Access to the eLearning Course will be removed 3 months from the communication of the final results to the Participants.• The exam papers from the written exam and the evaluations of the oral exam will be kept until the end of the Appeal procedure of the corresponding course cycle, which is 3 months (from the notification of the results) then they will be destroyed.• Personal data of the participants who will not pass the final examination will be kept for 12 months from the final decision confirming the failing grade in order to allow them to participate in the next course cycle and sit the final exams again.• List of successful Participants will be kept for 50 years after the end of the corresponding course cycle in order to be able to assess petitions for inclusion in the Alumni scheme or petitions for issuing a duplicate of the Certificate.• Medical certificates, requested only in exceptional cases, will be kept 1 month after the collection takes place. <p>II. External teachers</p> <ul style="list-style-type: none">• Recordings of presentations of external teachers will be used in the eLearning course and will be governed by the EUIPO Academy Learning Portal retention policy. <p>III. Members of the Steering Committee and the Examination Board</p> <ul style="list-style-type: none">• Opinions of Examination Board members expressed during evaluation of the exam papers and the oral exam will be kept until the end of the Appeal procedure of the corresponding course cycle, which is 3 months (from the notification of the results) then they will be destroyed. <p>In addition, information related to the organization of the event will be retained as defined in the DPO notification DPN-2017-042 Organisation & Management of Meetings and Events. This includes:</p> <ul style="list-style-type: none">• Personal and financial data related to the enrolment of candidates.• Personal data necessary for travel arrangements of external teachers and members of the Steering Committee and the Examination Board.• Personal data necessary for payment of DSAs/lecture fees.
Recipients of the data	It is not foreseen that the personal data is disclosed to any recipients other than the processors, although fellow participants in the programme will have access to the list of participants.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The security measures will be the ones applicable to the EUIPO Academy Learning Portal and the EUIPO's documents management system ShareDox.</p> <ul style="list-style-type: none">• Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access will be allowed.• Access to the Education Centre section in the EUIPO Academy Learning Portal is restricted by username and password and subject to prior validation by the EUIPO Academy.• Authentication and authorization to view and access information based on roles.• Servers are physically protected at the Data Protection Centre.• Networking security configured to prevent external threats from accessing the servers. <p>Security measures for the information managed by Pomilio Blumm for the travel arrangements or financial enrolment are included in in DPO record DPR-2019-007.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>http://sharedox.prod.oami.eu/share/page/repository?file=PRIVACY%20STATEMENT%20ET... http://sharedox.prod.oami.eu/share/page/repository?file=PRIVACY%20STATEMENT%20ETMD%20EP%20-%20External%20trainers.docx#filter=path%7C%2FOffice_Docs%2FK%20INST%20AFFAIRS%2FK03%20DP%2FK0305%20DP%20Domains%2FDPC-ACAD%2F4.%20Records%2C%20notifications%2C%20privacy%20statements%2FETMD%20Education%20Programme</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-059
Name of the processing operation	Space management in EUIPO
Last Updated:	15/07/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Vincent Polomé, Head of Facility management service, IBD Workplace team , IBD External processor: Space management service providers: Servicio Movil S.L. and Ferrovial Servicios S.A External Mail Distribution provider EULEN IDOM Consulting IDASA sistemas (provider of ROSMIMAN® IWMS Global Site) and its subcontractor Acens Technologies, S.L.U.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The application ROSMIMAN® IWMS is used as a tool for the management and control of the staff workplaces (EUIPO internal staff & external resources). Personal data are processed in order to ensure that each member of staff is associated with his/her corresponding workplace. The space allocation to the staff is done through My Service Desk using the corresponding "request":</p> <ul style="list-style-type: none">• New staff / Move staff / Leave staff request used for Small moves (relocations);• Large moves request;• New teleworker request. <p>The request for Small moves is initiated by the corresponding department. In the end of the process, the information in ROSMIMAN® IWMS is actualised.</p> <p>The request for Large moves is initiated by the Workplace team in IBD. A table (T-0018-Plan de mudanza) with the related information is sent to DTD, Servicio Movil S.L., Ferroviaal and Mail internal distribution. In the end of the process, the information in ROSMIMAN® IWMS is actualised.</p> <p>DTD sends a list of teleworkers to the Team Leader of Workspace (for information) and Ferroviaal team or Servicio Movil S.L. (in order to perform the service).</p> <p>Personal data of people working in the EUIPO installations can appear as well in the plans/drawings of the Office spaces created through the use of the tool Autocad.</p> <p>The management of car park spaces for EUIPO TOP management staff members, people with reduced mobility and staff members with electric vehicles is done through the use of an Excel file stored in the document management system Shardox.</p>
Purpose of the processing	The purposes of the processing are: 1) to ensure that a concrete work or car park place is associated with the corresponding staff member/external resource and his/her related data; 2) to ensure the quality and the follow up on the performed service.
Data Subjects	All EUIPO staff and external resources working in EUIPO, as well as teleworkers.



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Personal data related to relocations are as follows: name, email, office phone number, type of contract, personal number, team, service, department, location and signature, IT equipment assigned. The personal data that can appear in the Autocad plans is only name, surname and location.</p> <p>Personal data related to teleworkers are as follows: name, surname, type of contract, % of teleworking, personal number, telephone number, personal address, equipment/furniture assigned.</p> <p>Personal data related to the management of car park spaces are as follows: type of car park space (EUIPO TOP management staff members, people with reduced mobility and staff members with electric cars), name, surname, department, plate number, car brand and model.</p>
Retention period	<p>In the space management tool ROSMIMAN® IWMS and in the Autocad plans (stored in the Autocad tool, Sharedox and in the (Y:) server) the data is stored for as long as the person works at the Office (in the case of teleworkers, the data is stored for the period the person works as teleworker).</p> <p>On paper, the data in the T-0093 Inventario personalizado mudanza (name, surname, signature, location) in case of large relocation are stored for the period of one month after the staff has been moved.</p> <p>The personal data T-0018-Plan de mudanza is stored for 1 year.</p> <p>The personal data in the Excel table for the management of car park spaces is retained till the person is authorised to park in one of these three types of car park space: spaces for EUIPO TOP management staff members' vehicles, spaces for vehicles of people with reduced mobility and spaces for staff members' electric vehicles.</p> <p>The data are stored in Outlook till it is needed for the performance of the service- relocation of teleworkers.</p>
Recipients of the data	<p>The following users have access to the data in Rosmiman:</p> <p>1) For control and supervision purposes: Facility management internal team in IBD has access as follows: Space Management Read/Write/ Modify/Delete Maintenance Management Read Inventory Read Administrator Full Access Role Space management accesses all fields except employee number. Roles Maintenance management and Inventory access all data except from employee number and type of contract. Role Administrator accesses all data.</p> <p>2) FM service provider Servicio Movil S.L. and Ferrovial in order to perform the service. The application administrators will be EUIPO staff. The tool provider can access the data only under previous authorisation of EUIPO.</p> <p>When external audit companies are auditing the space management process in EUIPO, they are given as well access to tool (including to the personal data).</p> <p>Mail Distribution team may receive data stored in Rosmiman in order to actualise its data base with all staff and resources working in EUIPO premises.</p> <p>Access to the table T-0018-Plan de mudanza is given to the Space management team, DTD, Servicio Movil S.L., Ferrovial and Internal mail distribution team.</p> <p>Access to the Excel table for management of car park spaces for EUIPO TOP management staff members, people with reduced mobility and staff members with electric vehicles is given to:</p> <ul style="list-style-type: none">- Space management team in IBD for the purpose of assignment and management of the spaces;- Maintenance management team in IBD for the purpose of the maintenance of the spaces;- Security team in IBD for the purpose of supervision of the Car Park Rules and management of car park breaches.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES



Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	The data is transmitted to the IDASA sistemas (provider of ROSMIMAN® IWMS Global Site) and its subcontractor Acens Technologies, S.L.U which stores the data on security-hardened and physically protected servers at a data processing centre in Madrid, Spain.
General Description of security measures	<p>All personal data in Rosmiman is stored in secure cloud system that complies with the recognized standard ISO 27001. The data is protected with access control measures and firewall system. Servers are security-hardened and physically protected at the Data Processing Centre in Madrid, Spain. Appropriate levels of access are granted individually only to the user groups listed above.</p> <p>For more information, please, consult the links towards Acens Infrastructure and Security requirements Rosmiman.</p> <p>All personal data in the document management system Sharedox is stored according to the security standards of the Office. Appropriate levels of access are granted individually only to the above recipients. The database is password protected under single sign-on system and automatically connected to the user ID.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/d1ef9654-8b2d-4d57-b4e9-71b774e843a6
EDPS Prior consultation	NO



Reference number	DPR-2019-060
Name of the processing operation	User Satisfaction Survey for the Newcomers entering into service at EUIPO
Last Updated:	15/07/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the User Satisfaction Survey for the Newcomers entering into service at EUIPO.</p> <p>The participation in this survey is fully voluntary and represents a regular consent to the processing of personal data within this survey. Newcomers are encouraged to participate in this survey as their feed-back is very important to improve the quality of the selection and recruitment processes, as well as the mentoring programme.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purpose of the processing of data is to receive feed-back from the newcomers entering into service at EUIPO in order to improve the quality service for the selection and recruitment processes, as well as for the mentoring programme.
Data Subjects	Newcomers entering into service at EUIPO.
Description of categories of persons whose data EUIPO processes and list of data categories	The email address of all persons concerned and their opinion.
Retention period	<p>Individual answers and all personal data collected will be deleted not later than 1 year after the anonymous results have been delivered. The anonymous statistic data will be kept according to EUIPO's retention period (5 years).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>The results with the answers of the aggregated and anonymised data of the survey will be accessible to:</p> <ul style="list-style-type: none">- the Director and Heads of Service of the Human Resources Department;- the EUIPO management;- a limited number of staff of the HRD (Internal Control Correspondent);- the IT staff processing the survey tool. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The collected personal data and anonymous answers are kept in the Common User Satisfaction Survey (Harmonized User Satisfaction Survey) - Lime Survey Servers.</p> <p>Anonymous reports are stored in Sharedox (Human Resources Department).</p> <p>Data is stored according to the security measures of the EUIPO's Information Systems. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the User Satisfaction Survey for the Newcomers entering into service at EUIPO:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f297d28b-e700-4820-aa1d-21a379050ecc</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-062
Name of the processing operation	Processing personal data within the framework of the User Satisfaction Survey regarding the Traineeship programme 2017-2018 at EUIPO
Last Updated:	09/07/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of Entitlements and Staff Welfare Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the User Satisfaction Survey regarding the Traineeship programme 2017-2018 at EUIPO.</p> <p>The participation in this survey is fully voluntary and represents a regular consent to the processing of personal data within this survey.</p> <p>Trainees are encouraged to participate in this survey as their feed-back is very important to improve the quality of the Traineeship programmes.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purpose of the processing of data is to receive feed-back from the trainees in order to improve the quality service for the Traineeship programmes at EUIPO.
Data Subjects	Trainees at EUIPO
Description of categories of persons whose data EUIPO processes and list of data categories	Trainees at EUIPO. The email address of all persons concerned and their opinion.
Retention period	<p>Individual answers and all personal data collected will be deleted not later than 1 year after the anonymous results have been delivered.</p> <p>The anonymous statistic data will be kept according to EUIPO's retention period (5 years).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The results with the answers of the aggregated and anonymised data of the survey will be accessible to:</p> <ul style="list-style-type: none">- the Director and Heads of Service of the Human Resources Department;- the EUIPO management;- a limited number of staff of the HRD (Internal Control Correspondent) and other Departments working in the Survey;- the IT staff processing the survey tool. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The collected personal data and anonymous answers are kept in the Common User Satisfaction Survey (Harmonized User Satisfaction Survey) - Lime Survey Servers.</p> <p>Anonymous reports are stored in Sharedox (Human Resources Department).</p> <p>Data is stored according to the security measures of the EUIPO's Information Systems.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data the User Satisfaction Survey for the Traineeship programmes:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/f3e1047d-dc7d-441a-8e29-08ff5a05ceaa</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-063
Name of the processing operation	Processing personal data within the framework of the User Satisfaction Survey for the Mentoring Programme at EUIPO
Last Updated:	13/09/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Head of Staffing , Development and Recognition Service
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Processing of personal data within the framework of the User Satisfaction Survey for the Mentoring Programme at EUIPO.</p> <p>The participation in this survey is fully voluntary and represents a regular consent to the processing of personal data within this survey.</p> <p>Staff members are encouraged to participate in this survey as their feed-back is very important to improve the quality of service for the Mentoring Programme.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purpose of the processing of data is to receive feed-back from the staff members participating in the Mentoring Programme in order to improve the quality of service.
Data Subjects	EUIPO staff members (officials/temporary agents/contract agents and Seconded National Experts participating in the Mentoring Programme.
Description of categories of persons whose data EUIPO processes and list of data categories	The email address of all persons concerned (staff members participating in the Mentoring Programme) and their opinion.
Retention period	<p>Individual answers and all personal data collected will be deleted not later than 1 year after the anonymous results have been delivered.</p> <p>The anonymous statistic data will be kept according to EUIPO's retention period (5 years).</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The results with the answers of the aggregated and anonymised data of the survey will be accessible to:</p> <ul style="list-style-type: none">- the Director and Heads of Service of the Human Resources Department;- the EUIPO management;- a limited number of staff of the HRD (Internal Control Correspondent);- the IT staff processing the survey tool. <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The collected personal data and anonymous answers are kept in the Common User Satisfaction Survey (Harmonized User Satisfaction Survey) - Lime Survey Servers.</p> <p>Anonymous reports are stored in Sharedox (Human Resources Department).</p> <p>Data is stored according to the security measures of the EUIPO's Information Systems.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data - User Satisfaction Survey for the Mentoring Programme at EUIPO: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/82eaa4c4-28d8-467e-926f-54f574670985</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-064
Name of the processing operation	Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO
Last Updated:	16/07/2019
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	Head of Staffing, Development and Recognition Service HRD
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO. The processing of data consists in collecting information and gathering evidence, accurate and validly obtained, into a file which will be submitted to the Appointing Authority (AA) or the Authority Authorized to conclude Contracts of Employment (AACC). The processing of personal data is not intended to be used for any automated decision making, including profiling.
Purpose of the processing	The purpose of the processing of data is to collect information and gather evidence into a file in order to enable the AA / AACC to determine whether there has been a failure by an official, servant or other person working for the Office, to comply with his/her obligations under the Staff Regulations (SR) and the Conditions of Employment of Other Servants (CEOS). The AA/ AACC will then evaluate whether a disciplinary sanction is necessary.
Data Subjects	Statutory staff working at EUIPO (officials, temporary agents and contract agents) or other persons working for the Office.



Description of categories of persons whose data EUIPO processes and list of data categories

We process the following personal data of a staff member or former staff member, a witness or third party (e.g.: informant collected during an investigation). Information can relate to all or some of the following data:

Retention period

According to Article 20 of Decision ADM 08



Recipients of the data	<p>Access and disclosure of personal data is restricted to those who have a legitimate, authorised purpose for gaining access to said data, i.e.:</p> <ul style="list-style-type: none">- The staff member of the Office appointed and authorized by the AA/AACC to conduct an administrative investigation (the Inquiry Team Leader or the Chairman of Board) and his/her alternate;- The members of the Inquiry Team or the Disciplinary Board, their alternates and the additional members, where appropriate;- The Secretary of the Inquiry Team or the Board, and the administrative support provided by the authorized Human Resources Department staff member with respect to the personal information transcribed in the minutes of the Inquiry Team or Board's meetings.- The Litigation Service for advice regarding the sanction decision;- The AA/AACC, as regards the investigation reports and conclusive opinions of the Inquiry Team and the Disciplinary Board;- Human Resources Authorized Staff, only as to the decision of the AA/AACC (written warning / or reprimand / or disciplinary decision) which is stored in the personal file;- A copy of the decision is sent to the Director of Department of the person concerned;- The PMO, only as to the decision of the AA/AACC when it has a financial impact on the career of the member of the staff concerned;- Professional interpreters present at the hearing in case of need;- The disciplinary decision is transmitted to OLAF when the proceeding follows an OLAF Administrative inquiry;- The Human Resources Department as custodian of documents generated in the framework of administrative inquiries and disciplinary proceedings. These documents are to be filed in the corresponding personnel files and administrative inquiry files in accordance with the retention policy applied. <p>The Human Resources Department sets up and keeps a register of administrative investigations, which shall be declared to the EDPS.</p> <p>The persons in charge of processing data in the context of administrative inquiries and disciplinary procedures are requested to sign a declaration of confidentiality.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director or IT-technician. The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security policy of the EUIPO is based on the ISO27001 standard, which is considered the most comprehensive and accredited in its category.</p> <p>A declaration of confidentiality is signed by the persons having access to the HR database.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the framework of administrative investigations and disciplinary proceedings:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/b0d0ebf1-526b-4e15-9df0-a17247b4d18b</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-065
Name of the processing operation	Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO
Last Updated:	21/02/2020
Controller Organizational entity	Human Resources
Controller contact details	<p>1) For ongoing administrative inquiries: The respective lead inquirer as determined by the Appointing Authority/ Authority Authorised to Conclude Contracts, acting as delegated EUIPO data controller.</p> <p>2) For disciplinary procedures and closed administrative inquiries: the Director of the Human Resources Department, acting as the delegated EUIPO data controller. hrddpc@euiipo.europa.eu</p> <p>Director of the Human Resources Department hrddpc@euiipo.europa.eu</p>
Name and contact details of processor	HRD (Central team)
Name and contact details of DPO	<p>Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante</p>
Description	<p>Processing of personal data within the framework of Administrative Investigations and Disciplinary proceedings at EUIPO.</p> <p>The processing of data consists in collecting information and gathering evidence, accurate and validly obtained, into a file which will be submitted to the Appointing Authority (AA) or the Authority Authorized to conclude Contracts of Employment (AACC).</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of the processing of data is to collect information to enable the AA / AACC to determine whether there has been a failure by an official, servant or other person working for the Office, to comply with his/her obligations under the Staff Regulations (SR) and the Conditions of Employment of Other Servants (CEOS).</p> <p>The AA/ AACC will then evaluate whether a disciplinary sanction is necessary.</p>
Data Subjects	Statutory staff working at EUIPO (officials, temporary agents and contract agents) or other persons working for the Office.



Description of categories of persons whose data EUIPO processes and list of data categories	We process the following personal data of a staff member or former staff member, a witness or third party (e.g.: informant collected during an investigation). Information can relate to all or some of the following data:
Retention period	According to Article 20 of Decision ADM 08



Recipients of the data	<p>Access and disclosure of personal data is restricted to those who have a legitimate, authorised purpose for gaining access to said data, i.e.:</p> <ul style="list-style-type: none">- The staff member of the Office appointed and authorized by the AA/AACC to conduct an administrative investigation (the Inquiry Team Leader or the Chairman of Board) and his/her alternate;- The members of the Inquiry Team or the Disciplinary Board, their alternates and the additional members, where appropriate;- The Secretary of the Inquiry Team or the Board, and the administrative support provided by the authorized Human Resources Department staff member with respect to the personal information transcribed in the minutes of the Inquiry Team or Board's meetings.- The Litigation Service for advice regarding the sanction decision;- The AA/AACC, as regards the investigation reports and conclusive opinions of the Inquiry Team and the Disciplinary Board;- Human Resources Authorized Staff, only as to the decision of the AA/AACC (written warning / or reprimand / or disciplinary decision) which is stored in the personal file;- A copy of the decision is sent to the Director of Department of the person concerned;- The PMO, only as to the decision of the AA/AACC when it has a financial impact on the career of the member of the staff concerned;- Professional interpreters present at the hearing in case of need;- The disciplinary decision is transmitted to OLAF when the proceeding follows an OLAF Administrative inquiry;- The Human Resources Department as custodian of documents generated in the framework of administrative inquiries and disciplinary proceedings. These documents are to be filed in the corresponding personnel files and administrative inquiry files in accordance with the retention policy applied. <p>The Human Resources Department sets up and keeps a register of administrative investigations, which shall be declared to the EDPS.</p> <p>The persons in charge of processing data in the context of administrative inquiries and disciplinary procedures are requested to sign a declaration of confidentiality.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



<p>General Description of security measures</p>	<p>Personal data is stored and processed in Sharedox (working documents) and Open Text tool (Personal File Repository kept in EUIPO servers and accessible through HR database "SAP SuccessFactors").</p> <p>The HR database has restricted access rights designed for each type of information. The accesses are given individually to each profile following the type of job in HRD, staff member, line manager, director or IT-technician. The HR database is password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security policy of the EUIPO is based on the ISO27001 standard, which is considered the most comprehensive and accredited in its category.</p> <p>A declaration of confidentiality is signed by the persons having access to the HR database.</p>
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on processing personal data within the framework of administrative investigations and disciplinary proceedings:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/b0d0ebf1-526b-4e15-9df0-a17247b4d18b</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-066
Name of the processing operation	Workstation Management
Last Updated:	30/08/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Operators and Windows administrators from IECISA ALTIA have full processing rights over user data stored in the Active Database. User objects team and Helpdesk also from IECISA ALTIA can perform limited number of processing operations with regard to the data stored. IECISA ALTIA is an external service provider for the DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Management of personal data during the usage of workstation
Purpose of the processing	Users are assigned workstations to carry out their daily work at the EUIPO. Workstations are to be used for professional purposes but there can be occasional management of personal data. That data could be stored in the home directory in their desktop/laptop (My Documents/Documents). When users finish their contractual obligations with the EUIPO, workstations are kept in storage for three months for easy access to information that is important to the EUIPO and cannot be found anywhere else. In these cases, access is granted only after receiving written consent and approval from the user and after validation by IT Security and the Data Protection Officer.
Data Subjects	All EUIPO statutory staff and any external service provider assigned with a workstation owned by EUIPO.
Description of categories of persons whose data EUIPO processes and list of data categories	All EUIPO statutory staff and any external service provider assigned with a workstation owned by EUIPO. In principle, workstations are to be used for professional purposes. However, in the course of carrying out professional duties it is possible that the user stores some data which can qualify as personal. This might include, but is not limited to, documents containing the subject's first name(s) and surname(s), address, phone and mobile phone numbers, copies of ID documents, including photos. Users can store personal information and/or documents in the home directory in their desktop/laptop (My Documents/Documents). These folders are stored in DFS server.
Retention period	While being assigned a workstation, the data will be retained for as long as the user wishes to keep it. Upon finishing a contractual obligation with the EUIPO, the workstation and any personal data stored in it will be retained for 2 months. After expiry of this period, all the information stored in the workstation is deleted.
Recipients of the data	Under normal conditions, nobody other than the data subject has access to the data stored on their workstation. This includes any personal data that could be stored within. However, in exceptional cases when the professional information stored in the workstation is not stored in any other data repository (such as Sharedox) and is required by the Office, administrators can obtain access to the information stored in those workstations. Every attempt to obtain access to data by someone other than the data subject is done under the validation of IT Security and the Data Protection Officer, and shall be only upon a written consent and authorization by the data subject even in the cases where the data subject has already left the EUIPO.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	All personal data stored in workstations is protected by a username and a password that is secret and known only by the user. Workstations are also configured for preventing unauthorized access of any other kind. Administrators shall sign a confidentiality declaration that is kept in the EUIPO's systems. In the event that an administrator is granted access to a user's workstation (after obtaining the authorisation and consent of the user), administrators are required to follow the rules outlined in this confidentiality agreement and any non-compliance will result in a disciplinary process.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/0e0e9d6e-6022-442b-bba0-517e24377997/170331_Privacy%20Statement%20on%20Management%20of%20EUIPO%20Workstations%20.pdf?a=true
EDPS Prior consultation	NO



Reference number	DPR-2019-067
Name of the processing operation	User account details from DTD systems stored in the Active Directory Database (WID)
Last Updated:	22/07/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Operators and Windows administrators from IECISA ALTIA have full processing rights over user data stored in the Active Database. User objects team and Helpdesk also from IECISA ALTIA can perform limited number of processing operations with regard to the data stored. IECISA ALTIA is an external service provider for the DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	This process concerns input and storage of user information in a common repository or set of repositories. The Active Directory serves as a master notification for all directories with specific processing characteristics. It provides user authentication, access control and authorisation facilities for registered information systems and infrastructure services. The information contained in the Active Directory is automatically imported from user accounts in the HR directory Allegro. However, user information stored in Allegro contains more types of personal data as it is a database used for HR management, and not all of that information is transferred to the DTD Active Directory. Therefore, information stored in Allegro is not within the scope of this notification but is subject to the provisions of DPR-2018-016.
Purpose of the processing	<ul style="list-style-type: none">• Manage user populations and rights in the context of IT systems for ensuring appropriate level of security is applied in a consistent fashion across IT services with the ability to identify the user of the service and / or determine his or her authorisations and roles within the context of their service.• Additionally, the processing enables client applications to provide the following services: - "white pages" services, allowing users contact details to be found (e.g. profile on Insite, e-mail address book or telephone directory); - selection of users from lists, usually based on some selection criteria - construction of lists of users, primarily e-mail distribution lists; - customisation of user interfaces according to users' individual characteristics.
Data Subjects	All EUIPO staff, as well as any service provider or partner that has been provided with an EUIPO user account (Windows).
Description of categories of persons whose data EUIPO processes and list of data categories	Not all of the pre-set categories in the Active Directory are filled in with actual data. The data actually stored includes: name, surname, email address, display name, logon name, account status, company, description, department, phone number, last log on date. The rest of the categories are not filled in with information: full address, city, state, post code, country/region, office, manager.
Retention period	<ul style="list-style-type: none">• The data is stored for as long as the subject has an active user account and has professional obligations towards the EUIPO.• Once a user ceases to have a contractual obligation with the Office and the contract is terminated, the subject's data is stored for 2 months.• Backups of the information are stored for 1 year, for the purposes of restoration in case of a technical incident.• In case of a legal claim or an administrative investigation, be it a disciplinary or criminal offense, information could be stored longer than the time limits indicated above. These measures are treated on a case by case basis.
Recipients of the data	Operators and Windows administrators from IECISA ALTIA, an external service provider for the DTD, have full processing rights over user data stored in the Active Directory. Additionally, user objects team and Helpdesk also from IECISA ALTIA can perform limited number of processing operations with regard to personal data. Occasionally, in circumstances compromising the security of the IT systems, the IT Security team, which consists of internal staff from the DTD, might also access the data for verifying user account status, last log-in date for investigation of IT security incidents. However, the IT security team cannot modify or delete data. Lastly, the data is backed up on tapes and sent to a storage providing company.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	Operators, Windows administrators, user objects team and Helpdesk's accounts which have been granted with data access and processing rights are protected with passwords. The IT security team's rights with regard to personal data are limited to access only, meaning that they cannot modify, erase, block, etc. The data backed up on tapes is encrypted and stored securely.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://insite.prod.oami.eu/digital-transformation-department/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-068
Name of the processing operation	Management of log files on EUIPO telecommunications systems
Last Updated:	19/07/2019
Controller Organizational entity	Digital Transformation
Controller contact details	For internal users: UserFeedback@euipo.europa.eu For external users: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IT security team and network/system administrators' team from IECISA ALTIA. IT security team consists of internal staff members. IECISA ALTIA is an external service provider for the DTD.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	This process relates to the operational systems of EUIPO. It covers the IT and telecommunications systems, more precisely processing data related to operation and administration of servers, storage and telecommunications. Servers automatically record information that the browser sends whenever a user visits a website, normally, called log files. Log files are created to record elements that trace any operation or event on a system.
Purpose of the processing	Personal data is included in the logs for the purposes of being able to identify the persons that carried out the activities that have been logged, in order to address any possible error or security incident that is detected. This is important because: • Log files are used to trace events in an information system and to help debugging and repair. They are part of the systems and are essential tools to provide the security and an efficient support when information systems are not working correctly. • Log files of EUIPO systems are processed for investigation and elimination of security incidents and malware infections on devices connected to the EUIPO network, and/or for prevention of data leaks. • Additionally, log files might be processed for statistical purposes or eliminating problems with users' access to EUIPO telecommunications systems.
Data Subjects	Everybody who is using the information systems of EUIPO and is connected to its network, including all statutory staff, contract service providers, and external users/clients might have their user ID recorded in the corresponding log file.
Description of categories of persons whose data EUIPO processes and list of data categories	Everybody who is using the information systems of EUIPO and is connected to its network, including all statutory staff, contract service providers, and external users/clients might have their user ID recorded in the corresponding log file. System information related to tracing users' activities on production systems, including user name, originating machine, IP address, destination URL, web browsing history, time stamp giving the beginning and the end of the operation/visit of a website, browser type, browser language, browser screen size. Examples of log files: - Websites visited by users; - Logging to management stations of network components; - Connections to databases; - Connections to Unix/Windows computers.
Retention period	Log files are stored automatically and are kept for an agreed period of time depending on the type of information and the system to which it refers. Data can be stored for 1-2 weeks, 1-2 months but in any case for up to maximum 6 months. Log files are not archived.
Recipients of the data	Log files are stored automatically and nobody other than the IT security team (internal staff members), system/network administrators (external service providers from IECISA ALTIA which is provider for the DTD) have access to all of them. Log files might be processed / inspected manually when needed (incidents, errors, malware infections, etc.). The permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies has been granted with access to perimeter security devices logs and workstation security logs, including: - Proxy logs; - Antispam/mail gateway log; - Domain controller security logs; - Antivirus logs; - Workstation security logs; - Firewall logs.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	The permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies has been granted with access to perimeter security devices logs and workstation security logs, including: - Proxy logs; - Antispam/mail gateway log; - Domain controller security logs; - Antivirus logs; - Workstation security logs; - Firewall logs. The transfer of information to CERT-EU has been justified by reasons of IT security. CERT-EU does not process log files on a regular basis but only if its involvement is needed for the investigation and resolution of security incidents. Even in those circumstances, the personal data to which CERT-EU might obtain access is limited only to user name, IP address, time stamp giving the beginning and the end of the operation/visit of a website on a device where the incident has been detected. Furthermore, the information shared with CERT-EU is protected with a non-disclosure agreement (NDA). • In addition, in case of ongoing legal investigations or disciplinary processes, information might be made available to other parties but only upon approval by the DPO (e.g. Human Resources).
General Description of security measures	<ul style="list-style-type: none">• Standard security measures of the EUIPO Information Systems: - Information will be stored in security hardened servers with access control measures and protected by Username and Password. No anonymous access allowed. - Access to the log management tools is restricted by username and password. - Authentication and authorization based on roles. - Servers are physically protected at the Data Processing Centre. - Network security configured to prevent external threats from accessing the servers. • Other security measures specifically applied to management of log files: - Log files are stored automatically but they are manually processed only when needed (incidents, errors, malware, etc.) and upon valid justification. - Log files are kept on online repositories (syslogs, Cert-EU, Splunk) separated from the systems where they are produced for avoiding leaks in case of malware or security incidents. - The people that manage log files are obliged to sign a confidentiality agreement prior to commencing their duties with the EUIPO. - The information shared with CERT-EU is protected by a non-disclosure agreement.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://insite.prod.oami.eu/digital-transformation-department/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2019-069
Name of the processing operation	Management of personal data by Cisco Advanced Malware Protection
Last Updated:	19/07/2019
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Cisco Advanced Malware Protection software and Cisco's cloud services; IT Security Team consisting of internal staff members of the DTD; Cisco (private company)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Cisco Advanced Malware Protection operates in the following way: Agents are installed on each Endpoint for the purposes of providing protection in devices, stations and Windows servers. Those agents collect information from what applications on users' computers are doing, and use Cisco's AMP Cloud to provide continuous protection and analysis as well as file analysis. When a suspicious file is detected, the AMP Cloud is used for the analysis and decision making, reducing the performance impact on the endpoints. The AMP Cloud retains information about file metadata so that it can be used during future analysis. Actions taken depend on the nature of the threat detected, for example, a file could be deleted and moved to quarantine.
Purpose of the processing	The data is collected in order to establish a pattern of the normal processes' behaviour and operations, and to create a list/repository of acceptable/legitimate operations for further analysis and comparison.
Data Subjects	All Office staff members, service providers employees, contract agents and trainees that have been assigned an EUIPO workstation.
Description of categories of persons whose data EUIPO processes and list of data categories	The following data is collected from the machines: • User GUID, a random number established by Cisco in order to know the user where the data is coming from. • Business GUID, a random number established by Cisco in order to know the company where the data is coming from. • IP Address • MAC Address • Information of the application that executed the file • Information on the type of action executed (file open, move, copy or execute) • Information of the network where the machine is located. (IP address, MAC address, host, query string, port) • If applicable and available, information of the network where the machine that has transmitted the suspicious file is located. • Cryptographic hash (for unique identification of the file) • Machine Learning Fingerprint, used by the system to identify the characteristics of the file. • Information of the third party security products installed in the computer • Endpoint Indications of Compromise (IOCs), system information regarding how the endpoint has been compromised. Also could include username in the file path description (personal profile)
Retention period	Customer endpoint monitored activity is retained for thirty (30) days so the customer can view specific events in the AMP Console. Cisco retains events and audit logs for the duration of the contract for Customer reporting purposes. The Office will request the deletion from Cisco's datastores and backups at the termination of the contract. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-amp-endpoints-privacy-data-sheet.pdf
Recipients of the data	In principle, nobody except the software itself has access to the data. The data sent to the cloud is encrypted. Three Members of the IT Security team consisting of internal staff members of DTD will be able to access the information stored in the cloud upon authentication.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES



Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>Cisco AMP Cloud on Amazon Web Services (AWS) located in Ireland. Data could also be sent to CISCO Service Providers (Sub-processors) for threat intelligence research, and this may require sending data outside Europe, under Standard Contractual Clauses and/or to USA under Privacy Shield framework. More information about AMP Endpoints in the Privacy Data Sheet:</p> <p>https://trustportal.cisco.com/c/dam/r/ctp/docs/privacypdatasheet/security/cisco-amp-endpoints-privacy-data-sheet.pdf</p> <p>More information about Cisco and Sub-processors Standard Contractual Clauses:</p> <p>https://www.cisco.com/c/en/us/about/legal/supplier-portal.html</p>
General Description of security measures	<p>Information sent to the cloud is encrypted by using SSL protocol. • Each customer has their own dedicated virtual data store that is separated from other customers. AMP Cloud server is protected by the following measures: • Cisco follows a regular patch cycle, including expedited patch installation for critical updates. • Access to the AMP Cloud servers requires SSHv2 with multi-factor authentication and installed certificates. • Information stored for one customer is not accessible to other customers via the implementation of network access control lists. • Servers are hardened, and only the services required for the functioning of the system are active. Cisco Cloud AMP implements the security measures provided by the Amazon Web Services. More information can be found at</p> <p>https://aws.amazon.com/compliance/</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement:</p> <p>http://shredox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/d9bfd501-eae9-4714-8ab6-49e4a871f884/Privacy%20Statement%20on%20Cisco%20AMP.pdf?a=true</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-070
Name of the processing operation	Procedure for EUIPO Library Management System (EUIPO Knowledge Hub)
Last Updated:	23/10/2019
Controller Organizational entity	Academy
Controller contact details	Academy@euipo.europa.eu
Name and contact details of processor	Ex-Libris: ExLibris : C/Tuset 19, 2nd floor, 08006 Barcelona / Tel: 34 93 265 34 24/ info-espana@exlibrisgroup.com GRUPO EULEN: GOBELAS 25-27 - URBANIZACIÓN LA FLORIDA, 28023 MADRID / TEL.: 916 310 800 / dcomercial@eulen.com IECISA-ALTIA: 4 Travesía de Costa Brava, (Mirasierra), 28034 Madrid / +34 91 387 47 00
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>The Academy is responsible EUIPO Library Management System (EUIPO LMS) commonly known as the EUIPO Knowledge Hub through which the loaning of books in the EUIPO is carried out.</p> <p>The EUIPO LMS is based on ALMA and PRIMO, a unified library services platform provided by the company ExLibris that allows EUIPO to:</p> <ul style="list-style-type: none">• manually add or delete users;• users can search for books and e-books, videos, articles, digital media, and more;• access open-source (publicly available) and internally indexed material via the EUIPO Knowledge Hub to have books on loan for 15 working days or on a long term basis.• Manage a private user area "Library Card" with details loan activity, requests, overdue books and blocks, and personal details. <p>The data processing is semi-automated.</p> <p>When a member of the EUIPO staff borrows a book from the EUIPO Knowledge Hub for the first time only their relative personal data is stored in ALMA:</p> <ul style="list-style-type: none">• Full name;• EUIPO e-mail address;• office number;• telephone. <p>Users may though erase all data except their names and e-mails.</p> <p>Automatic e-mails are generated to office accounts for loans, returns, overdue, holding requests and library activity.</p> <p>Visitors may use Knowledge Hub (Library) material when on the EUIPO premises.</p> <p>An e-mail sent by visitors indicating the following information must be addressed in advance to EUIPO.Library@euipo.europa.eu, in order to allow visitor's access to the EUIPO premises:</p> <ul style="list-style-type: none">• Knowledge Hub material to be consulted;• Reason for the consultation;• Full name;• ID card or passport number; <p>Telephone number.</p> <p>Once at the EUIPO premises, a completely anonymous guest access to the Knowledge Hub is granted to visitors by GRUPO EULEN.</p> <p>The content manager of ALMA deletes the personal information of the user on termination of the contract with the EUIPO.</p>
Purpose of the processing	<p>Personal data is required for the correct functioning of the EUIPO Knowledge Hub (LMS). Data are processed in order to allow user to consult and/or to register in the Knowledge hub, and in order to be able to keep track of the book loans and materials.</p>
Data Subjects	<p>EUIPO staff members and external visitors that request access to the EUIPO Knowledge Hub.</p>



Description of categories of persons whose data EUIPO processes and list of data categories	<p>We process the data below indicated, on every person who borrows a book from the EUIPO Knowledge Hub, EUIPO staff only.</p> <ul style="list-style-type: none">• Full name;• EUIPO e-mail address;• office number;• telephone. <p>Visitors' personal data processed are:</p> <ul style="list-style-type: none">• Knowledge Hub material to be consulted;• Reason for the consultation;• Full name;• ID card or passport number;• Telephone number.
Retention period	<p>The content manager of ALMA deletes the personal information of the user on termination of the contract with the EUIPO</p> <p>Changes made in personal data take effect and are completely anonymized/eliminated in the system on a daily basis after 24 hours.</p> <p>E-mails sent by visitors are kept only for the time necessary to process their access to the EUIPO premises via my service desk. Once access is granted, visitors' e-mails are immediately deleted.</p>
Recipients of the data	<ol style="list-style-type: none">1. Recipients within the controller: the data are accessed by the staff of the Learning Resources and Tools Service of the EUIPO Academy in order to manually create the EUIPO staff accounts in ALMA and request access to EUIPO premises by visitors via My service desk.2. Processor: Ex-Libris for maintenance of the ALMA IT system (cloud storage).3. Processor: GRUPO EULEN for registration of new EUIPO staff users requested on-site.4.Processor: IECISA-ALTIA for managing the access request for external visitors made by EUIPO Academy.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>The EUIPO Knowledge Hub is connected via ALMA to certain online platforms placed in third countries. Whenever a user wishes to download content from such platforms the user needs to create an account, for which a disclaimer informs the user that their personal data may be processed. They are equally informed to read the privacy statement available on that platform.</p> <p>The specific data transfers with third-country platforms and related safeguards have been described in the following fiches:</p> <ul style="list-style-type: none">- Transfer of personal data to US providers of the EUIPO Library;- Transfer of personal data to UK providers of the EUIPO Library.



<p>General Description of security measures</p>	<p>All personal data related to EUIPO Library Management System is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p> <ul style="list-style-type: none">• Only certain members of the Learning Resources and Tools Service of the EUIPO Academy have the permissions to make changes (create/delete/modify) to personal data. These access rights in the ALMA System are controlled by the Team Leader of the Knowledge Management Team of the Learning Resources and Tools Service in the Academy.• The EUIPO Knowledge Hub depends on registration in ALMA of the data subject upon which the EUIPO internal staff directory (EUIPO Active Directory) single sign on identifies the patron's work e-mail address and permits the single sign-on. Only internal users EUIPO staff can access catalogue and material, whereas external users may only consult the catalogue.• The EUIPO network security is configured to prevent external threats from accessing this information.• All personal data is held in the Ex-Libris cloud on a server owned by the company and is only accessible by the EUIPO (Alma Privacy Impact by Ex-Libris and Ex-libris information security policy).• The Ex-Libris has a backup plan that includes snapshots, incremental and full backups. There are executed "on a regular basis" though based on the documentation.• The EUIPO security system implements authentication and authorization mechanisms to prevent unauthorized access.• Ex-Libris guarantees 99.5% availability, well above the requirements of the e-Library Knowledge Hub. The measures indicated in the documentation include:<ul style="list-style-type: none">- All servers support active-active fault tolerance;- Database components have automatic fail-over;- The data center is planned at any given time to provide over 15% of the required capacity. They maintain stand-by servers ready in case of multiple-server failure;- The Ex-Libris data center maintains a clear mitigation plan for any malfunction scenario (hot standby cold standby, etc.); and- The Ex-Libris data center provides 24x7 support for all hardware components with our vendors, with an SLA for replacement hardware on site when needed.• Ex-Libris carries out monitoring primarily in the following two areas:<ul style="list-style-type: none">- 24x7 monitoring for real-time issues such as identification and resolution; and- Proactive trend analysis and health check validation.• Ex-Libris uses a standard mechanism for handling encryption keys: all encryption keys are random, and are stored separately from the credential management zone. Encryption keys are never exposed in a clear form, and they are destroyed at the end of their designated period.• Data is encrypted both in transit and in storage. This includes the encryption of data during the communications between the application server and the database server.
<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:</p>	<p>Privacy Statement on the procedure for EUIPO Library Management System (Knowledge Hub). : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3447b072-4ccb-409a-9312-44bc81fdf227</p>
<p>EDPS Prior consultation</p>	<p>NO</p>



Reference number	DPR-2019-071
Name of the processing operation	Publications manage by Communication Service
Last Updated:	23/08/2019
Controller Organizational entity	Communication
Controller contact details	Controller: EUIPO, Avenida de Europa 4, 03008 Alicante, Spain. Contact: Head of Communication Service PersonalDataCS@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	In order to carry out a publication of books, magazines or similar publications the communication service will proceed to collect the data necessary to create it. Publications may be in all formats, both written and digital, and related to the different events and projects of the Office. Communication Service also inform to the participants in the publications that the photos taken will be used for the communication external channels of EUIPO (like Facebook, LinkedIn, Twitter, etc.)
Purpose of the processing	The purpose is to be able to publish books, magazines and written publications in general in order to disclosure stories, important office events and knowledge about intellectual property.
Data Subjects	All those who participate in the publications, whether internal EUIPO staff or external.
Description of categories of persons whose data EUIPO processes and list of data categories	Name, last name, company name, country, email address, photos, personal declarations and anecdotes (written & digital format)
Retention period	.For the data, photographing of publications carried out by the Communication Service, the time limit for storage differs according to the following classification criteria: • Historic: 25 years renewable for events that mark a particular milestone in the development and history of the Office; events with management; finished productions.
Recipients of the data	Reprography service EUIPO.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	All personal data related to Publications is stored in secure IT applications according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	PUBLICATIONS PRIVACY STATEMENT: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/c9cbe94a-142b-4402-9393-1a69edfc4ec9
EDPS Prior consultation	NO



Reference number	DPR-2019-072
Name of the processing operation	Confidential Surveys conducted through Limesurvey
Last Updated:	09/09/2019
Controller Organizational entity	EUIPO
Controller contact details	Avenida de Europa, 4, 03008 Alicante, Spain DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA-ALTIA– DTD Operations service provider Other service providers from the Department conducting the survey may be involved for the correlation of survey results.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO annually performs a number of internal surveys organised by different departments and services with the main purpose of gathering information concerning their particular activities and processes. These surveys are carried out as part of operational activities of the Office.</p> <p>These surveys are conducted using the Limesurvey tool. In general terms, these surveys are managed anonymously, though under certain circumstances, it is necessary for the Departments to know the identity of the person responding, as follow-ups may be necessary. Examples of these cases are:</p> <ul style="list-style-type: none">• Surveys sent to an event organiser related to the satisfaction of the organization of the event.• Internal Departmental surveys related to the annual planning of activities.• Post-event surveys sent to users related to their satisfaction with an event.• Surveys sent to users related to the satisfaction with the services provided in relation to user queries and complaints. <p>These surveys are managed confidentially, as they require keeping personal data to identify the respondent.</p>
Purpose of the processing	Personal data is collected for the following purposes: - To ensure that it is possible to identify the individual responding to a survey. - To contact the respondent for follow-up.
Data Subjects	EUIPO Staff, and service providers of EUIPO, and Survey respondents
Description of categories of persons whose data EUIPO processes and list of data categories	Depending on the nature and specificities of the survey, the following information may be collected when answering a survey that keeps information confidential: <ul style="list-style-type: none">• name and surname;• organizational assignment (department, area and/or service)• user id• email tracking id• email• ip address• timestamp of the answers• answers to the survey• telephone number <p>Additional personal data, such as the location, may be collected, depending on the nature of the Survey.</p>
Retention period	Information is kept for the minimum time required to carry out the survey analysis. In general terms, information is kept for one year after the survey closes, for possible follow-up and/or complaints. For surveys which are of permanent nature (i.e. no closing dates), information is kept for two years after the date of the response to the survey for possible follow-up, suggestions and/or complaints. In some instances, surveys are linked to activities associated with EUIPO Management systems, such as Health & Safety. In these cases, surveys may be kept for up to three years, in line with the standard audit cycle.



Recipients of the data	Personal data related to a survey is not shared with any recipients. It is possible that aggregated results are distributed to other recipients, though in this case, no personal data is included.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	Information that is stored in Limesurvey and in Sharedox is protected by the security measures implemented for EUIPO systems: <ul style="list-style-type: none">• Limesurvey and Sharedox require username and password to access.• Authentication and authorization based on roles.• Systems are installed in security hardened servers with access control measures and protected by username and password. No anonymous access allowed.• Server is physically protected at the Data Processing centre.• Network security configured to prevent external threats from accessing the servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement Limesurvey: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/LimeSurvey_en.pdf
EDPS Prior consultation	NO



Reference number	DPR-2019-073
Name of the processing operation	Privacy statement on processing personal data in registers of activity
Last Updated:	19/11/2019
Controller Organizational entity	Finance
Controller contact details	Director of the Finance Department FD.DataProtection@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>As part of operational activities of the Office, Departments sometimes keep registers of activity. These registers normally include the information of a task and the persons involved in the task (responsible and affected users), therefore requiring to store the personal data of those involved in the activities of the register.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	<p>The purpose of processing personal data is:</p> <ul style="list-style-type: none">- Exception logs- Register of notes and reports- List of External Resources Management System (ERMS)- List of participants in meetings- List of staff holidays corresponding to the current year not taken before year-end.
Data Subjects	As part of operational activities of the Office, Departments sometimes keep registers of activity. These registers normally include the information of a task and the persons involved in the task (responsible and affected users), therefore requiring to store the personal data of those involved in the activities of the register.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following information is normally collected in a register of activity, for the purposes of following-up with those involved in the activities collected:</p> <ul style="list-style-type: none">• Name and surname;• Organisational assignment (department, area and/or service);• Link to the activity (responsible, affected user, or similar).• Additional personal data, such as the email or location, may be collected, depending on the nature of the register of activity.
Retention period	Information is kept for the period that the activity in the register is being completed. Once the activity is completed, information is subject to an administrative retention period of up to 7 years, in line with the Office's retention policy and schedule for financial files.
Recipients of the data	<p>Personal data associated with a registers of activity will be accessible to:</p> <ul style="list-style-type: none">• Department staff in charge of coordinating the activities collected in the Register.• Department Management, for validation of results.• DTD Operations service provider, for the administration of Sharedox, and/or Remedy tool. <p>Other service providers from the Department may be involved in the management of the registers.</p> <ul style="list-style-type: none">• Other service providers may be involved in the management of the registers.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>Personal data is stored in secure IT applications according to the Office's security standards, as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients.</p> <p>These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data in registers of activity:</p> <p>http://sharedox.prod.oami.eu/share/proxy/alfresco/slideshow/node/content/workspace/SpacesStore/affcb603-b801-430d-b1df-cafef3da49e1/Privacy%20Statement%20on%20processing%20personal%20data%20in%20registers%20of%20activity.docx</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-074
Name of the processing operation	Internal Audits in BoA
Last Updated:	30/09/2019
Controller Organizational entity	Boards of Appeal
Controller contact details	Boards of Appeal (BoA) of the European Union Intellectual Property Office (EUIPO), Avenida de Europa 4, ES-02008 Alicante, Spain BOA-ICC-QPROs@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Auditing of BoA systems, processes and procedures and issuing of the corresponding audit reports addressed to the President and the Presidium of BoA. The personal data is collected via the EUIPO directory and the organisation chart just before an audit starts. The information is used for any further communication between the BoA Internal Audit Team and the audited area. It is also used to provide corresponding permissions in the document management tool (ShareDox).
Purpose of the processing	The internal audits are done in order to provide reasonable assurance and make recommendations regarding the quality of the BoAs management and control systems. The data will be used solely in the framework of the internal audits; the data will not be used for any other purposes. It will, in particular, not be used for the evaluation of individual performances. The internal audits only serve the evaluation of processes, not of staff's individual performance. The internal audits only serve the evaluation of processes, not of staff's individual performance. The purpose of the processing operation is to keep record of the audit process, meetings and information provided during the audit.
Data Subjects	BoA staff working in the audited area
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data of the staff working in the audited area. The following personal data is processed: name and surname, e-mail, department/service, work-address, title, position, functions.
Retention period	The documents are kept in line with the following retention period: 7 years since the publication of audit plan, in line with EUIPO Financial Regulation No CB-1-15 (Art. 42(5) and Art. 107).
Recipients of the data	The personal data in the documents used to draft the audit reports is disclosed only to the following recipients on a strict need-to-know basis: <ul style="list-style-type: none">• BoA Internal auditors Team;• BoA Survey requestors.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related are stored in secure IT applications (ShareDox/LimeSurvey) according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients. These security measures include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network.• Logical security hardening of systems, equipment and network.• Physical protection via secure Data Centre. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC2)</p> <p>Surveys in LimeSurvey are anonymous and confidential, with no personal data required.</p> <p>All audit staff have received appropriate instructions on the processing of personal data in the course of internal audits and on the ethical use of the information made available to them. To minimise the risk of data being transferred in breach of our obligations under the regulation, Auditors are asked to avoid, in so far as possible, the inclusion of personal data in observation forms by rendering it anonymous.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing personal data within the context of internal audits in BoA:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/8a0cef67-db0c-4200-bcf8-172cf95a0df2</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-076
Name of the processing operation	Processing personal data within the framework of the organisation of internal competitions at the EUIPO and the constitution of related reserve lists
Last Updated:	21/01/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Head of the Staffing, Development and Recognition Service (EUIPO - HRD) and EPSO
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The EUIPO, in cooperation with EPSO, which assists the European institutions and other EU bodies and agencies with the selection of statutory staff, processes personal data to select candidates in order to establish reserve lists of suitable laureates with a view to their appointment.</p> <p>Data processing starts from the moment a candidate submits an application or, regarding successful laureates on a reserve list, when they confirm their interest in the appointment process. Data processing operations relating to the appointment process are covered under the 'Recruitment' information contained in EUIPO's general data privacy statement .</p> <p>Candidates provide the Office with personal data on their identity, qualifications and professional experience due to the very nature of the selection process.</p> <p>Data is processed in the following phases:</p> <p>Application phase:</p> <p>During the application phase, candidates will be requested to fill out and validate an online application form and provide information / submit documents in order to prove compliance with the requirements established in the Notice of Competitions (NoC).</p> <p>Selection phase:</p> <p>Candidates' data will be processed to evaluate their eligibility, expertise and relevance of their profile for the competition. This evaluation is based on elements provided by the candidates in their application form, as well as information introduced by candidates in their EPSO account , relevant data already in the possession of the Office in EUIPO HR databases (Allegro/myPortal, including a section of myPortal named my Personal File under "Recruitment documents" and "Assignments" folders) and documents submitted by the candidate in support of their application.</p>
Purpose of the processing	<p>Processing personal data is necessary to organise internal competitions to constitute reserve lists from which EUIPO will appoint civil servants.</p> <p>The personal data is collected and processed in accordance with the Staff Regulations of Officials of the European Union (SR) and the Conditions of Employment for Other Servants of the European Union (CEOS), as well as the relevant Notice of Competitions.</p>



Data Subjects	EUIPO statutory staff members (temporary agents and contract agents).
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data processed by EUIPO as controller:</p> <ul style="list-style-type: none">• All personal data which are part of the application, including data allowing identification of the candidate (e.g. family name, first name, name at birth, date of birth, gender, nationality, number and validity date of identification document, address, e-mail address, phone number, EUIPO employee number).• Information provided by the candidate to allow practical organisation of admission tests and other tests (e.g. address, postcode, city, country, telephone numbers, languages for correspondence, language for tests, photograph).• Information provided to the Selection Board to allow for the verification of the candidate's admissibility against the eligibility conditions fixed by the Notice of Competitions (e.g. citizenships, language and other relevant skills, diploma/training with year of award, title, name of the awarding body, professional experience including administrative status and career, function group/grade, profile/position, organisational assignments and related periods, extract of objectives from appraisals (any type of assessment excluded)).• Results of the eligibility verification, MCQ and assessment centre tests, including the competency passport and other data concerning the candidates' skills and competencies.• Information provided in cases of requests, complaints, appeals. <p>All relevant personal data and information are contained in the EPSO online account, application form, CV if relevant, and supporting documents submitted by the candidates as well as in the relevant EPSO tools and EUIPO HR databases (e.g. Allegro/myPortal, including a section of myPortal named my Personal File under "Recruitment documents" and "Assignments" folders).</p> <p>Adding a photo to the application is entirely voluntary.</p> <p>Data processed by EPSO as processor:</p> <ul style="list-style-type: none">• All personal data which are part of the application, including data allowing identification of the candidate (e.g. family name, first name, date of birth, gender, nationality, number and validity date of identification document, address, e-mail address, phone number, EUIPO employee number).• Information provided by the candidate to allow practical organisation of admission tests and other tests (e.g. address, postcode, city, country, telephone numbers, languages for correspondence, language for tests, photograph).• Information provided by the candidate concerning special needs.• Results of the eligibility check, MCQ and assessment centre tests, including the competency passport and other data concerning the candidates' skills and competencies.• Information provided in cases of requests, complaints, appeals.



Retention period	<p>For successful candidates:</p> <p>Data is kept in the personal file of the established official, in accordance with Article 26 SR. The personal data from the appointment file is kept for 8 years after the expiry of all the rights of the person concerned and of any dependents, and for at least 120 years after the date of birth of the person concerned.</p> <p>For successful candidates whose names were placed on a reserve list but who were not appointed or who did not take up duties as officials:</p> <p>Data is kept on file for 2 years after the expiry of the reserve list.</p> <p>For unsuccessful candidates:</p> <p>Data is kept on file for 2 years after candidates have been notified that they were unsuccessful.</p> <p>In the event of a formal complaint/litigation, all data held at the time of the complaint/litigation will be retained until the completion of the process.</p> <p>For the retention policy for data processed by EPSO: as indicated in the relevant privacy statement (published on EPSO online).</p>
Recipients of the data	<p>Candidates' data is disclosed to a limited number of staff of EUIPO HRD and EPSO staff dealing with internal competitions, as well as to the Chairperson and Members of the Selection Board and/or to the persons designated by the Appointing Authority as observers/assessors from the departments and/or markers for the correction of tests.</p> <p>Relevant data is kept in the EUIPO HR databases (Allegro/myPortal, including a section of myPortal named my Personal File under "Recruitment documents" and "Assignments" folders).</p> <p>For economy of proceedings, HRD staff dealing with internal competitions may provide Selection Boards with the relevant information contained in the EUIPO HR databases (Allegro/myPortal, including a section of myPortal named my Personal File under "Recruitment documents" and "Assignments" folders) in order to verify whether candidates comply with the eligibility conditions set in the Notice of Competitions.</p> <p>Before the Selection Boards verifies the eligibility conditions, the HRD staff dealing with internal competitions will ensure that in the Personal File under "Recruitment documents" and "Assignments" folders there is no confidential information that is not necessary for the purpose of this verification (this processing operation shall be described on a Note to the file).</p> <p>The reserve lists are published on the EUIPO's Insite.</p> <p>The names of all successful laureates as well as their competency passports will be available in the EPSO Recruiter Portal accessible to a limited number of EUIPO staff members dealing with recruitment. All names and, when relevant, the candidates' data will also be disclosed to the EUIPO Appointing Authority and/or subdelegated authorities.</p> <p>Information may be shared with other EU Institutions and agencies, upon request and after having received the candidates' agreement.</p> <p>EUIPO's contractors and subcontractors might have access to data for maintenance and development of the applications supporting the HR "Allegro" database and "SAP SuccessFactors" in the cloud under request and supervision of EUIPO .</p> <p>The data is not used for any other purposes or disclosed to any other recipients.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All candidates' data related to EUIPO internal competitions will be processed and stored by EPSO with the same security standards as those applied for EPSO open competitions as detailed under the EPSO specific privacy statement .</p> <p>At EUIPO, candidates' data is processed and stored in secure IT applications according to the security standards of the Office, as well as in specific electronic and/or paper folders accessible only to the authorised recipients.</p> <p>The EUIPO HR databases "Allegro" and "myPortal", including the section of myPortal named my Personal File under "Recruitment documents" and "Assignments" folders, have restricted access rights designed for each type of information and are used only on a need to know basis. Depending on the data, the accesses are granted individually or under a generic role (e.g. 'Selection Board').</p> <p>All EUIPO HR databases are password protected under single sign-on system and automatically connected to the user ID and general password. Replacing users is strictly prohibited. The records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 270011 standard, which is considered the most comprehensive and accredited in its category. "SAP SuccessFactors" is also certified in ISO 27001.</p> <p>Personal data are not intended to be transferred to a third country. Data will be processed and stored only in EU.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on processing data for the organisation of EUIPO internal competitions and the constitution of reserve lists:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/6dfd19db-9cec-4c7f-b102-1ea7d445eb23</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-077
Name of the processing operation	Staff Satisfaction Survey 2020
Last Updated:	22/01/2020
Controller Organizational entity	Human Resources
Controller contact details	EUIPO Director of the Human Resources Department hrddpc@euipo.europa.eu
Joint Controller organizational entity	Human Resources
Name and contact details of processor	<ul style="list-style-type: none">• Willis Tower Watson (WTW) - Reigate (UK - close to London)• Willis Towers Watson Global Business Services, Inc (Manila-Philippines)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Staff Satisfaction Survey 2020, as part of the Feedback Exercise, will be sent to all statutory staff and seconded national experts and will be used as an important tool to assist the Office's management team.</p> <p>To this aim, an independent external provider, Willis Towers Watson (WTW) which is a consultancy firm providing Human Resources solutions in employee surveys, will carry out the Staff Satisfaction Survey 2020.</p> <p>Each statutory staff member and seconded national expert will receive an individual link from WTW to access the survey. The participation on the survey is entirely voluntary and fully confidential. The conditions of confidentiality are stated in the contract signed between the Office and the provider and will be strictly respected by both EUIPO and WTW.</p>
Purpose of the processing	<p>The purpose of the Staff Satisfaction Survey 2020 is to take into account staff feedback to develop action plans and to take managerial decisions in order to improve staff satisfaction at work.</p> <p>The Survey will contribute to the continual improvement cycle established at the Office.</p> <p>The processing of data is done according to Article 24a of the Staff Regulations (SR) of Officials and Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS) of the EU, as well as the Regulation (EU) 2017/1001 on the EUTM, in particular Article 157 (4) (a).</p>
Data Subjects	Statutory staff members and seconded national experts



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data collected: electronic address of statutory staff and seconded national experts and their opinion.</p> <p>In addition, for each staff member the following information will be pre-coded by the provider based on the data sent by the Office:</p> <ul style="list-style-type: none">• Department, Service;• Hierarchical level (Senior management, Middle management, Team Leader, Staff);• Teleworker regular (yes or no);• Working relationship (official, temporary agent, contract agent or SNE);• Length of service (less than 5 years, 5 to 10 years, more than 10 years);• Age (under 35 years of age, 35 to 45 years of age, 46 to 55 years of age, 56 years or older);• Gender;• Function group; Administrator (including Contract Agent function group 4) or Assistant (including Contract Agent function groups 1 to 3).
Retention period	<p>Personal data will remain in the database until the results have been completely analysed and the final report with the aggregated results has been delivered. Any Personally Identifiable Information (PII) is deleted from WTW systems no later than 6 months after the event closes.</p> <p>The aggregated data on groups (excluding individual - level data) will be kept until the next survey is carried out, for the purpose of research analysis and reporting, and specifically, to make a comparison.</p> <p>Only the aggregated final report and analysis of results (consolidated data) will be stored in EUIPO document management system (in HRD confidential folder) for five years according to the Office's security measures.</p>
Recipients of the data	<p>The survey will be delivered online and will be entirely managed by WTW guarantying that data will be treated with the highest level of confidentiality under the conditions stated in the contract signed with EUIPO. The whole process is automated.</p> <p>The processed and aggregated results of the survey (anonymous) will be accessible to all EUIPO staff in the form of a final report summarising the overall findings and results per category and department.</p> <p>An additional and more detailed report (with aggregated anonymous results of the survey) will be accessible to the following persons: Director of the HRD, the Head of Staffing, Development and Recognition Service (HRD), the EUIPO management and a limited number of staff of the HRD and other Departments working in the survey.</p> <p>A specific report (with aggregated anonymous results of the survey), grouping those questions related to psychosocial factors, will be made available to EUIPO's Health and Safety Officer.</p> <p>The information concerning the detailed results will only be shared with people necessary for the implementation of such measures on a "need to know basis". The data is not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?	<p>The conditions are stated in the clauses of the contract signed between EUIPO and WTW.</p> <p>The responses given to the staff satisfaction survey questionnaire will not allow the identification of respondents (“who said what”) as the information will be consolidated and a minimum number of 10 respondents per group has been established for the report to be generated and the results to be shown.</p>
General Description of security measures	<p>Pre-populated personal data and pseudonymised answers are stored on the WTW servers according to their security measures and processes access being provided only to the core project team and technical support on a “need to know” basis. The servers are located in a datacentre in Reigate (UK close to London) that is ISO 27001 certified.</p> <p>In case of transfer of personal data, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.</p> <p>Only the final report and analysis of results will be stored on EUIPO servers and in Sharedox (confidential HRD folder), according to the security measures of the EUIPO Information Systems.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement on the procedure of Staff Satisfaction Survey 2020:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/3b935b58-f377-4b7b-bc9b-53f3f2660807</p>
EDPS Prior consultation	NO



Reference number	DPR-2019-078
Name of the processing operation	Survey Peer and 360° Feedback
Last Updated:	22/01/2020
Controller Organizational entity	Human Resources
Controller contact details	EUIPO Director of the Human Resources Department hrddpc@euiipo.europa.eu
Name and contact details of processor	<ul style="list-style-type: none">• Willis Tower Watson (WTW) - Reigate (UK - close to London)• Willis Towers Watson Global Business Services, Inc (Manila-Philippines)• Leading Indicator Systems, LLC (USA) - (sub-processor of WTW)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO is launching in 2020 the peer / 360° feedback questionnaires, as part of a single "Feedback Exercise", including also Staff Satisfaction Survey. The entire Feedback exercise is voluntary, confidential and used for development purposes.</p> <p>Peer feedback will enable staff members and seconded national experts to perform self-perception assessment and provide and receive feedback to and from their peers through an on-line questionnaire. Peer feedback is designed to help staff reflect on how they collaborate and work with each other focusing on aspects of teamwork and engagement.</p> <p>In addition, 360° feedback will offer an opportunity for managers to receive feedback not only from their peers but also from other sources as direct reports and line managers about their leaderships skills. Both peer and 360° feedback will play an important role in staff's professional and leadership development respectively.</p> <p>An independant external provider, Willis Tower Watson (WTW) which is a consultancy firm providing Human Resources solutions in employee surveys, will carry out the peer/360° feedback exercise 2020. Each statutory staff member and seconded national experts will receive an individual link from WTW to access the peer/360° feedback exercise.</p> <p>The observable behaviours that compose the questionnaire are fully aligned with the EUIPO competency framework and the 10 Best Management Practices agreed in 2017 by the EUIPO managers.</p> <p>Data will be treated with the highest level of confidentiality under the conditions stated in the contract signed between WTW and EUIPO. The feedback received by the participant will not allow the identification of the feedback providers ("who said what") as the information will be consolidated and a minimum number of three (3) feedback providers per group of respondents has been established for the report to be generated and the results to be shown. The only exception when the content of the reply can be linked to a specific person will concern feedback received by a manager from his/her line manager.</p>



Purpose of the processing	<p>In the context of the EUIPO Strategic Plans 2020 and 2025, the purpose of the processing is to reinforce a feedback rich culture helping staff and the Office develop their strenghts, identify areas of improvement and grow. It will help EUIPO staff to raise awareness by identifying gaps between their self-perception and the perception of others and to identify development needs, helping them to develop their competencies.</p> <p>The processing of data is done according to Article 24a of the Staff Regulations (SR) of Officials and Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS) of the EU, as well as the Regulation (EU) 2017/1001 on the EUTM, in particular Article 157 (4) (a).</p>
Data Subjects	EUIPO statutory staff members and seconded national experts.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data is processed:</p> <ul style="list-style-type: none">• full name, electronic address, group (staff, team leader, manager), department/ service and line manager;• replies to the questionnaire in form of scores given to the different statements according to a defined scale;• individual feedback reports mentioning strenghts and areas for development - available only to the person concerned.
Retention period	<p>The individual contributions of the participants in the peer/ 360° feedback questionnaire collected through the tool will be kept until the exercise is completed and when the results have been completely analysed and the reports produced.</p> <p>Any Personally Identifiable Information (PII) is deleted from Willis Towers Watson's systems and Leading Indicators's system no longer than six months after the event closes.</p> <p>Feedback group reports stored in the internal document management system will be deleted after five years since the results have been delivered.</p>
Recipients of the data	<p>The questionnaires will be delivered online and entirely managed by WTW (working with Leading Indicators as a dedicated sub-contractor) guarantying that the data will be treated with the highest level of confidentiality under the conditions stated in the contract signed with EUIPO.</p> <p>The confidential individual report will be only accessible to the person concerned (participants - statutory staff members and seconded national experts).</p> <p>For 360° and peer feedback reports as it concerns managers and team leaders respectively, the individual report will also be accessible to the consultant who provides interpretation guidelines on results.</p> <p>The report with aggregated anonymous results of the survey will be available to all EUIPO staff and will include a summary of the overall results for managers, team leaders and staff, as well as the highest/lowest average feedback outcomes showing areas for improvement.</p> <p>A more detailed report showing average feedback outcomes by behaviour items per group and non-identifiable participants will be made available only on a need to know basis to:</p> <ul style="list-style-type: none">• the persons specifically designed within HRD to organize the peer/ 360° feedback questionnaire;• the Executive Director.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	All the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.
General Description of security measures	<p>The personal data and confidential answers are stored on the WTW servers according to their security measures and processes accesses being provide only to the core project team and technical support on a "need to know basis".</p> <p>The servers are located in a datacentre in Reigate (UK close to London) that is ISO 27001 certified.</p> <p>In case of transfer of personal data, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed.</p> <p>Only the final report and analysis of results will be stored on EUIPO servers and in Sharedox (confidential HRD folder), according to the security measures of the EUIPO Information Systems.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p> <p>No personal data is transmitted to parties which are outside the recipients and the legal framework mentioned, nor used for other purposes.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Data protection statement on the procedure of Peer / 360° Feedback : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3a85f417-4fae-4a35-9410-5b646682eaa5
EDPS Prior consultation	NO



Reference number	DPR-2019-080
Name of the processing operation	EPQCs concerning the Vienna Codes classification of EUTMs
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Director of the Customer Department, EUIPO CDLegalDPO&FraudCoordination@euipo.europa.eu.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>A group of examiners of the S&P team is in charge of classifying the Vienna Codes of EUTMs. The only item examined during the Ex-Post Quality Checks is the relevant classification of the Vienna Codes by the examiners. Examiners open the available marks in Vienna Coding queue and classify the graphic elements. Then, checkers open the available marks in Question queue.</p> <p>These checkers review the logo and the Vienna codes previously assigned, and either give their point of view about the correctness of the classification (1st EPQC) or give some comments and/or changes in case they consider that the initial coding introduced is incorrect (2nd EPQC).</p> <ul style="list-style-type: none">• 1st EPQC <p>Each first Monday of the month, the Team Leader receives an automatic email from TMSS-Automation with an Excel file composed of data regarding the examiners and the tasks performed regarding the EUTMs. Then the Team Leader allocates the EUTMs to be checked between checkers that did not previously examine the EUTM.</p> <p>The checkers give their point of view (yes/no) about the accuracy of the classification and can make a comment.</p> <p>Once the Team Leader receives all checkers' assessments, it removes the examiners' usernames and published the Excel file in Sharedox, leaving the data regarding the checkers.</p> <ul style="list-style-type: none">• 2nd EPQC <p>This EPQC implies the same process and procedure, but checkers must correct and suggest the relevant coding if the examiners were wrong.</p>



Purpose of the processing	<p>The purpose of the processing is to carry out an ex-post quality check of the Vienna Codes classification of EUTMs done by examiners.</p> <p>The purpose of the processing is to carry out ex-post quality checks of the Vienna Codes classification of EUTMs done by examiners.</p> <p>The aim of the 1st EPQC is to calculate the percentage of errors of each examiners by allocating some EUTMs' checks between checkers who did not previously take part in the EUTM processing.</p> <p>The checkers only check if the Vienna Codes chosen by examiners are relevant regarding the figurative EUTM by mentioning if the classification is correct, or not.</p> <p>The aim of the 2nd EPQC is to guarantee that the final outcome of the EU search is of the expected quality before it is provided to our customers. In order to do so the checker will review and if necessary correct the initial Vienna coding done by the prior search examiner.</p> <p>The common aim is to carry out statistics in order to make the future coding better.</p>
Data Subjects	<ul style="list-style-type: none">- Examiners of figurative EUTMs (who are staff members of the Search & Publication team).- Checkers: Team members of quality checks (who are staff members of the Search & Publication team who did not take part in the EUTM proceeding yet).
Description of categories of persons whose data EUIPO processes and list of data categories	<p>Data subjects:</p> <ul style="list-style-type: none">- Examiners of figurative EUTMs (who are staff members of the Search & Publication team).- Checkers: Team members of quality checks (who are staff members of the Search & Publication team who did not take part in the EUTM proceeding yet). <p>Data categories collected in two separate Excel files:</p> <ul style="list-style-type: none">• 1st EPQC<ul style="list-style-type: none">- Current date- Usernames of examiners- Operation date- EUTM number- IR yes/no- Correct yes/no- Comment- Name of the checkers• 2nd EPQC<ul style="list-style-type: none">- Current date- EUTM/IR number- Initial coding- Amended coding- Comment- Name of checkers (initials)- Name of examiners (initials) <p>Even if only initials of names of examiners and checkers are mentioned in tables, given that the information is shared with the individual team members, initials allow to identify directly each members and should be considered as personal data.</p>



Retention period	<ul style="list-style-type: none">• 1st EPQC Once the Team Leader gets the checkers' comments, it deletes the Examiners usernames' column before publishing the Excel file on Sharedox. The previous Excel files are stored in Sharedox indefinitely in accordance with article 112 EUTMR.• 2nd EPQC The data will be retained until the appraisals of the following year have been done.
Recipients of the data	<p>The recipient of the data is a Team Leader's member in the Search and Publication Team (Customer Department).</p> <p>Once the Team Leader publishes the Excel file on Sharedox, the data is only accessible for:</p> <ul style="list-style-type: none">• CD Direction• Team Leader• CD EPQC group (examiners and checkers)
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the ex-post quality check of the Vienna Codes classification of EUTMs done by examiners is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Access to client information is restricted. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>EPQCs concerning the Vienna Codes classification of EUTMs - Privacy Statement :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/0967a39c-8a17-46fe-8db6-860cc32223f9</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-001
Name of the processing operation	Management of mobile telecommunications
Last Updated:	02/04/2020
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	- Orange Espagne S.A.U - IECISA ALTIA DTD Operations external service provider
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing consists on the following activities: • Management of user requests to be assigned a mobile device. • Management of user requests to modify mobile device plans and/or configuration, when needed. • Maintenance activities required for EUIPO mobile devices. • Activities required in case of a theft of a mobile device. • Activities required when collecting a mobile device from a user. Any user can request a mobile device, and when already assigned, any user can request a change in configuration. These requests are supported by workflow mechanisms implemented in Remedy and managed through the process for Management of Incidents and Changes (DPR-2019-038), including a series of validations and/or authorizations by DTD support services or other EUIPO services depending on the nature of the request. Mobile device management is mainly carried out through the Intune Device Management tool, this system is connected to all EUIPO mobile devices and kept synchronized. Migrations are carried out manually, and require collaboration with the user assigned. During this process, personal data may be made available to the administrator doing the migration, the process is made by the cloud migration available on each mobile device (i.e. iCloud for iPhone or Smart Switch for Samsung). Theft and robbery reports are managed through workflow mechanisms implemented in Remedy and follow the process for Incident and Change Request Management. This step, however, requires the user to submit a Police report indicating the details of the person and the robbery, and it may be necessary to pass this information to service providers in order to receive a new device. This Notification is linked to the DPO Notification - DPR-2019-037 Processing personal data within the framework of EUIPO Mobile Telecommunications Services Policy.</p>
Purpose of the processing	It is necessary to collect personal data in order to know the user that was assigned the device, identify the device, and provide maintenance as needed.
Data Subjects	All EUIPO Staff that has been assigned a mobile device (statutory or not)
Description of categories of persons whose data EUIPO processes and list of data categories	<p>During normal assignment and maintenance of the device: • Name and surname • Mobile telephone number assigned • Login • Approximate location (to within 2 Kms): As currently configured, the geo-localisation won't give the exact location of a mobile, but will identify the country that the mobile is in, in order to do a security validation of the phone, and send an informational message regarding the use of roaming in case the mobile has left the country. When the user requests a change in roaming due to travel: • It is necessary to know the country that the user will be traveling to, in order to activate the required roaming plan.</p> <p>During management of theft or robbery of the device Police report of the theft, including all the information available in it: Name, surname, address, contact information, device model, IMEI number and any details included in the report, only shared with Orange Espagne S.A.U for new device replacement process.</p>
Retention period	• Information for mobile device management is stored for as long as the user is assigned the device. Once the device has been collected, Information is kept for up to 90 days. • Police reports are kept for 6 months for reporting the theft of the device. • Any information managed through My Service Desk apply the storage limits indicated in DPR-2019-038.
Recipients of the data	The service provider and any subcontractor after duly notification to EUIPO and its acceptance. • EUIPO Management (during approval process and in case that investigating mobile usage is required)



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	<p>The Tool is connected to EUIPO's authentication systems in order to verify the person that is trying to access the information. • Tool includes access control measures to grant or deny access based on the profile of the user that is connecting. • For the process of data migration: • the process is made by the cloud migration available on each mobile device (i.e. iCloud for iPhone or Smart Switch for Samsung).</p> <ul style="list-style-type: none">• The device itself is configured with data encryption and a security pin for access control, in order to ensure that any data stored in the device is properly protected against unauthorized access. This configuration is remotely enforced by the Intune MDM, preventing the user from deactivating it.
General Description of security measures	<p>The Tool is connected to EUIPO's authentication systems in order to verify the person that is trying to access the information. • Tool includes access control measures to grant or deny access based on the profile of the user that is connecting. • For the process of data migration: • the process is made by the cloud migration available on each mobile device (i.e. iCloud for iPhone or Smart Switch for Samsung).</p> <ul style="list-style-type: none">• The device itself is configured with data encryption and a security pin for access control, in order to ensure that any data stored in the device is properly protected against unauthorized access. This configuration is remotely enforced by the Intune MDM, preventing the user from deactivating it. <p>For this process, the standard security measures of the EUIPO Information Systems is applied:</p> <ul style="list-style-type: none">• EUIPO username and password required in order to access EUIPO network and systems.• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers.• Network security configured to prevent external threats from accessing the mail servers. Furthermore, the access to the data will be granulated according to the authorizations agreed upon for each individual.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/a9115d3c-01f8-443f-b2a5-633e64b2ccdd</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-003
Name of the processing operation	Privacy Statement on processing personal data for reporting serious irregularities and wrongdoings "Whistleblowing"
Last Updated:	24/02/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Joint Controller organizational entity	Human Resources
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>EUIPO's staff members or persons other than the Office's staff can report serious irregularities and wrongdoings. Seconded national experts (SNE's), trainees and interims agents can also blow the whistle. These persons can also be affected by the processing operation because they might be witnesses, accused persons or third parties mentioned in the whistleblowing report.</p> <p>The processing operation requires guiding potential whistleblowers, establishing reporting channels for whistleblowers, managing and following-up reports of wrongdoings and ensuring protection for whistleblowers, the alleged wrongdoers, the witnesses and the third parties appearing in the report.</p> <p>Whistleblowing channels should not be used when staff may wish to exercise their statutory rights, i.e. by lodging a request or complaint to the Appointing Authority under article 90 of the Staff Regulations or for harassments claims and personal disagreements when staff may address themselves to the Human Resources Department.</p> <p>Whistleblowers may proceed anonymously, but they are encouraged to mention their identity to allow their effective protection against retaliation. This will also allow a better management of the file if further information would be necessary.</p> <p>The identity of the whistleblower who reports serious wrongdoings or irregularities in good faith shall be treated with the utmost confidentiality, except in certain exceptional circumstances if the whistleblower personally authorises the disclosure of his/her identity or if this is a requirement in any subsequent criminal law proceedings.</p> <p>Bad faith report, particularly if it is based knowingly on false or misleading information may lead to disciplinary measures.</p> <p>The report of wrongdoings can be done internally to an immediate superior or to the Executive Director or, alternatively, to the MB Chairperson or to OLAF. The receiver of this information is obliged to transmit it to OLAF. As a last resort, whistleblowers may turn to other entities from other EU institutions (the President of the Council, or of the European Commission, or of the European Parliament, or of the European Court of Auditors, or the European Ombudsman.</p>
Purpose of the processing	<p>The purpose of this processing operation is to enable EUIPO's staff members or persons other than the Office's staff to report suspected illegal activity, including fraud or corruption, detrimental to the interests of the EU, or other serious professional irregularities at EUIPO.</p> <p>Article 22a, 22b and 22c of Staff Regulations (SR) as well as Articles 11 and 81 of the Conditions of Employment of Other Servants (CEOS) provide for the rules on whistleblowing.</p>



Data Subjects	EUIPO's staff members (officials, temporary agents and contract agents) or persons other than Office's staff , including SNE's, trainees and interim agents.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The personal data processed is the data contained in the report submitted by the whistleblower and any subsequent document drawn up in response to that initial report. These documents may contain:</p> <ul style="list-style-type: none">• identification of the data subject (names, other personal data);• contact details;• evaluation of personal aspects of the data subject (e.g.: conduct, activities, working relations and economic or social behaviour);• administrative data (grade, position and responsibilities, department/service);• documents produced at work (emails, notes, correspondence, etc.);• identification of whistleblowers, witnesses, third parties mentioned in the report and the person(s) against whom the allegations have been made.
Retention period	<ul style="list-style-type: none">• Cases not to be referred to OLAF or out of the scope of whistleblowing procedure: 2 months after the finalisation of the preliminary assessment or after being referred to the right channel (e.g.: alleged harassment).• Cases referred to OLAF: 3 years after receiving the final outcome of OLAF's procedure (investigation not launched, investigation closed with no further action, or final report).• In case of ensuing administrative inquiries or disciplinary procedures, data is kept for the periods defined in the related specific privacy statement. <p>At the end of the retention period, data is destroyed.</p>
Recipients of the data	<p>Access to data may be granted on a strict need to know basis to the following persons:</p> <ul style="list-style-type: none">• authorised staff members of the Human Resources Department designated to offer guidance and support to (potential) whistleblowers;• immediate superior of whistleblower, Executive Director, Chairperson of the Management Board or any other staff member to whom it is reported;• OLAF;• As option of last resort, the President of the Council, or of the European Commission, or of the European Parliament or of the European Court of Auditors or the European Ombudsman.• Director of Human Resources Department and a limited number of staff members of HRD dealing with the case;• Appointed Authority or Authority Authorised to Conclude Contracts of Employment and/or subdelegated authorities;• Any staff member of the Office responsible or involved in protective measures and any follow up actions.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Data related to whistleblowing procedures has controlled restricted access rights. Technically, both accesses and the access rights will be reviewed regularly.</p> <p>Only a limited number of authorized staff members working in these procedures have access to data on a strict need to know basis. They have an obligation of secrecy and access to the whistleblowing reports will be monitored whatever in electronic or paper form.</p> <ul style="list-style-type: none">• Electronic files: The documents are held securely so as to safeguard the confidentiality and privacy of the data therein. The access rights will be documented.• Paper files: The storage will be done only in locked cupboards kept by HRD. The access to locked cupboards will be limited.• Destruction of documents: The destruction will be done only on approved paper shredder.• Transfer of data: Requirements for transferring data must be assessed on a case- by-case basis. Personal information will be transferred only when necessary for the legitimate performance of tasks covered by the competence of the recipient.• Transmission to OLAF: If the file needs to be transmitted to OLAF, the same security measures as to internal transfers will apply. <p>All persons designated to work in whistleblowing files must ensure the utmost confidentiality of these files and respect security measures applied to these procedures.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement on processing personal data for reporting serious irregularities and wrongdoings "Whistleblowing" : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/68c4795a-5546-483f-b310-1602a2a1f467
EDPS Prior consultation	NO



Reference number	DPR-2020-005
Name of the processing operation	EUIPO eRegister
Last Updated:	17/04/2020
Controller Organizational entity	Operations
Controller contact details	Ms. Karin KUHL, Director of the Operations Department, EUIPO ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The Office shall keep a Register of EU trade marks (Article 111 EUTMR) and shall keep a register to be known as the register of Community designs (Article 72 CDR).</p> <p>It is an official record of every entry made in the Register in relation to an EUTM or RCD application or registration, where the entry is required by the EUTMR, CDR or related texts.</p> <p>All entries made in the Register, are made into a electronic register ('eRegister' in beta version for the time being). The eRegister beta version allows for one single repository of all entries in the Register of a specific IP right. It is composed of two main features: a back-office tool which allows for the technical storage and compilation of all the entries, and a front-office feature which offers a publicly accessible user interface to access and visualise the information contained therein.</p>
Purpose of the processing	<p>a) administering the applications and registrations as described in the EUTMR and CDR Regulations and acts adopted pursuant to them, see in particular Article 111(8) EUTMR, Article 69 and 71 CDIR;</p> <p>b) maintaining a public register for inspection by, and the information of, public authorities and economic operators, in order to enable them to exercise the rights conferred on them by these Regulations and be informed about the existence of prior rights belonging to third parties; and</p> <p>c) producing reports and statistics enabling the Office to optimise its operations and improve the functioning of the system</p> <p>as foreseen, for trade marks, in Article 111(8) EUTMR and for designs in Recital 7 and Article 6 of the Decision No EX-14-3 of the President of the OHIM.</p>
Data Subjects	All applicants for EUTM and RCD
Description of categories of persons whose data EUIPO processes and list of data categories	<p>EEUIPO's eRegister beta version will contain all the entries into the Register, and particulars provided for by the regulations, namely each individual item listed in the subparagraphs of Article 111(2), (3) and (4) EUTMR, Article 69(2), (3) and (4) CDIR and Article 4 (2) of the Decision No. EX-14-03 of the President of the Office, which include some personal data, in particular the following:</p> <ul style="list-style-type: none">• Name, nationality and address of the trade mark or design applicant/owner/holder, including later changes thereof.• Name of the designers of an RCD.• Name and business address of the representative (when it is a natural person), and changes thereof.• Name and address of the beneficiaries and their representatives (when they are natural persons), in cases of transfers of ownership, rights in rem, licenses and levies.• Name and address of the liquidator (when it is a natural person), in cases of insolvency proceedings.
Retention period	Indefinite (for reasons of legal certainty), as foreseen by Article 111(9) EUTMR and Article 7(1) of the Decision No EX-14-3 of the Executive Director of the Office.



Recipients of the data	<p>In view mode only, all internet users connecting to the EUIPO website, be it individuals or public and private entities, either EU or non-EU sited, in application of Articles 111(5) and (9) EUTMR and 71(1) and (2) CDI.</p> <p>The eRegister beta version is accessed through 'eSearch plus'. Upon finding a specific EUTM or RCD application or registration in 'eSearch plus', the user is presented with the option of viewing the eRegister beta version repository for this specific IP right in a separate interface.</p> <p>There is public access to view the eRegister beta version of any IP right, however for the final version of the eRegister, the user will have to be logged into the User Area to download extracts of the eRegister.</p> <p>In the case of deferred designs, only the registered RCD holder and appointed representative are able to view the details of the RCD in the eRegister beta version.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>All personal data related to the eRegister is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Specific Privacy Statement:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/7d3bc4e6-cbe0-4361-b736-43d736233087</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-007
Name of the processing operation	Amazon Web Services as support for EUIPO IT infrastructure
Last Updated:	27/05/2020
Controller Organizational entity	Digital Transformation
Controller contact details	For internal users: UserFeedback@euipo.europa.eu For external users: DPOexternalusers@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Amazon Web Services (AWS) is an on-demand Cloud computing system that is being used by DTD as the infrastructure for deployment of applications, including "Desktop as a service", a virtual desktop located in the Cloud.</p> <p>In order to support EUIPO infrastructure, these tools might require managing personal data, such as for the connection between AWS and EUIPO systems. This implies exchanging personal data with AWS.</p>
Purpose of the processing	Desktops are to be used for professional purposes but there can be occasional management of personal data.
Data Subjects	EUIPO's staff, SNE's and trainees.
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data to be managed will depend on the application. This includes data which can qualify as personal, and that will be accessible from AWS applications implemented by EUIPO. This might include, but is not limited to, documents and data containing identifying information such as name(s) and surname(s), addresses, phone numbers, photos, and more.
Retention period	Any personal data managed in AWS would be kept in accordance with the retention periods outlined in the EUIPO Data protection notice. In the event of EUIPO finishing their contractual relationship with AWS, all the data contained in AWS would be deleted after 90 days upon contract termination, for security purposes.
Recipients of the data	DTD Operations, AWS and IECISA-ALTIA as the service provider supporting DTD Operations, will have access to the information stored in AWS, in order to carry out their system administration tasks and ensure the correct functioning of the system. The data is not used for any other purposes nor disclosed to any other recipient.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	AWS implements several physical security measures to protect their datacentres, including perimeter security, professional security staff, video surveillance, access control that includes two-factor authentication, fire detection and suppression, and many more. More details here.



General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>Access to the AWS applications is protected by username and password that is secret and only known to the specific staff members that have been granted access on a need-to-know basis. Any connections with AWS are done via secure protocols, in order to prevent unauthorised access.</p> <p>Information that is managed by AWS is kept in secure servers, protected by encryption, strict access control mechanisms, anti-malware systems, and monitoring tools.</p> <p>The Office is using only the following AWS datacentres for EUIPO operations:</p> <ul style="list-style-type: none">• Frankfurt• Dublin and Parkwest, Ireland• Paris• Stockholm. <p>All datacentres are certified under ISO 27001:2013, ISO 27017:2017 and ISO 27018:2019. AWS implements several physical security measures to protect their datacentres, including perimeter security, professional security staff, video surveillance, access control that includes two-factor authentication, fire detection and suppression, and many more. More details on the security measures of AWS can be found here.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Amazon Web Services (AWS) Privacy Statement : https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/data_protection/General_Privacy_Statement_AWS_en.pdf
EDPS Prior consultation	NO



Reference number	DPR-2020-008
Name of the processing operation	Microsoft Teams
Last Updated:	27/05/2020
Controller Organizational entity	Digital Transformation
Controller contact details	For internal users: UserFeedback@euipo.europa.eu For external users: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA ALTIA (DTD external service provider) MICROSOFT (the service provider)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Due to the outbreak of the coronavirus COVID-19 virus, the Office has extended the use of Microsoft Office 365, and in particular 'Microsoft Teams' to organise virtual meetings and teleconferences with internal staff and external stakeholders. MS Teams is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Office. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing.
Purpose of the processing	The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services of business messaging, calling, video meetings and file sharing.
Data Subjects	All EUIPO Staff and external providers with an EUIPO e-mail address. Additionally, EUIPO staff members and EUIPO externals users included in the MS Team that is used for the exchange of information.
Description of categories of persons whose data EUIPO processes and list of data categories	The categories/types of personal data processed are the following: <ul style="list-style-type: none">• Personally identifying Information: username, name, surname, email, work telephone number, current function and preferred language.• Electronic identifying information: IP address, cookies, connection data and access times.• Movies, pictures, video and sound recordings.• Metadata used for the maintenance of the service provided.• Any data as (potentially) processed in the context of file sharing for professional activities (e.g. message, image, files, voicemail, calendar meetings, contacts, and similar) This personal data is processed in accordance with the Processing of personal data for events, trainings and meetings (
Retention period	Retention periods will be in line with the management of personal data in Office 365, that is, for EUIPO staff, data will be retained for as long as there is a contractual relation with the Office. Once a contract expires, information is retained for 90 days for the purposes of collection from the Office or possible renewal. After this period, information is deleted. When dealing with external users, data will be stored in MS Teams for one year after the exchange activity is completed.
Recipients of the data	The personal data is disclosed, under the need to know basis, to the following recipients: <ul style="list-style-type: none">• EUIPO staff members and EUIPO externals users included in the MS Team that is used for the exchange of information;• DTD, Microsoft and DTD's external service provider involved in the data processing necessary to provide the service. Personal data is stored in the EU according to the application configuration implemented by EUIPO.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES



Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>In general terms, Personal data is stored in the EU according to the application configuration implemented by EUIPO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise.</p> <p>Nevertheless, if access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented.</p> <ul style="list-style-type: none">• In all transfers to third countries, Microsoft uses EU Standard contract clauses for the transfer with its subprocessors.• Microsoft requires sub processors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardise and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft. <p>In addition to this, Microsoft implements additional subprocessors to provide ancillary services to support Microsoft Online Services, that as per the documentation of Microsoft, are necessary to support, operate, and maintain online services. In the particular case of MS Teams, Microsoft implements "Interana" for operational analytics. After validation with Microsoft, they confirm that Internana has gone through the assurance program described above to ensure the appropriate management of personal data, and ensures that they are contractually obliged to comply with the data protection requirements of Microsoft.</p>
General Description of security measures	<p>MS Teams has been configured to preserve the confidentiality of the information you exchange by implementing encryption during all communications and in storage, and anonymous access is not authorized. Any information you add to a group in MS Teams, be it via chat, video conference or file sharing, will be available only to the recipients described above.</p> <p>Microsoft data centres are certified in several security standards, most notably ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud.</p> <p>Microsoft has implemented several safeguards to ensure the availability of the information. As a minimum, data is replicated between two data centres within the same region, has redundancy controls and implements backups that are encrypted before being transmitted and stored.</p> <p>Data centres have physical and logical security monitoring measures, such as:</p> <ul style="list-style-type: none">• video surveillance of the perimeter;• seismic and environmental monitoring at the buildings;• monitoring of security threats, such as worms, denial of service attacks, unauthorised access, or any type of unlawful activity. <p>Microsoft has implemented a list of over 700 safeguards in Microsoft's systems, servers, and data centres. This includes safeguards against accidental or unlawful destruction, loss, unauthorised access, use, modification or disclosure. These internal controls are audited on a yearly basis, if required, audit information can be provided under a Non-Disclosure Agreement (NDA). Information is encrypted while at rest and in transit.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement:</p> <p>https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/vi/DPR_2018-003_Office_365_MS_Teams_PRIVACY_STATEMENT.pdf</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-009
Name of the processing operation	Virtual events organised through Zoom Video Communications
Last Updated:	11/06/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Infrastructures and Buildings Department acts as processor when the use of Zoom is requested by other Department/Service of EUIPO. In this situation, the requesting Department/Service will act as controller. External Processor: audio- visual services provider Vitelsa (http://www.vitelsa.es/es/home), videoconference services provider Zoom Video Communications (https://zoom.us/)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

In the light of the outbreak of the coronavirus COVID-19 and its rapid expansion, the Office has taken a number of precautionary measures in order to ensure the health and safety of its staff, resources and stakeholders. One of these measures is to substitute the face-to-face meetings/events with video conference meetings/events. Infrastructures and Buildings Department (IBD) has looked at different providers of video conference services. It has been concluded that the tool that answers best to the technical requirements for virtual events (availability of interpretation, moderator features, etc.) of the Office is Zoom Video Communications (Zoom). Zoom is a cloud-based videoconferencing platform that ensures the successful organisation of events in a virtual environment and the effective interaction with the Office stakeholders as close as possible to the face to face experience. The initial Privacy and security risk assessment of the tool indicates that the risk for the rights and freedoms of the data subjects is Medium in case a series of mitigation measures are implemented.

Nevertheless, important security and privacy vulnerabilities related to the use of Zoom were made public in numerous press releases and other publications, which naturally raised serious concerns at the Office. For this reason the EUIPO set up a technical task force, composed of representatives of relevant departments to assess technical, security and data protection aspects of the use of Zoom and support EUIPO Management to take an informed decision on the use of the platform. As far as the security issues are concerned, Zoom released a series of IT patches which solved part of the identified issues. Moreover, the Office has reduced the majority of the remaining issues to the extent possible by configuring the existing settings in the Zoom platform.

As far as the data protection aspects are concerned, the EUIPO delegated data controller, together with the EUIPO DPO, conducted a threshold assessment using the EDPS methodology.

The risk is qualified as Medium in case a series of mitigation measures are implemented. Detailed information can be found in the risk assessment linked below.

After configuring the Zoom platform according to the most secure options available and upgrading the platform with the latest patches provided by Zoom, the task force has come with the conclusion that the security, the data protection and the technical risk of using this solution for EUIPO virtual events has been reduced to Medium. Nevertheless, external factors such as the reputational issues and the benchmarking with other EU institutions and agencies heighten the overall risk to High.

On the basis of this analysis and the conclusions of the task force, EUIPO management has decided to:

- use Zoom in specific events with external stakeholders and when necessity can be justified (such as MBBC);
- Closely monitor the evolution of Zoom.

With the release of the version 5.0 of the software Zoom, some open issues have been resolved, particularly the weak encryption question which now provides a secure standard encryption mechanism. This release brings other security improvements such as password complexity, meeting identifications (IDs) protection, or meeting lock. However, the end to end encryption feature, which is a key issue from a data protection point of view, is not fixed within this release. The updated assessment of the task force indicates that although some considerable technical and security aspects have been improved with the last release of the Zoom software, the overall assessment of the platform remains high.

Due to the particular situation (Business Continuity scenario launched as result of the expansion of the COVID-19 virus) the processing operation is based on 5.1 a of Regulation (EU) 2018/1725: processing is necessary for the performance of a task carried out in the public interest on the basis or in the exercise of official authority vested in the Union institution or body.

IBD (through its audio-visual services provider) is in contact with Zoom in order to ensure that the identified mitigations measures are implemented. One of these measures that has been already implemented is the signature of a Data Processing Addendum through which Zoom has committed to comply with the requirements of the applicable data protection Regulation (EU) 2018/ 1725 and to act only under the instructions of the data controller. Another measure taken by IBD as delegated controller was to give clear instructions to the data processors regarding the way data should be processed on behalf of EUIPO.

Moreover, IBD has prepared User Manual for Zoom that provides user-friendly information and description of the main



features available to event participants in Zoom.



Purpose of the processing	Personal data is processed for the purpose of organisation and conducting of virtual events organised by EUIPO.
Data Subjects	Participants (external participants and EUIPO staff and resources) in virtual events organised through Zoom.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The data processed for the purpose of organisation of video conference meetings is as follows:</p> <ul style="list-style-type: none">• username;• general information about service preferences;• information about user's device, network and internet connection, such as IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version;• information about usage of or other interaction with Zoom Products ('Usage Information');• other information the user uploads, provides or creates while using the service;• metadata used for the maintenance of the service provided;• optional data: telephone number of a person making a call using Zoom services (e.g. Zoom Phone) and data collected through the use of cookies and pixels (only in case the user visits one of Zoom marketing website) <p>As part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between the Office and stakeholders, such as instant messages (chat), images, files, whiteboards, transcripts and recordings. Recordings are done in the tool only if strictly necessary for legitimate and explicit purposes. The user is automatically notified when a recording starts and will be given the option to leave the virtual event in case he/she does not wish to be recorded. In case the user objects to the recording on the basis of compelling and legitimate grounds, the recording will be paused during the intervention of this user.</p> <p>Additional data (for example an email address) could be collected depending on whether the user joins the virtual event through an Android or an iOS device.</p>
Retention period	<p>Personal data processed by the data controller or the service providers under its supervision are generally stored for the period of time necessary to achieve the purpose for which they have been processed.</p> <p>Zoom shall retain the Personal Data for 1 month, unless the European Union or national laws of Member States of the European Union would require a longer storage of personal data.</p>
Recipients of the data	<p>The personal data is disclosed, on a need to know basis, to the following recipients:</p> <ul style="list-style-type: none">• EUIPO staff members and EUIPO externals users participating in the virtual events organised through Zoom;• IBD Hospitality team and external providers like the events management provider 'Pomilio Blumm', audio-visual services provider 'Vitelsa' and its provider Zoom. <p>In case of transfer of personal data to third parties outside the EEA, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed. Zoom has certified its compliance with Privacy Shield Framework and uses Standard Contractual Clauses as appropriate safeguard.</p> <p>EUIPO does not process personal data for any other purposes nor discloses it to any other recipient. Data may be accessed by Zoom subcontractors (https://zoom.us/subprocessors). Zoom signs agreements with all its service providers that prevent them from processing of data for their own purposes or for the purposes of another third party.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?

In case of transfer of personal data to third parties outside the EEA, all the provisions stipulated in Chapter V of Regulation (EU) 2018/1725 will be observed. Zoom has certified its compliance with Privacy Shield Framework and uses Standard Data Protection Clauses as appropriate safeguard. The Standard DP clauses were signed between Zoom and the audio-visual provider of the EUIPO as part of the Data Processing Addendum.



<p>General Description of security measures</p>	<p>Zoom uses Amazon Web Services (AWS) for the storage of their platform and any data contained within. AWS is certified in several information security frameworks, including ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC2 and SOC as per information available on the web.</p> <p>AWS Datacentres have implemented multiple security measures to prevent technical issues such as unauthorized access, destruction, loss, etc. These measures include:</p> <ul style="list-style-type: none">• redundant power systems and environmental controls• access logs• 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses.• back-up power supply;• data encryption capabilities available in AWS storage and database services, such as Amazon Elastic Block Store, Amazon Simple Storage Service, Amazon Relational Database Service, and Amazon Redshift.• flexible key management options, including AWS Key Management Service (KMS), allow customers to choose whether to have AWS manage the encryption keys or enable customers to keep complete control over their keys.• AWS customers can employ Server-Side Encryption (SSE) with Amazon S3-Managed Keys (SSE-S3), SSE with AWS KMS-Managed Keys (SSE-KMS), or SSE with Customer-Provided Encryption Keys (SSE-C). <p>Zoom is certified SOC 2 (type II) and implements standard industry security measures, such as: Audio signature, Chat Encryption and communications are established using 256-bit TLS encryption and all shared content can be encrypted using AES-256 encryption.</p> <p>In addition, according to the Data Processing Agreement-Exhibit B, Zoom commits to implement the additional controls to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.</p> <p>EUIPO staff and service providers (events management provider and audio-visual services provider) dealing with personal data in the context of conducting of video conference meetings sign a confidentiality declaration.</p> <p>EUIPO has pre-configured the tool settings in order to make sure that the personal data is protected and that all possible measures have been taken to safeguard the confidentiality, integrity and availability of the information within the tool. The following settings have been configured in the tool:</p> <p>The meeting is protected by a random password (except for webinars)</p> <p>The participants join a waiting room before they are authorized to join the event by the host (except for webinars)</p> <p>Participants do not have to authenticate themselves before they join the meeting</p> <p>Participants cannot share videos/files of their screen during virtual events</p> <p>The host of the meeting can admit/remove participants in the meeting (sending them to the waiting room, putting them on hold or removing them completely from the meeting, unabling them to join again)</p> <p>Hosts can lock conference (thus avoiding unwanted participants from joining the meeting)</p> <p>Participants cannot take control of the presentation/screen</p> <p>Recording in Zoom can be done only by the host and co-host and only if strictly needed for legitimate and explicit purposes</p> <p>Participants are automatically notified by the tool when a recording starts (by sound notification and a disclaimer appearing on the screen)</p> <p>Recordings should be done locally on the computer of the host (except for webinars where the recording can be done on Zoom cloud)</p>
---	---



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Specific Privacy Statement for participants in video conference meetings organised by EUIPO through Zoom Video Communications : http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/ed5dd152-f7ae-46ce-a56d-5a7e7ffd34c6
EDPS Prior consultation	NO



Reference number	DPR-2020-010
Name of the processing operation	CD Events Management and Feedback
Last Updated:	11/09/2020
Controller Organizational entity	Customer
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain
Joint Controller organizational entity	Other
Joint Controller contact details	For events managed via the Office's event management provider: Infrastructures and Buildings Department (IBD) For recording, photographing and communication purposes: Communication Service (CS) For feedback purposes, the use of Lime survey is maintained by Digital Transformation (DTD)
Name and contact details of processor	eXTEL Contact Centre which provides Information Centre (First Line) services DELOITTE consulting services (feedback analysis) Other processors are used for the general management and coordination of events (e.g. Pomilio Blumm, recording & taking of pictures/videos, media and website communication). For more information: Standard PS for external participants Standard PS for EUIPO's staff For feedback of the event, Lime survey tool is used and personal data is supported by IECISA-ALTIA, for the purposes of managing EUIPO IT infrastructure and maintenance tasks. For more information: https://euiipo.europa.eu/ohimportal/en/data-protection
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description

The CD organises and manages different types of events with customers, potential customers and stakeholders of the SME Programme during the year (e.g.: physical or virtual IP for You events, physical or virtual fairs, video-conferences, loyalty visits). These events can be face to face or virtual.

IP for You: series of seminars aimed at customers of the Office's services in a series of EU cities. The purpose is to promote the products and services of the Office.

Loyalty visits: ad-hoc and personal visits to customers at their premises carried out by EUIPO experts.

Videoconferences: series of videoconferences to connect with customers in a more direct way.

Fairs for SMEs and entrepreneurs in order to gather information and trainings needs.

The processing is automated and is described as follows:

a) Management of Events

The promotion and invitation to an event (except for fairs) is initiated by the Information Centre who contacts EUIPO's customers directly by phone or email. The Office's external provider is in charge of the events online registration and logistics coordination. For further information, please consult [here](#).

For contact management purposes, the customers' data is obtained via PER, SAP CRM, SAP BCM and the internal Consumer Contact Database.

The Office's external provider managed by IBD is in charge of the events online registration and logistics coordination.

Event participants are requested to confirm attendance in a paper attendance list during the event(physical fairs or events). After the event, this list is further shared with the internal team in charge of feedback at the Customer Department, and, in the context of IPforYOU, can be transferred to national intellectual property offices and other organisations co-organising the events with EUIPO. The Mission Reports from workshops can contain personal data.

Physical or virtual fairs, allowing networking and contact with the stakeholders and partners of the SME Programme, are organised by EUIPO, in order to allow exchange of information between the participants and the exhibitors, gather information and training needs of entrepreneurs, start-ups and European Union SMEs and promote intellectual property.

Some of the events (e.g. loyalty visits and video-conferences) can be entirely managed and coordinated by staff of the Customer Department. All personal data is gathered in a mission plan and mission report documents.

This records should be read in conjunction with the general Office's records managed by IBD.

b) Feedback of Events

Feedback from customers is generally gathered through surveys that are sent via email to the participants after an event. The Office's Lime survey tool is used for these surveys.

Some additional Feedback can be gathered via email, such as information and training needs of SMEs in the context



of Fairs..

Any other feedback provided orally by a customer may also be collected. Some feedback can be gathered via emails, such as information and training needs of SMEs and start-ups related to intellectual property, in the context of fairs.

After each event, a mission report is drafted by the respective team where feedback of the customer may be collected. All mission reports are saved in ShareDOX.

The feedback is further processed through the Feedback Table and Suggestion Table, both excel files saved in ShareDOX. These tables allow Information Centre to follow up directly with customers, analyse customer's needs and enable the Office to implement required changes or improvements. Customers may be informed of the improvements that have been done following their feedback.



Purpose of the processing	<p>The purposes of this processing operation are:</p> <ul style="list-style-type: none">• to organise and manage events, coordinate any required follow-up activities;• to promote the EU trade mark and RCD systems, including EUIPO services;• to manage user expectations and increase satisfaction levels by solving users' issues, and collect information and training needs of SMEs;• to analyse data and identify areas of improvement for services rendered to the EUIPO's customers. <p>Your personal data is not intended to be used for any automated decision making, including profiling.</p>
Data Subjects	<p>The data subjects are customers who are invited to participate to the Events (external users, key users, potential key users). Personal Data of EUIPO's staff participating in the Events may also be processed.</p>



Description of categories of persons whose data EUIPO processes and list of data categories

The data subjects are customers who are invited to participate to the Events (external users, key users, potential key users). Personal Data of EUIPO's staff participating in the Events may also be processed.

The categories/types of personal data processed are the following:

- Customer's data:
 - PER ID
 - name
 - email
 - telephone number
 - dietary preferences
 - feedback or testimonials

- EUIPO staff (Key User Managers):
 - name
 - email
 - telephone number
 - function in the Office
 - dietary preferences
 - feedback or testimonials

For both Customers and EUIPO staff, in the context of visits (e.g. IPforYou): photos, sounds, videos and audio-visual recordings can be collected. (Users will be informed of the processing of such data at the beginning of each event and a notice will appear in screens of the place of the event).

In the context of virtual IPforYOU events, we use the external provider Zoom. The personal data processed through Zoom is as follows:

- username;
- general information about your service preferences;
- information about your device, network and internet connection, such as your IP address(es), MAC address, other device ID (UDID), device type, operating system type and version, and client version;
- information about your usage of or other interaction with Zoom Products ('Usage Information');
- other information you upload, provide or create while participating in the event;
- metadata used for the maintenance of the service provided;
- optional data: telephone number of a person making a call using Zoom services (e.g. Zoom Phone) and data collected through the use of cookies and pixels (only in case you visit one of Zoom marketing websites)

As part of the nature of a collaborative tool, additional personal data may be included in the information that is exchanged between the Office and stakeholders, such as instant messages, images, files, whiteboards, transcripts and recordings. You will be automatically notified when a recording starts in the tool and will be given the option to leave the virtual event in case you do not wish to be recorded. Moreover, if you do not want your image/voice to be recorded in the tool, for compelling and legitimate grounds, you can exercise your right to object by indicating it to the event host so that the recording is paused during your intervention. Please note that if there is any recording during the event, it will be carried out only for legitimate and explicit purposes.

Additional data could be collected depending on whether you use an Android or an iOS device.



For further details on the processing of your data in the context of virtual IPforYOU events through Zoom, please consult this [privacy statement](#).



Retention period	<p>Personal data will only be kept for the time necessary to achieve the purposes for which it is processed.</p> <p>Your personal contact details are kept in the internal document management database for the purposes mentioned above for 2 years.</p> <p>The certificates of attendance issued for the users who participated in events will be stored in the internal databases for a period of 2 years after the event (closing date).</p> <p>Photos, sounds, videos and audiovisual recordings will be kept for a period of 2 years after the event (closing date).</p> <p>In general, feedback and testimonials (of any kinds) are kept for 2 years after receiving them for carrying out analysis, taking into consideration your suggestions and possible follow-up. However, we might publish them with your consent on EUIPO Insite, EUIPO website, or our other social media channels for a period of 5 years.</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal process.</p> <p>In the context of virtual IPforYOU events, Zoom shall retain the Personal Data for 1 month unless the European Union or national laws of Member States of the European Union would require a longer storage of personal data.</p>
Recipients of the data	<p>Personal data is made accessible only on a need to know basis to a public mainly composed of EUIPO staff members and possibly external providers and their subcontractors and the general public.</p> <p>Personal data is accessed by:</p> <ul style="list-style-type: none">• The CD, and in particular, the Information Centre (First Line and Second Line) and the internal teams of Customer Feedback and Key User Management.• Internal and external staff from the Digital Transformation Department for the technical maintenance of the IT tools.• External providers such as Deloitte and the events management provider 'Pomilio Blumm'.• In the context of visits (e.g. IPforYou): the list of participants can be shared with national intellectual property offices and other organisations co-organising the events with the EUIPO, and testimonials, photos, sounds, videos and audiovisual recordings can be published on EUIPO communication channels, or newsflashes sent to all Key Users.• In the context of virtual IPforYOU events: videoconference services provider 'Zoom Video Communications'. Zoom is the external provider used by the Office. Please consult the privacy statement.• Concerning information and trainings needs for SMEs, only the working group involved in the SME Programme.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre• Confidentiality and data protection clauses are signed-off by the service provider. <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement for CD Events Management and Feedback: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/331b57f5-7a82-4b2c-b73a-c0cfd2289185</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-011
Name of the processing operation	Delivery of Office equipment, materials and information to EUIPO staff during business continuity scenario
Last Updated:	30/03/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal Processors: EUIPO Departments Secretariats IBD Secretariat FM team Externl Processors: Severiano Servicio Movil. DHL
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	In the light of the outbreak of the coronavirus COVID-19 virus and its rapid expansion, the Office has taken a number of precautionary measures in order to ensure the health and safety of its staff, resources and stakeholders. One of these measures is to provide Office equipment, materials and documents to the homes of the staff members who have requested this. In order to be able to perform this service IBD has to maintain a table with the names and the contact details of the staff members of all departments who have expressed interest to receive Office equipment/material/information.
Purpose of the processing	The purpose of the processing operation is to ensure that EUIPO staff is provided with the necessary equipment/material/information in order to be able to perform their tasks during the business continuity scenario caused by the expansion of the novel coronavirus COVID 19
Data Subjects	All staff members who have requested to receive in their homes Office material/equipment/ information.
Description of categories of persons whose data EUIPO processes and list of data categories	The personal data processed is as follows: name, surname, address, telephone number.
Retention period	Data will be deleted once the Office equipment/material/information is returned to the Office premises.
Recipients of the data	Data will be accessed on a need to know basis only by authorized staff and resources strictly necessary for the achievement of the purpose of this processing operation like the Secretariat of the department of the person requesting equipment/material/information, IBD Secretariat, Workplace team in IBD and the external providers Severiano Servicio Movil and DHL.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to this processing operation is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2).</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Disclaimer inserted in the mail to the Staff members :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A/SpacesStore/7fd02d93-cfe5-4d29-9a53-d32e59caa1e1</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-012
Name of the processing operation	Management of services during business continuity scenario
Last Updated:	24/04/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal Processors: EUIPO contract managers, Secretariats of relevant EUIPO departments, Security team in Infrastructures and Buildings Department (IBD), Facility management service in IBD External Processors: Maintenance and cleaning services provider, Security services provider
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	During the business continuity scenario caused by the expansion of the novel coronavirus COVID 19s the minimum services in the European Union Intellectual Property Office (EUIPO) should be guaranteed. Therefore, staff members and external resources should be authorised to come to the EUIPO premises in order to perform their tasks. For this purpose, an excel table is managed in the document management system of EUIPO- Sharedox where personal data of the staff/resources authorised to access the Office premises during the business continuity scenario is managed. The location data is needed on order to ensure that the work spaces are cleaned and maintained in order to ensure the appropriate working conditions for staff/resources.
Purpose of the processing	The purpose of the processing operation is to ensure that the necessary minimum services are provided in EUIPO during the business continuity scenario caused by the expansion of the novel coronavirus COVID 19.
Data Subjects	Data subjects: Staff members and external resources who must access and perform their tasks in the Office premises during the business continuity scenario.
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data: name, surname, company, department, authorised day/hour to access the premises, activity
Retention period	The data of the staff members (the majority of which are part of the BCP team) will be stored for 1 year as the possibility that the business continuity scenario is launched again is high. The data of the external resources will be deleted within 1 month from the end of the current business continuity scenario.
Recipients of the data	Data recipients are as follows: EUIPO contract managers, Secretariats of relevant EUIPO departments, Security team in Infrastructures and Buildings Department (IBD), Facility management service in IBD Maintenance and cleaning services provider, Security services provider
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>All personal data related to this processing is stored in secure IT applications according to the security standards of EUIPO. These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Specific Privacy Statement for participants in video conference meetings organised by EUIPO through Zoom Video Communications:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/df55a96b-8941-4b73-9174-1117d308dc2a</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-013
Name of the processing operation	Processing Personal Data for Legal Entity and Financial Identification
Last Updated:	07/04/2020
Controller Organizational entity	Finance
Controller contact details	Director of the Finance Department FD.DataProtection@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Personal data is collected and managed by the Office in a common file (Legal Entity and Financial Identification) and recorded in the Office's accounting system only to the extent necessary to process and account for financial and contractual relations you have or will have, directly or indirectly, with the Office.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	Data is collected and managed by the Office to ensure that contacts are channelled and contracts are signed through/by the person(s) identified in the Legal Entity and Financial Identification and payment is made to the bank account stated therein.
Data Subjects	Personal data processed is the one recorded in the Legal Entity and Financial Identification.
Description of categories of persons whose data EUIPO processes and list of data categories	Personal data processed is the one recorded in the Legal Entity and Financial Identification.
Retention period	<p>The data is subject to the administrative retention period stated in the Office's retention policy in force. Once the period has elapsed, paper documents stored in the Office archives will be destroyed. The retention period runs from the date the file is closed.</p> <p>Furthermore, to provide an audit trail and allow queries on past payments at all times, no recorded data is deleted from the accounting system. The forms and documents are archived electronically.</p>
Recipients of the data	Personal data collected will be treated confidentially and processed by authorised staff members. For the purposes of safeguarding the Union's financial interests, the personal data may be transferred to internal audit services, to the European Court of Auditors or to the European Anti-Fraud Office (OLAF), and between authorising officers of the Union bodies, the Commission and the executive agencies, the European Court of Justice and any other institution responsible for audits and investigations.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>Personal data is stored in secure IT applications according to the Office's security standards, as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients.</p> <p>These include:</p> <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre <p>Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2)</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing personal data for Legal Entity and Financial Identification:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/3f73ce04-e2a7-4b07-8fb7-043b42af8b9f</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-014
Name of the processing operation	Transfer of email addresses of applicants and representatives filing International Applications to WIPO in the emergency context of COVID-19
Last Updated:	20/04/2020
Controller Organizational entity	ICLAD
Controller contact details	EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Email: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	For the purposes of the transfer of personal data to WIPO, authorised staff of the Customer Department, the Digital Transformation Department and the Operations Department will act as internal data processors.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>In the emergency context of COVID-19, the World Intellectual Property Organisation (WIPO) requested EUIPO to provide the email addresses of applicants or representatives (users) who filed or file International Applications (IA) and whose email address is not available at WIPO. This request affects only applications with EUIPO as office of origin, not as designated office.</p> <p>Given the disruption of postal services worldwide including in Switzerland, WIPO is not able to send or receive communications by postal mail until further notice. From now on, applicants, holders and their representatives may continue to send communications under the Madrid System to WIPO, but they should do so by electronic means only. As office of origin, EUIPO is already transmitting to WIPO data included in IAs (including personal data). The EUIPO will now transfer an additional data set of email addresses that users provided in their EUIPO User Area (stored in the PER database). The e-mail addresses of the data subjects will be transferred to WIPO in compliance with the provisions on international transfers set out in Chapter V of Regulation (EU) 2018/1725.</p> <p>In the emergency context of COVID-19 the collection and transfer of the above email addresses is justified as it is necessary for important reasons of public interest. For existing IAs, users will be contacted by EUIPO and offered the possibility to opt out from the transfer. For new IAs, the field of the email address of the applicant will be converted into a mandatory one with an explanation of the reason and that it will be a temporary measure.</p>
Purpose of the processing	The collection, storage, processing and transfer of new email addresses or the transfer of email addresses already available in EUIPOs PER database for IA users of EUIPO serves the purpose of temporarily palliating the effects of the current emergency situation due to the COVID-19 pandemics. The users filing international applications will be contacted by WIPO by email given the disruption of the postal services.
Data Subjects	For new and existing users who file or have filed an International Application with the EUIPO, natural persons who provide their email address to EUIPO.
Description of categories of persons whose data EUIPO processes and list of data categories	For the new and existing users who file or have filed an International Application with the EUIPO, the personal data provided to the WIPO is the email address indicated by the applicant, owner or representative provided in their EUIPO User Area (stored in the PER database) and, if the latter is a physical person, his/her name.
Retention period	<p>The data files which form part of the transfer to WIPO will be kept only as long as they are necessary due to the exceptional circumstances caused by COVID-19.</p> <p>Email addresses available in the EUIPO PER database (record DPR-2018-078) will be kept in accordance with Article 112(5) of Regulation (EU) 2017/1001 which provides that all data will be kept indefinitely. However, the party concerned may request the removal of any personal data from the database after 18 months from the expiry of the EU trade mark or the closure of the relevant inter partes procedure. The party concerned will have the right to obtain the correction of inaccurate or erroneous data at any time.</p>



Recipients of the data	<p>Access to the personal data which form part of the transfer will be available to:</p> <ul style="list-style-type: none">• authorised staff of the International Cooperation and Legal Affairs Department for the purposes of transferring the data to WIPO• examiners from the Operations department in charge of the PER database where all the particulars of the users of the EUIPO services are kept• experts (database administrators) from the Digital Transformation Department in charge of extracting existing contact details from the EUIPO PER database• authorised staff of the Customer Department for the purposes of interaction with the affected users <p>The email addresses will be transferred to the WIPO only in the emergency context of COVID-19 and to WIPO's authorised staff.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>World Intellectual Property Organization (WIPO), an international organisation which accepted the conditions of an arrangement for the transfer.</p> <p>The transfer of personal data to WIPO is based on:</p> <p>Memorandum of Understanding signed by WIPO and EUIPO on 2 March 2015</p> <p>Article 50(1)(d) of Regulation (EU) 2018/1725</p> <p>Articles 183 and 184 of Regulation (EU) 2017/1001</p>
General Description of security measures	<ul style="list-style-type: none">• Authentication and authorization based on roles.• Authentication and authorization at server level, no anonymous access allowed.• Server is physically protected at the Data Processing Centre.• Logical security hardening of the servers. <p>The information is also available directly in the database. The access to the database is restricted to some DTD staff internal and external. Confidentiality and data protection clauses are signed-off by the service provider.</p> <p>All the standard security measures available for EUIPO's databases. The Office's server has been certified by an international certifying authority (Verisign Inc.), which guarantees that users have in fact connected to the Office. All information transmitted via the internet is encrypted using SSL protocol.</p> <p>For the transfer of the data set, encryption is available.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Transfer of email addresses of applicants and representatives filing international applications to WIPO in the emergency context:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/90a72216-c974-4e97-97ac-aa0938d858bb</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-016
Name of the processing operation	OD Calls for Interest
Last Updated:	08/05/2020
Controller Organizational entity	Operations
Controller contact details	Contact: Director of the Operations Department, EUIPO ODDPC@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>OD organises internal Calls for interest (Cfl) each time the Department has an internal need for, or is requested to appoint speakers, trainers, participants, members, observers, etc. for a variety of activities of the Department and of the Office, such as missions, trainings, horizontal networks, knowledge circles, quality initiatives, to name just a few. Whenever there is such request, an email is sent to all OD staff, from a functional inbox (OD Calls for Interest), containing the details of the activity, the selection criteria and the deadline to apply. Replies with applications are received, collected and saved into an excel sheet in ShareDox. The excel sheet contains the name of the examiner, the team and service, the HoS and TL, the working languages and the experience, whenever they are relevant and have been requested, and the motivation for the application. The list of applications is examined by OD Management and the selection of the candidate/s is done, taking into account the criteria stated in the initial email to OD staff. Both the successful and the unsuccessful candidates are informed of the outcome of the Cfl, by way of follow-up emails sent from the OD Calls for Interest mailbox, with the corresponding TL and HoS in copy. The participants who are not selected are never named in the follow-up emails (they are not identifiable because the email informing them is sent in blind copy), but the selected ones are named for the sake of transparency.</p> <p>The information on the participation of the selected and appointed OD staff members is kept into another excel sheet in ShareDox that contains the event type, name, organiser, place and date, the type of profile sought for, the language, the appointed person(s), and the number of candidates for each specific Cfl.</p> <p>The task of coordinating the OD Cfl (sending emails with new Cfl, receiving and compiling the applications, presenting them to OD Management for decision, informing the candidates of the outcome and the requester in case of Cfl for activities outside of OD) and keeping track of every participation in ad hoc events of permanent horizontal networks are handled by a member of the OD Central team in charge of the coordination of all Cfl, and OD Secretariat (acting as back-up).</p>
Purpose of the processing	The purpose of the processing is to: Give the opportunity and encourage more OD examiners to participate in horizontal activities (both department and Office-wide) so that they expand their knowledge and experience; Guarantee the transparency of the decision making process on the appointments for participation and assignments outside the core activity of the department.
Data Subjects	Data subjects are OD staff members who apply for a Call for Interest.
Description of categories of persons whose data EUIPO processes and list of data categories	Data subjects are OD staff members who apply for a Call for Interest. The name, service, team, working languages, profile, experience and motivation provided in the application email will be collected.
Retention period	Three years



Recipients of the data	The member of the OD Central team responsible for the Cfl coordination OD Secretariat OD Management (Heads of Service, Deputy Directors and Director) OD Central team Only in specific and restricted number of cases, OD Reference Persons, OD Training Think Thank, OD QPROs. All participants to a Call for interest are informed of the name/s of the selected candidates.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	Standard security measures of the ShareDox knowledge management system.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Specific Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/27330ffd-d589-4b89-b18c-77830f3a2f7a
EDPS Prior consultation	NO



Reference number	DPR-2020-017
Name of the processing operation	Processing of personal data by IBD in the framework of the Plan for the return to the Office's campus
Last Updated:	02/06/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processors: Security, space, maintenance and internal distribution teams in IBD, IBD Secretariat, contract managers in IBD External processors: <ul style="list-style-type: none">• events management provider 'Pomilio Blumm' for the purpose of scheduling the medical tests;• security services provider 'Securitas' for the purpose of organization of the access to the Office premises;• maintenance service provider Ferrovial Servicios S.A and cleaning service provider Ferroser Servicios Auxiliares S.A. for the purpose of maintaining the Office spaces;• external provider of mail/parcel distribution services EULEN for the purpose of internal mail distribution.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante



Description	<p>On 14 March 2020, Spain declared the state of alarm because of the COVID-19 outbreak and the sanitary crisis triggered by the coronavirus pandemic. As a consequence thereof, on 16 March 2020 the Office moved to full teleworking status and its campus was emptied, except for a very small number of staff members and/or external contractors who remained on-site to ensure maintenance of basic infrastructures and services.</p> <p>In view of the evolution of the pandemic in Spain, the confinement may be partially lifted as of 9 May 2020. Consequently, the Office has prepared a plan for a gradual return of staff to the campus.</p> <p>The return process will take place in two phases</p> <ul style="list-style-type: none">• The first phase starts when the Spanish authorities move away from the present confinement situation by lifting significant confinement measures (at national, regional or provincial level) and ends with the full re-opening of the European School and the rest of schools. <p>The main purpose of this first phase is to begin taking steps towards the gradual and controlled re-use of the campus and will be open only to voluntary participation except when the nature of the tasks and the interest of the service require staff to be present on campus.</p> <p>On the first phase of return to the Office premises, all internal staff will be medically tested by the Medical Service before coming back to the Office, as a preventive measure to comply with the Staff Regulations (SR) and Conditions of Employment of Other Agents (CEOS).</p> <p>As far as the external resources are concerned, EUIPO requires from its service providers to comply with health and safety requirements stemming from Ley31/1995 and Real Decreto 171/2004. In order to comply with the applicable regulation, service providers must ensure their employees do not present a risk for the health and safety of the rest of the people working in the Office premises. Service providers can choose between performing medical tests on their employees on their own or with the help of the Medical services at EUIPO premises. In any case, EUIPO will not process health data of external resources.</p> <ul style="list-style-type: none">• The second phase starts with the full re-opening of the European School and the rest of schools and ends when the Spanish authorities lift the last significant confinement measures at national, regional or provincial level. This phase will be extended to all staff. <p>IBD Secretariat will process the list of staff members in IBD who have volunteered to return to the Office premises or for whom the nature of their tasks and the interest of the service require their presence at the campus.</p> <p>Contract managers in IBD will process the data of the external resources in IBD who are authorised to return to the Office premises by their companies.</p> <p>For the purpose of scheduling of the medical testing, the events management provider of IBD will process personal data (name, surname and email) of the staff members who must pass through medical testing performed by the Medical services at EUIPO. This processing will be done in the events management database Metis as described in Record DPR-2019-007.</p> <p>Data of staff members and external resources authorised to return to the Office premises will be processed by IBD teams for the purpose of access, space, maintenance and internal mail distribution management.</p>
Purpose of the processing	<p>IBD processes personal data of staff members and external resources for the purpose of:</p> <ul style="list-style-type: none">• access management in order to organize the access of the people authorized to return to the Office premises;• space management in order to adjust the areas of the buildings assigned to the different departments and ensure social distancing;• maintenance management in order to ensure the cleaning and maintenance of the occupied Office spaces;• Internal mail distribution. <p>IBD will as well process personal data (name and email) of internal staff for the purpose of scheduling the timetable for the medical testing.</p>
Data Subjects	<p>Staff members and external resources authorised to return to the Office premises.</p> <p>Staff members who must go through a medical testing before returning to the Office premises.</p> <p>Staff members of IBD who have volunteered to return to the Office premises or for whom the nature of their tasks and the interest of the service require their presence at the campus.</p>



Description of categories of persons whose data EUIPO processes and list of data categories	IBD will process personal data as follows: <ul style="list-style-type: none">• Name, surname and email of staff members who will be invited to do the medical tests;• Name, surname and office location of the staff members and external resources authorized to return to the Office premises.
Retention period	Personal data of the staff members and external resources authorised to return to the Office premises is retained in the document management system Sharedox for the duration of the COVID-19 crisis and deleted afterwards. The list of IBD volunteers should be deleted by IBD after confirmation of the final list of staff authorised to return to the Office premises; The list of staff members who are invited to do the medical tests, which is processed by IBD for the purpose of organization of the access to the Office premises, will be deleted by the Security team in 1 day after the end of the period of medical testing. The events management provider has been instructed to delete the data of staff members (who have booked a slot for the medical tests through the page provided by Pomilio) from its database after the end of the booking period and after the information was sent to HRD (Medical services).
Recipients of the data	Data of the staff members and the external resources authorised to return to the Office premises is accessed by IBD teams as follows: <ul style="list-style-type: none">• events management provider 'Pomilio Blumm' accesses data of staff members only for the purpose of scheduling the medical tests;• security services provider 'Securitas' and internal security team for the purpose of organization of the access to the Office premises;• maintenance service provider Ferrovial Servicios S.A and cleaning service provider Ferroser Servicios Auxiliares S.A. and internal maintenance and space management teams for the purpose of maintaining the Office spaces;• external provider of mail/parcel distribution services EULEN for the purpose of internal mail distribution. IBD Secretariat will access the list of staff members in IBD who have volunteered to return to the Office premises or for whom the nature of their tasks and the interest of the service require their presence at the campus. Contract managers in IBD will process the data of the external resources in IBD who are authorised to return to the Office premises by their companies.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	All personal data related to the processing of IBD is stored in Sharedox according to the security standards of EUIPO. These include: <ul style="list-style-type: none">• Role-based access control to the systems and network• Logical security hardening of systems, equipment and network• Physical protection via secure Data Centre Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) Security measures applied in the events management database Metis are described in Record DPR-2019-007.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement Return Plan: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/322ca62d-87c3-4e1d-8914-39095eaefcd2



EDPS Prior consultation NO



Reference number	DPR-2020-018
Name of the processing operation	Manage of personal data in CISCO Umbrella
Last Updated:	03/09/2020
Controller Organizational entity	Digital Transformation
Controller contact details	UserFeedback@euipo.europa.eu
Name and contact details of processor	Cisco Systems, Inc. IECISA-ALTIA, DTD Service provider for IT operations
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Cisco Umbrella is a cloud security platform that unifies multiple security services in a single cloud-delivered platform to secure internet access and control cloud app usage from your network, branch offices, and roaming users. Cisco Umbrella integrates secure web gateway, cloud-delivered firewall, DNS-layer security, and cloud access security broker (CASB) functionality for effective protection anywhere users go. Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the internet and delivers deep inspection and control to support compliance and block threats. This implies management of personal data of EUIPO staff in order to monitor the internet use of the Office.
Purpose of the processing	The purpose of processing personal data is to prevent users to connect into malicious sites on the internet. To monitor internet use, and in case there is a malicious activity allowing the possibility to identify the PC and take mitigating action on a timely manner.
Data Subjects	All Office staff members, service providers employees, contract agents and trainees that have been assigned an EUIPO workstation.
Description of categories of persons whose data EUIPO processes and list of data categories	<ul style="list-style-type: none">• DNS query data contained in DNS logs (domain, DNS record type, DNS response, IP address, potential user email ID),• Device ID,• IP logs,• HTTP traffic and HTTP header info (e.g., URL), but excluding HTTP body content contained in proxy logs• Data contained in customer files sent to Cisco Umbrella for analysis• Non unique IP addresses In addition, for administrators connecting to Umbrella the following data is also managed: <ul style="list-style-type: none">• Name, surname• Usernames• Email addresses



Retention period	<p>CISCO Umbrella retains data for 2 years or less and in the following way:</p> <p>Report Retention: The reporting of information begins as soon as the application starts sending traffic to Umbrella. The following reports are available for one calendar year:</p> <ul style="list-style-type: none">-Total Requests-Top Destinations-Top Categories-Top Identities <p>Activity Volume is retained for one calendar year.</p> <p>The following reports are limited to a 30-day search window:</p> <ul style="list-style-type: none">-Top Destinations-Total Requests-Security Activity-Activity Search <p>Note: Umbrella does not retain Security Activity or Activity Search data for more than 30 days.</p> <p>Admin Audit log Retention: The Admin Audit log retains data for one year. Data can be access data in three-month increments. For more information, see the Admin Audit Log Report.</p> <p>Cisco Umbrella Privacy Data Sheet: https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/umbrella-privacy-data-sheet.pdf</p>
Recipients of the data	<p>In principle, nobody except the software itself has access to the data. The data sent to the cloud is encrypted. Only members of the IT Security team consisting of internal staff members of DTD will be able to access the information stored in the cloud upon authentication and system admins from DTD external provider.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>Yes</p> <p>By default, Usage and Event Data is then sent to Amazon Web Services (AWS) data centers in AWS East and West regions of the United States, Frankfurt, and Ireland for additional processing, statistical analysis, and storage. This is necessary for the delivery of Cisco Umbrella services, as big data analytics requires the examination of worldwide data in real time. Data sent outside Europe is sent under Standard Contractual Clauses and/or to USA under Privacy Shield framework. More information about Cisco Umbrella in the Privacy Data Sheet: https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/umbrella-privacy-data-sheet.pdf More information about Cisco and Sub-processors Standard Contractual Clauses: https://www.cisco.com/c/en/us/about/legal/supplier-portal.html</p>



General Description of security measures	Information sent to Cisco is encrypted. Raw DNS query data (domain, DNS record type, DNS response, IP address) and Device ID: AES 128 encryption in transit. Logs are not encrypted at rest, but encryption at rest is a roadmap item for the business; -Administrator personal data: Backups are encrypted with GPG; -Active Directory identity and Device ID: Encryption in transit over TLS 1.2 (full Cipher list available upon request) No encryption at rest; -HTTP Traffic (if using package with the selective web proxy, full proxy, or block page bypass capabilities) and HTTP Header info (e.g. URL) but excluding HTTP body content: Encryption in transit. Logs are not encrypted at rest, but encryption at rest is a roadmap item for the business; -Data contained in customer files sent to Cisco Umbrella for analysis (if using package with the selective web proxy, full proxy, or block page bypass capabilities): Encryption in transit.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/e3391160-08a5-4bfd-8088-af55956534a7
EDPS Prior consultation	NO



Reference number	DPR-2020-019
Name of the processing operation	Pan-European Seal Exchange Programme
Last Updated:	21/05/2020
Controller Organizational entity	Academy
Controller contact details	Ms. Patricia Garcia-Escudero Marquez, Director of the Academy at the EUIPO EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Academy@euipo.europa.eu
Joint Controller organizational entity	Academy
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The processing of the personal data is carried out by the Director of the EUIPO Academy, acting as EUIPO data controller.</p> <p>Personal data are processed directly by the Pan-European Seal team of the EUIPO Academy.</p> <p>Personal data are intended to be transferred to the EPO, which is an international organisation established by its own international treaty, the European Patent Convention, signed by 38 member states with its organisational autonomy. The EPO is not a body of the EU or bound by EU law and is legally autonomous for its mission, applying its own legal framework.</p> <p>Personal data will be kept only for the time necessary to achieve the purpose for which they will be processed. The data will be only retained for a maximum period of 1 year from the day of delivery of the list of candidates to the EPO.</p> <p>The processing is automated since the data of the candidates are received via e-mail and included in an excel sheet that is sent to the EPO also by e-mail.</p> <p>The EUIPO shares with the EPO the list of candidates who have submitted an application under the Pan-European Seal Exchange Programme, in order to allow the EPO to identify and only consider for selection those candidates that have been previously confirmed by the EUIPO as Pan-European Seal trainees.</p>
Purpose of the processing	The purpose of the processing of personal data is to allow the participation of Pan-European Seal trainees of the EUIPO in the selection process taking place under the Pan-European Seal Exchange Programme with the EPO.
Data Subjects	EUIPO's Pan-European Seal trainees that apply for a traineeship position at the EPO.
Description of categories of persons whose data EUIPO processes and list of data categories	We process the following data on every person to whom applies for the PES programme Exchange Program: <ul style="list-style-type: none">• Name• Surname• E-mail address• EUIPO Department assigned to the trainee
Retention period	Personal data will be kept only for the time necessary to achieve the purpose for which they will be processed. The data will be only retained for a maximum period of 1 year from the day of delivery of the list of candidates to the EPO.
Recipients of the data	<ol style="list-style-type: none">1. For the EUIPO, the staff integrating the Pan-European Seal team of the Academy and the staff of the Traineeships service of the Human Resources Department.2. For the EPO, the staff of the European and International Co-operation and Human Resources Department.



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>a list of EUIPO candidates is sent to the EPO by e-mail.</p> <p>The corresponding fiche on international transfer of personal data in the context of the PES Exchange Programme can be found on this link: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/6ee2a228-1231-4c16-8e4f-00404acf61d4</p>
General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>All personal data related to the Pan-European Seal Exchange Programme procedures are stored in secure IT applications (e.g. ShareDox) according to the security standards of the Office as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients.</p> <p>The database is password protected under single sign-on system and automatically connected to the user ID. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Processing of personal data in the context of the Pan-European Seal Exchange Programme: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/793ade62-a1df-4216-8939-caf09ca6b6c5</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-020
Name of the processing operation	Processing of personal data in the context of EUIPO staff accessing the content on the PressReader platform through the EUIPO Knowledge Hub and the PressReader's App
Last Updated:	27/05/2020
Controller Organizational entity	Academy
Controller contact details	Ms. Patricia Garcia-Escudero Marquez Director of the Academy at the EUIPO EUIPO, Avenida de Europa 4, 03008 Alicante, Spain Academy@euipo.europa.eu
Name and contact details of processor	PressReader International Limited 2nd Floor The Boat House Bishop Street, Dublin 8 D08 H01F Ireland
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>The EUIPO staff may consult PressReader on-line through the Knowledge Hub using the EUIPO WiFi, or offline during 3 days, through the PressReader App.</p> <p>For that, PressReader will process the following personal data:</p> <ul style="list-style-type: none">• Device's name.• Mobile device IDs.• Location data. <p>The PressReader App does not require location services in order to authenticate. GPS authentication is not used at EUIPO, thus it is not necessary for users to enable location services, so EUIPO staff are recommended to configure the App settings in order to disable the access to their location information.</p> <p>There is not special category of data processed (no sensitive information).</p> <p>Since the processing operation is done through an on-line platform and an App, the processing can be considered automated.</p>
Purpose of the processing	<p>The processing of personal data of EUIPO staff by PressReader, aims to allow them consulting the content of PressReader on-line via the Knowledge Hub or through their mobile devices using the PressReader's application with the EUIPO WiFi. When outside the EUIPO premises or out of the EUIPO WiFi reach (EUIPO red), the EUIPO staff may consult offline the PressReader's content downloaded in their mobile devices during a period of three days.</p> <p>The processing is based on Article 5.1 (a) of the Regulation (EU) 2018/1725 (a task attributed to EUIPO by the EU legislation).</p> <p>The personal data are collected and processed in accordance with the following legal instruments: Staff Regulations of Officials of the European Union and Decision N° ADM-17-66 on the Internal Structure of the Office.</p>
Data Subjects	EUIPO staff



Description of categories of persons whose data EUIPO processes and list of data categories	<p>Category of persons: EUIPO staff using PressReader</p> <p>The following data categories can be found:</p> <ul style="list-style-type: none">• Device's name.• Mobile device IDs.• Location data. <p>The PressReader App does not require location services in order to authenticate. GPS authentication is not used at EUIPO, thus it is not necessary for users to enable location services, so EUIPO staff are recommended to configure the App settings in order to disable the access to their location information.</p>
Retention period	<p>EUIPO staff's personal data will be kept only for the time necessary to achieve the purpose(s) for which it will be processed.</p> <p>The data will be retained for as long as information deletion is requested (see the PressReader Privacy Policy '11. You're in control of your Personal Information').</p> <p>In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.</p>
Recipients of the data	<p>Within the EUIPO, the Academy staff in charge of the Knowledge Hub.</p> <p>Outside the EUIPO:</p> <ul style="list-style-type: none">• PressReader staff;• Microsoft in Canada staff.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	YES
If so, to which ones and with which safeguards?	<p>PressReader transfers the data to Microsoft in Canada, for the storage of the data in their servers and cloud services(Microsoft Azure Cloud & MS SQL) storing your personal data. Such processing involves sharing information with a third party outside of the EEA.</p> <p>The transfer of your personal data is secured by Microsoft, acting as Press Reader's sub-processor, which has several security certifications (including ISO/IEC 27001:2013 Information Security Management Standards, or ISO/IEC 27017:2015 Information technology — Security techniques for cloud services).</p> <p>The transfer is based on the following derogation to Regulation (EU) No 2018/1725:</p> <ul style="list-style-type: none">• Art. 50. 1 (b): transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.
General Description of security measures	<p>PressReader implements the following measures to protect the information they manage:</p> <ul style="list-style-type: none">• A physical backup in secured data warehouse is in place to avoid accidental or unlawful destruction or loss of the Offices' personal data.• To avoid unauthorised access, use, modification or disclosure of personal data, multiple versioning and digital signatures are required.• Internal systems are in place to ensure the availability of the information.• All tools are internally build and external tools are properly vetted to ensure the integrity of the information.• All PCI certification measures are complied with to ensure the confidentiality of the information.• Computers used to access the personal data of the Office are subject to tight active directory controls.



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	EUIPO staff accessing the content on the PressReader platform through the EUIPO Knowledge Hub and Pressreader's App: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/2f0e1c87-d09d-4a70-b5c3-fabfed206a75
EDPS Prior consultation	NO



Reference number	DPR-2020-021
Name of the processing operation	Covid 19 - Plan of return to the Office
Last Updated:	29/05/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department - EUIPO hrddpc@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>On 14 March 2020, Spain declared the state of alarm because of the Covid-19 outbreak and the sanitary crisis triggered by the coronavirus pandemic. As a consequence thereof, on 16 March 2020, the Office moved to full teleworking status and its campus was emptied, except for a very small number of staff members. In view of the evolution of the pandemic of the Covid-19, the Office has prepared a plan for a gradual safety return of staff to the campus in 2 phases, reducing as much as possible the chances of contagion of Covid-19.</p> <p>A limited number of staff (including Statutory Staff Members, SNEs and Trainees) will be invited to come back to the Office premises during the first phase. It includes staff who must be present on the campus because of the nature of their tasks, as well as staff volunteering to return to the campus. On the first phase of return to the Office premises, all internal staff will be medically tested by the Medical Service before coming back to the Office, as a preventive measure.</p> <p>The departments will propose a short list of staff based on the needs of the service. This short list will be included in the list of volunteers.</p> <p>The list of volunteers prepared by each Department will be shared with HRD secretariat who will merge it in one list and forward to the Medical Service which, in turn, will clear the list to remove possible, probable or confirmed active cases (and close contacts with such cases), as well cases with previous relevant health conditions. If, during the test phase, the Medical Service considers that one person is not "apt" for returning to the Office, it will inform HRD.</p> <p>HRD secretariat subsequently sends the final list to IBD for organizing the office's spaces and a department list of staff to each department.</p> <p>HRD secretariat will share the list of staff to be invited for medical tests with IBD to schedule the timetable for the tests and organize the access of staff to the buildings in coordination with the Medical Service.</p> <p>The result of the test will be communicated by the Medical Service to the staff member concerned and may be shared with the Spanish health authorities upon request.</p> <p>The final list of "apt" staff will be shared by HRD with IBD for the purpose of:</p> <ul style="list-style-type: none">• access management in order to organize the access of the people authorized to return to the Office premises;• space management in order to adjust the areas of the buildings assigned to the different departments and ensure social distancing;• maintenance management in order to ensure the cleaning and maintenance of the occupied Office spaces;• Internal mail distribution.



Purpose of the processing	<p>The processing of data is necessary to coordinate the measures in place for a safety return of staff to the Office 's premises.</p> <p>The processing of data is done in compliance with the Staff Regulations (SR) and Conditions of Employment of Other Agents (CEOS), according to which statutory staff in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties.</p>
Data Subjects	Statutory staff members (officials, temporary agents and contract agents) , seconded national experts (SNE 's) and trainees.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following personal data are collected and processed by different internal stakeholders :</p> <p>Office 's departments:</p> <ul style="list-style-type: none">• list of staff set up by each department, including surname/ forename, department of assignment, place of employment and office. <p>HRD secretariat:</p> <ul style="list-style-type: none">• list of staff received from each department to be merged in one list and sent to the Medical Service;• list of staff invited for medical tests;• final list of staff who will return to the Office premises. <p>Medical Service:</p> <ul style="list-style-type: none">• list of staff eligible to return to the Office premises in phase 1;• list of staff to be invited for medical tests;• results of the medical tests (Covid-19), on a case by case ;• symptoms and list of close contacts with the data subject after appearance of the first symptoms;• list of staff considered apt to come back to the Office premises. <p>IBD will process:</p> <ul style="list-style-type: none">• Name, surname and email of the staff members who will be invited to do the medical tests;• Name, surname and office location of the staff members authorized to return to the Office premises.
Retention period	<p>Personal data are kept only for the time necessary to fulfil the purpose of collection or further processing, namely:</p> <ul style="list-style-type: none">• Personal data will be kept by the different Departments (based on the data accessible to each of them) in confidential/restricted Sharedox folders for the duration of the COVID-19 crisis and deleted afterwards;• The list of volunteers should be deleted by each department after confirmation of the final list of staff authorised to return to the Office premises;• The list of staff members who are invited to do the medical tests, which is processed by IBD for the purpose of organization of the access to the Office premises, will be deleted in 1 day after the end of the period of medical testing;• Health data will be kept by the Medical Service in the Medical file of the staff member concerned for 30 years in accordance with the retention period for such files . <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>Medical Service: only the doctors and the nurse have access to data concerning health and the medical file.</p> <p>Lists of volunteers and staff authorised to return to the Office premises will be accessed by authorised staff of:</p> <ul style="list-style-type: none">• HRD (all lists as described in section 2 above);• IBD (list of staff invited for medical tests, list of staff authorized to return to the Office premises and their own lists);• Other departments (their own lists). <p>In addition, only certain administrative and financial data related to health may be disclosed on a temporary basis to the Director of HRD, the Head of Service of Entitlements and Staff Welfare Service, the Social Worker, the Appointing Authority (AA), the Authority Authorized to Conclude Contracts (AACC), the Legal Service and the Court of Justice in case of complaints.</p> <p>Access to aggregated data only without names will be granted to:</p> <ul style="list-style-type: none">• ED, ED Secretariat and assistants;• Members of Advisory Committee (MAC); <p>Your name and other justified information may be shared with the Spanish health authorities if so required in line with public health reasons and national requirements.</p> <p>The data are not used for any other purposes nor disclosed to any other recipient other than the ones mentioned in the paragraphs above.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Access to EUIPO information systems made by registered users follows an identification, authentication and authorization process. Mechanisms of access tracking and monitoring of use of systems are established. Authorised users have a unique and personal identifier that is to enter the system through the corresponding password. The use of user IDs is strictly personal and not transferable. Replacing users is strictly prohibited.</p> <p>Servers are physically protected at the data Processing Centre, Network security is configured to prevent external threats from accessing the servers. The records are held securely so as to safeguard the confidentiality of the data therein.</p> <p>The Information Security Policy of the EUIPO is based on the ISO 27001 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy Statement - COVID-19 - Plan of return to the Office :</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/a4a5ecfc-c110-4b89-9ba7-f0eef8c984c7</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-023
Name of the processing operation	Provision of catering services during the process of return to the EUIPO´ premises
Last Updated:	15/09/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euiipo.europa.eu
Name and contact details of processor	Internal processors: authorised staff of Internal catering team in IBD External processors: authorized staff of Pomilio Blumm (events management provide) and EUIPO internal hospitality team and the external catering team (IDOM Consulting).
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euiipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	During Phase 2 of the process of return to the EUIPO´ premises a seat booking system will be launched through which EUIPO staff and resources will be able to reserve a seat for lunch at the Winter Garden or any of the adjoining terraces. The booking system will enable users to select a concrete time slot and receive a QR code as confirmation for their reservation. Personal data will be collected in the booking system in order to make possible the process of reservation of seats.
Purpose of the processing	The purpose of the processing operation is to ensure the health and safety of EUIPO staff and resources during Phase 2 of the Return Plan.
Data Subjects	EUIPO Staff members and external resources who book a seat in the Canteen through the booking system.
Description of categories of persons whose data EUIPO processes and list of data categories	The only personal data that will be processed is: name, surname, email address.
Retention period	The data will be retained for a maximum period of 2 months.
Recipients of the data	The data will only be shared with people necessary for the implementation of the purpose of the processing operation on a need to know basis. Access to the data will be given only to the events management provider Pomilio Blumm which manages the reservation page and authorized staff of both EUIPO internal hospitality team and the external catering team (authorised staff of IDOM). The data is not used for any other purposes nor disclosed to any other recipient.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	NO
If so, to which ones and with which safeguards?	Data is transmitted to the secure servers of the data storage provider of Pomilio- DigitalOcean. The data storage provider is ISO 27001 certified and applies all physical and IT security measures in order to protect the data.



General Description of security measures	<p>The personal data stored in the Metis tool is located in Frankfurt, Germany. The access to the tool is protected with passwords. The data storage is subcontracted to a provider named DigitalOcean. Systems are monitored, and information is backed up regularly to ensure that, in case of destruction or loss, data can be restored. Backups of the database and the software are performed weekly. Information is backed up regularly, to ensure recovery in the event of a disaster. Datacentre service provider has 24/7/365 monitoring of their systems, and a status page to verify if there is degraded performance or unavailability. All servers are protected by UPS to ensure continuity in the event of a power failure. There are several security measures applied in order to ensure the integrity of the information. Mainly, there are restricted access controls and centralised logging and monitoring to detect any potentially malicious activity. The database is encrypted using a symmetric key algorithm. Communications are encrypted using SSL3. There are several physical security measures applied in order to ensure that the servers that store personal data are protected: 24/7 Physical security guard services; Physical entry restrictions to the property and the facility; Physical entry restrictions to the co-located data centre within the facility; Biometric readers with two-factor authentication; Secure loading zones for delivery of equipment; Full CCTV coverage externally and internally. Data centre service provider's Security team utilises monitoring and analytics capabilities to identify potentially malicious activity within their infrastructure. User and system behaviours are monitored for suspicious activity, and investigations are performed following an incident reporting and response procedures. The event management provider has established a Personal data breach management procedure (please, consult the link at the end of this record). Data storage provider of Pomilio (DigitalOcean) is: ISO22301:2012, ISO/IEC27001:2005, and ISO9001:2008 certified. For more detail regarding the security measures implemented by the event management provider, please, consult the link provided in the last section of this record.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/d23fdf1e-5bf5-4c1f-81d3-1c015efac251
EDPS Prior consultation	NO



Reference number	DPR-2020-024
Name of the processing operation	OD Appeals Notifier
Last Updated:	23/06/2020
Controller Organizational entity	Operations
Controller contact details	Karin KUHL Director Operations Department Tel: +34 965 13 9721 - Mobile:+34 620 851 058 Karin.KUHL@euipo.europa.eu
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>This processing operation consists of compiling data and sending an automatic email with the aim of informing OD examiners of whether a decision of theirs has been appealed and what the final outcome of the appeal has been. The initiative was launched after an ISO 9001 opportunity for improvement was identified in 2018.</p> <p>The data necessary for this automatic notification is already available in BoAST, IP Tool and Allegro.</p> <p>The first version of the OD Appeal notifier will send out weekly automatic emails to inform examiners (rapporteur and co-signers) of the outcome of the Appeal once it reaches the status "Closed as final".</p> <p>The second version of the OD Appeal notifier would also include a weekly email to rapporteurs and co-signers indicating when one of their recently notified decisions has been appealed.</p> <p>The notification is done via automated Outlook emails and is based on data available in BoAST, IP Tool and Allegro, extracted via a Business Objects report.</p>
Purpose of the processing	<p>The purpose of this activity is:</p> <p>a) To avoid the manual checks and follow-up that many examiners perform in order to learn if a decision of theirs has been appealed and what the final outcome is.</p> <p>b) To increase awareness and knowledge about the next instance that could prevent future complaints or even reduce the gap between OD practice and the BoA criteria.</p> <p>At no stage will the data extracted for the automatic notification will be used for any other purpose, and will never be considered in the framework of the appraisal exercise.</p>
Data Subjects	All OD examiners involved in decision taking on absolute and relative grounds, as rapporteurs or as co-signers.
Description of categories of persons whose data EUIPO processes and list of data categories	<p>All OD examiners involved in decision taking on absolute and relative grounds, as rapporteurs or as co-signers.</p> <p>The Business Objects extract contains the following identifiers:</p> <ul style="list-style-type: none">• Login, name, email and department of the rapporteur for all first instance decisions, and of the first and second co-signer (in case of relative grounds decisions only), extracted from Allegro•• Number and nickname of the appeal, appeal summary and appeal output (extracted from BoAST)•• Number of EUTM/RCD Invalidation dossier (extracted from IP Tool)•• ShareDox links to the first instance decision, and to the appeal decision whenever it becomes available for the second notification (extracted from IP Tool)
Retention period	Six months for the extracts and the back-up copies.
Recipients of the data	<p>Access to the excel sheets with the compiled data is open to the QPROs from the OD Central team in charge of the processing operation.</p> <p>Examiners have access only to their individual notifications in the form of an email sent to them from a generic Outlook mailbox.</p>



Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	The standard security measures of the EUIPO Information Systems are applied: <ul style="list-style-type: none">- EUIPO username and password required in order to access EUIPO network and systems.- Authentication and authorization based on roles.- Authentication and authorization at server level, no anonymous access allowed.- Server is physically protected at the Data Processing Centre.- Logical security hardening of the servers.- Network security configured to prevent external threats from accessing the mail servers.
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Specific Privacy Statement OD Appeals Notifier: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/036e2a35-520d-4cbc-bca3-b177767b79e4
EDPS Prior consultation	NO



Reference number	DPR-2020-025
Name of the processing operation	Processing of personal data by Infrastructures and Buildings Department in the Office 365 applications SharePoint and Power Apps
Last Updated:	19/06/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal processors: Authorised staff members of Infrastructures and Buildings Department responsible for the maintenance of registers (risk register, action logs, etc.) Digital Transformation Department (DTD) staff in charge of IT Operations, External processors: External service provider 'PREVING Consultores S.L.U.' (https://www.preving.com/) and IDOM Consulting (https://www.idom.com) for the maintenance of registers (risk register, action logs, etc.). External service provider of DTD- IECISA-ALTIA for the purposes of managing EUIPO IT infrastructure and maintenance tasks.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>As part of operational activities of the Office, Infrastructures and Buildings Department (IBD) uses Office 365 applications SharePoint and Power Apps to create and maintain several tools through which activities/tasks are registered and actions are followed up in the department. Example of such tools are 'Set Up and Collect of meeting rooms' and 'IBD Actions Management Tool' with its 5 modules:</p> <ul style="list-style-type: none">• Action logs;• Register of Action Plans;• Risks register;• Data Protection actions register;• Register of Lessons Learnt <p>These tools normally include the information of a task/action and the persons involved in this task (responsible and affected users) and therefore require the storage of their personal data.</p> <p>IBD has chosen to use SharePoint and Power App instead of MS Access/Excel for the maintenance of its registers and follow-up on activities on the basis of the following reasons:</p> <ul style="list-style-type: none">- SharePoint and Power App allow simultaneous updates by several users ;- The use of Excel as a tool to manage an Action Log has already been subject of an external audit's finding concerning traceability of the changes;- Excel does not allow for the creation of a user-friendly interface;- Excel has many limitations in terms of formatting (example: you cannot put multiple hyperlinks in the same cell, width / height of lines and columns limited, it cannot be handled well if there are many fields , it does not adapt to the dynamics of the action log that assumes that for an entry several follow-up actions are required, etc.)- Access is less intuitive when designing the structure of the Action Log- Access does not allow reporting in Power BI;
Purpose of the processing	The purpose of the processing operation is the elaboration and maintenance of registers of activities and follow up on open actions in IBD.



Data Subjects	Persons (responsible and affected users) involved in the tasks/actions followed up through the registers maintained by IBD
Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following data can be processed in the tools maintained by IBD through the use of SharePoint and Power Apps:</p> <ul style="list-style-type: none">• name and surname;• organisational assignment (department, area and/or service);• link to the activity (responsible, affected user, or similar).• Request number, if associated with a ticketing system, such as MyServiceDesk• Additional personal data, such as the email or location, may be collected, depending on the nature of the register of activity. <p>The exact data collected depends on the nature of the register.</p>
Retention period	<p>Information is kept for the period that the activity/action in the registers is being completed. Once the activity is complete, information is kept for up to three years (the standard ISO audit cycle), as evidence for audit purposes.</p> <p>Further to this, certain information not directly identifying an individual may be kept in the register for records and statistics management purposes, such as the location, PC number, or similar.</p>
Recipients of the data	<p>Personal data will be accessible only to staff and external resources of IBD responsible for the maintenance of the registers and Digital Transformation Department (DTD) staff in charge of IT Operations, supported by the external service provider IECISA-ALTIA.</p> <p>In principle the majority of the service operations are automated in order to reduce the need for human access. Microsoft engineers and support staff do not have access to customer data by default, and are only granted access in case it is required for maintenance purposes. That said, information may be stored in the US. In addition, information may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.</p> <p>The information will only be shared with people necessary for the correct functioning of the system, on a need to know basis. The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	YES
Are there any transfers of personal data to third countries or international organisations?	YES



If so, to which ones and with which safeguards?	<p>Information will be stored in Microsoft Datacenters, located in the "European Region": Netherlands, Ireland, Austria, Finland and France. Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. For Office 365, information may be stored in the US. In addition, information may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out. Regarding MS Teams, personal data is stored in the EU according to the application configuration implemented by EUIPO, however it may be made available to subcontractors in other countries, depending on the requirements for maintenance, support or operation of online services, and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the data required for the specific maintenance, support or operation procedure being carried out. The following safeguards are implemented. • In all transfers to third countries, Microsoft uses EU Standard contract clauses for the transfer with its subprocessors. • Microsoft requires sub processors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardise and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft.</p>
General Description of security measures	<p>The use of IBD of the Office 365 applications SharePoint and Power apps answers to the security policies established by the Digital Transformation Department.</p> <p>IBD has implemented the following security measures when configuring the applications:</p> <ul style="list-style-type: none">- No access to Power BI reports is authorised outside the EUIPO;- All data sources are based on Office 365 internal connectors, no 3rd party data sources;- IBD uses the tools for operating on working documents. The information is regularly uploaded to Sharex;- No features are needed and used outside the official Office 365 E3 license;- The access to the information is given only to authorised staff/external resources of IBD <p>Moreover, Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. As a minimum, data is replicated between two datacentres within the same region, has redundancy controls and implements backups that are encrypted before being transmitted and stored. Datacentres have physical and logical security monitoring measures, such as: • Video surveillance of the perimeter • Seismic and environmental monitoring at the buildings • Monitoring of security threats, such as worms, denial of service attacks, unauthorized access, or any type of unlawful activity. Microsoft has implemented a list of over 700 security controls in Microsoft's systems, servers, and datacentres. This includes security controls against accidental or unlawful destruction, loss, unauthorized access, use, modification or disclosure. These internal controls are audited on a yearly basis, if required, audit information can be provided under a Non-Disclosure Agreement (NDA). Information is encrypted while at rest and in transit. As mentioned above, information may be stored in the US, or may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise. Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out. The following safeguards are implemented: • In all transfers, Microsoft uses EU Standard contract clauses for the transfer. • In the specific case of transfers to the US, Microsoft is certified to the EU-US Privacy Shield Framework. • Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardize and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft. It is also possible to use the logs in the privacy console to verify when information has been shared with Microsoft staff or subprocessors. For more information, please check the Security and Privacy Risk Assessment:</p> <p>http://shredox.prod.oami.eu/share/page/document-details?nodeRef=workspace://SpacesStore/c4b23e3e-061e-40d0-9914-b298bc0a2158</p>



For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/2044c2ab-b29d-4aaa-bc7e-45174a303ee2
EDPS Prior consultation	NO



Reference number	DPR-2020-027
Name of the processing operation	Specific Privacy Statement on pulse survey related to the Staff Satisfaction Survey 2020
Last Updated:	09/07/2020
Controller Organizational entity	Human Resources
Controller contact details	Director of the Human Resources Department hrddpc@euipo.europa.eu
Name and contact details of processor	Independent external provider Willis Towers Watson (WTW)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	<p>Following the feedback given by EUIPO's staff on the Staff Satisfaction Survey 2020 and in the context of continuous organisational improvement, the Office would like to follow-up on the results obtained through a Pulse Survey that will focus on a limited number of selected items that the Office decided to monitor.</p> <p>In particular, the 2020 Pulse survey will focus on the categories Senior Management, My Manager and Supportive Culture but will also seek the feedback from EUIPO staff on the return to the Office following the COVID crises in particular on safety and teleworking.</p> <p>To this aim, the same independent external provider, Willis Towers Watson (WTW) which carried out the Staff Satisfaction Survey 2020 has been requested by EUIPO to conduct a follow-up activity composed of a Pulse Survey of 10 questions.</p> <p>Each staff member (including SNEs) will receive an email sent by WTW including an individual link to access the survey. The participation to the pulse survey is entirely voluntary. For those who do not wish to participate in the survey, they will not suffer any negative consequence and detriment. Only WTW will know the names of those who have declined their participation and such information will not be shared with EUIPO.</p> <p>The conditions of confidentiality are stated in the contract signed between the Office and the provider and will be strictly respected by both EUIPO and WTW.</p> <p>The processing of personal data is not intended to be used for any automated decision making, including profiling.</p>
Purpose of the processing	The purpose of processing data is the continuous organisation improvement focused. For these reasons, Willis Towers Watson (WTW) will process data within the follow-up activity composed of a pulse survey and focus groups.
Data Subjects	Statutory staff: officials, temporary agents and contract agents. Non-statutory staff: Seconded National Experts



Description of categories of persons whose data EUIPO processes and list of data categories	<p>The following information related to all EUIPO statutory staff and SNEs will be sent to the provider by the Office:</p> <ul style="list-style-type: none">• Department, service;• Hierarchical level (Manager, Team Leader, Staff);• Teleworker regular (yes or no);• Working relationship (official, temporary agent, contract agent or SNE);• Length of service (less than 5 years, 5 to 10 years, more than 10 years);• Age (under 35 years of age, 35 to 45 years of age, 46 to 55 years of age, 56 years or older);• Gender;• Function group; Administrator (including Contract Agent function group 4) or Assistant (including Contract Agent function groups 1 to 3); and• Electronic address
Retention period	<p>The personal data will be kept only for the time necessary to achieve the purpose for which they will be processed, consequently will remain in the database until the results have been completely analysed and the final report with the aggregated results has been delivered. Any Personally Identifiable Information (PII) is deleted from WTW systems no later than 6 months after the event closes.</p> <p>The aggregated anonymous data on groups (excluding individual - level data) will be kept until the next survey is carried out, for the purpose of research analysis and reporting, and specifically, to make a comparison (benchmarking).</p> <p>Only the aggregated final report and analysis of results (consolidated data) will be stored in EUIPO document management system (in HRD confidential folder) for 10 years according to the Office's security measures.</p> <p>In the event of a formal appeal, all data held at the time of appeal will be retained until the completion of the appeal process.</p>



Recipients of the data	<p>The "Questionnaire" will be delivered online and will be entirely managed by WTW guarantying that data will be treated with the highest level of confidentiality under the conditions stated in the contract signed with EUIPO. The whole process is automated.</p> <p>The processed and aggregated results of the survey (anonymous) will be accessible to all EUIPO staff in the form of a final report summarising the overall findings and results.</p> <p>An additional and more detailed report (with aggregated anonymous results of the survey) will be accessible to the following persons: Director of the HRD, the Head of Staffing, Development and Recognition Service (HRD), the EUIPO management, the Staff Committee and a limited number of staff of the HRD and members of the Cabinet involved in the pulse survey.</p> <p>The information concerning the detailed results will only be shared with people necessary for the implementation of such measures on a need to know basis. The data are not used for any other purposes nor disclosed to any other recipient.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>Processing of personal data is carried out by the service provider WTW and the Human Resources Department, acting as the data controller for this processing, will monitor and verify the implementation of the required organisational and technical security measures necessary to ensure compliance with the Regulation (EU) 2018/1725.</p> <p>Pre-populated personal data and pseudonymised answers are stored on the WTW servers according to their security measures and processes access being provided only to the core project team and technical support on a "need to know" basis.</p> <p>Only the final report and analysis of results will be stored on EUIPO servers and in ShareDOX (confidential HRD folder), according to the security measures of the EUIPO Information Systems.</p> <p>The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein. The Information Security Policy of the EUIPO is based on the ISO 27011 standard, which is considered the most comprehensive and accredited in its category.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Specific Privacy Statement on pulse survey related to Staff Satisfaction Survey 2020:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/53c8ee20-45db-4a18-ba5c-05ba18bba9f4</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-028
Name of the processing operation	Specific Privacy Statement on the processing of personal data in the procedure of follow up on occupational risk prevention incidents
Last Updated:	22/07/2020
Controller Organizational entity	Infrastructures and Buildings
Controller contact details	Director of Infrastructures and Buildings Department, EUIPO, Avenida de Europa 4, 03008 Alicante, Spain, ibddpc@euipo.europa.eu
Name and contact details of processor	Internal: IBD H&S internal team, External: the H&S service provider 'PREVING Consultores S.L.U.', Facility management service in IBD and any other service provider in IBD which may have to take an action (Catering services provider, audio-visual services provider, etc.)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	Pursuant to Decision No ADM-04-30 of 31 January 2005, the EUIPO complies with the provisions of Spanish Law 31/95 on occupational risk prevention. The purpose of the processing of personal data in this procedure is to comply with the provisions of Law 31/95 on occupational risk prevention and Royal Decree on the Prevention of Occupational Hazards 39/1997 which establish the obligation to maintain a register of occupational risk prevention incidents and follow up on them. The H&S team in IBD maintains the register of occupational risk prevention incidents which is accessed as well by the Facility management service in IBD, responsible to take actions in order to manage the registered incidents.
Purpose of the processing	The purpose of the processing of personal data in this procedure is to comply with the provisions of Law 31/95 on occupational risk prevention and Royal Decree on the Prevention of Occupational Hazards 39/1997 which establish the obligation to maintain a register of occupational risk prevention incidents and follow up on them.
Data Subjects	People involved in the occupational risk incident management (responsible staff of IBD and affected user in some cases).
Description of categories of persons whose data EUIPO processes and list of data categories	The categories/types of personal data processed are the following: <ul style="list-style-type: none">• name and surname;• location;• organisational assignment (department, area and/or service);• link to the activity (responsible, affected user, or similar).• Request number, if associated with a ticketing system, such as MyServiceDesk
Retention period	The data will be only retained for a maximum period of 5 years from the closure of the action.
Recipients of the data	The data will only be shared with people necessary for the implementation of such measures on a need to know basis as follows: IBD H&S internal team, the H&S services provider 'PREVING Consultores S.L.U.', Facility management service in IBD and any other service provider in IBD which may have to take an action (Catering services provider, audio-visual services provider, etc.). The data are not used for any other purposes nor disclosed to any other recipient.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO



General Description of security measures	<p>We implement appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.</p> <p>All personal data related to the process of occupational risk prevention is stored in secure electronic folder according to the security standards of the Office accessible only to the authorised recipients. Appropriate levels of access are granted individually only to the above recipients. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.</p> <p>The database is password protected under single sign-on system and automatically connected to the user ID.</p> <p>All persons dealing with personal data in the context of this procedure shall sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement: http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/03ed358d-fb90-4e70-9897-f2f45b8edeadead</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-029
Name of the processing operation	Manage of personal data in the context of eFiling applications
Last Updated:	28/07/2020
Controller Organizational entity	Digital Transformation
Controller contact details	For internal users: UserFeedback@euipo.europa.eu For external users: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	IECISA ALTIA (DTD external service provider)
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	eFilings are the web user interface to enter the information regarding registrations of trademarks and designs, amendments, international registrations, cancelations, oppositions, and invalidities, and recordals.
Purpose of the processing	The collection, storage and processing of data shall serve the purposes of: (a) administering the applications and/or registrations (EUTM/RCD) as described in the EUTMR and CDIR Regulations, and in acts adopted pursuant to them; (b) accessing the information necessary for conducting the relevant proceedings (examination, opposition, cancellation, RCD invalidity, recordals, appeals, PUB and MPS) more easily and efficiently; (c) communicating with the applicants and other parties to the proceedings (ex parte & inter partes); (d) producing reports and statistics enabling the Office to optimise its operations and improve the functioning of the system (as foreseen in Article 6(1) of Decision No EX-14-3 of The President of OHIM and Article 112(2) EUTMR).
Data Subjects	Applicants and representatives in trade marks and designs procedures.



Description of categories of persons whose data EUIPO processes and list of data categories

Together with all the data essential to the core tasks of the office, the eFiling applications contains personal data of the owners and representatives as follows:

Representative:



Retention period	<p>Two periods: 1. Indefinite (for reasons of legal certainty), as foreseen by Article 111(9) EUTMR and Article 7(1) of the Decision No EX-14-3 of the President of the OHIM.</p> <p>2. Upon request of a party concerned and as regards the data referred in Article 112(5), the retention period is of 18 months from the expiry of the EU trade mark or the closure of the relevant inter partes procedure.</p>
Recipients of the data	<p>All EUIPO's staff has view access to the IP Tool. Majority of IP examiners from OD and limited number of BoA examiners have edit rights to the trade mark and designs dossiers. A limited number of OD examiners (the ones with "owners and representatives" profile) have edit rights to the PER database which feeds the "Persons" section of the dossiers. A limited number of Finance Department examiners (the ones in charge of fees management) have access to financial data in the CPS database. A limited number of Customer Department examiners (the one in charge of the publications in the bulletins) have edit rights to the PUB database. The parties to the procedures of the EUIPO and any third parties (the data is considered to be of public interest) have access through eSearch to the information stored in the IP Tool.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>The security measures include: 1. Role-based access control to the systems and network 2. Logical security hardening of systems, equipment and network 3. Physical protection via secure Data Centre 4. Security measures are periodically reviewed by external auditors (ISO 27001 and SOC 2) The management of access and right is done at ADM level. Examiners need to authenticate against ADM to enter the application. Moreover each examiner is assigned some ADM profiles and each profile is given some rights in the application. Each user is provided a username and password which gives access to certain features (in order to access the EUIPO systems and databases). The basic permissions in IP Tool allow seeing the details but additional permissions are needed to update the data and/or link/unlink owners/representatives to dossiers. The access to the database is restricted to some DTD staff (internal and external). Confidentiality and data protection clauses are signed-off by the service provider. All the standard security measures available for EUIPO's databases. The Office's server has been certified by an international certifying authority (Verisign Inc.), which guarantees that users have in fact connected to the Office. All information transmitted via the internet is encrypted using SSL protocol.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy Statement: https://euiipo.europa.eu/ohimportal/en/data-protection
EDPS Prior consultation	NO



Reference number	DPR-2020-030
Name of the processing operation	Management of log files related to GI View
Last Updated:	30/07/2020
Controller Organizational entity	ICLAD
Controller contact details	ICLAD Director Email address: DPOexternalusers@euipo.europa.eu
Name and contact details of processor	Internal processor: staff of the Digital Transformation Department in charge of IT Operations. External processor: service provider IECISA - ALTIA for IT operations, for the purposes of managing EUIPO IT infrastructure and maintenance tasks.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	In the first release of the tool, personal data related to GI View is collected only to ensure the correct functioning of the website, and is then recorded in the system logs.
Purpose of the processing	Log files related to GI View are used to trace events in the information system and to help with its debugging and repair. They are part of the system and are essential tools to provide security and efficient support when the information system does not work correctly. Log files are processed in order to investigate and eliminate security incidents. Log files are also processed for statistical purposes or to resolve users' problems when visiting the website.
Data Subjects	Users visiting the GI View website
Description of categories of persons whose data EUIPO processes and list of data categories	The servers automatically collect personal data required for the proper functioning of the website. This data is then recorded in log files with information sent by the browser whenever a user visits the website. Log files are created to record elements that trace any operation or event on the system. These elements may include: <ul style="list-style-type: none">• logical address (Internet Protocol address);• timestamps for beginning and end of the operation / visit to the website;• browser type;• browser language;• browser screen size. Other, more technical information is also collected in the log files, but this is collected and processed to understand the behaviour of the system and is not considered personal data.
Retention period	Log files are stored automatically and are kept only for the time needed to achieve the purpose(s) for which they are processed. Data is stored for a maximum of 6 months. Log files are not archived. In the event of a complaint, all data held at the time of the complaint will be retained until the completion of the process.
Recipients of the data	Log files are stored automatically and only the IT security team (EUIPO staff members) and system/network administrators (staff of the external service provider for IT operations) have access to them. Log files may be processed or inspected manually when needed (in order to resolve incidents, errors, malware infections, etc.) In case of an investigation, relevant log files may be made available to the competent authority.
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO



Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.</p> <p>All personal data related to the management of log files is stored in secure IT systems according to the Office's security standards. Appropriate levels of access are granted individually only to the IT security team and system/network administrators.</p> <p>EUIPO systems and servers are password protected and require an authorised username and password to access.</p> <p>The information is stored securely so as to safeguard the confidentiality and privacy of the data therein. Data is stored on servers separate from the systems where the data is produced, so as to avoid leaks in case of malware or security incidents.</p> <p>Regardless of stage, everybody dealing with personal data in the management of log files must sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p>Privacy statement on the management of log files related to GI View:</p> <p>http://sharedox.prod.oami.eu/share/page/document-details?nodeRef=workspace%3A//SpacesStore/25754fa5-073b-4f3b-a6cd-4457820ca003</p>
EDPS Prior consultation	NO



Reference number	DPR-2020-032
Name of the processing operation	EU funded project portals (update of DPR-2017-046)
Last Updated:	15/09/2020
Controller Organizational entity	ICLAD
Controller contact details	International Cooperation and Legal Affairs Department d. director Email address: DPOexternalusers@euipo.europa.eu EUIPO Avenida de Europa 4 03008 Alicante, Spain
Name and contact details of processor	Personal data is processed by the EU-Funded Awareness and Communication Officer, EU-funded project management teams, International Cooperation Service, EU-funded team (EUIPO), Communication Service (EUIPO) and the service providers for photos and videos.
Name and contact details of DPO	Ms. Gloria Folguera (+34) 965 13 95 12 DataProtectionOfficer@euipo.europa.eu EUIPO European Union Intellectual Property Office Av. de Europa, 4, 03008 Alicante
Description	The EU-funded project team within the International Cooperation Service is in charge of implementing projects funded by the EU. Each project must provide for visibility and communication of its activities, which includes the setting up of project websites, produce visual promotional products for the purposes of advertising and awareness-rising of the actions carried out by the European Union.
Purpose of the processing	Personal data is processed for the purposes of communication/transparency to provide and make available information on the projects' activities/initiatives/events, etc. The following main activities are included: <ul style="list-style-type: none">• publication of events, including pictures and/or audiovisual items produced within the scope of EU-funded projects;• publication of agendas and conference material;• publication of the studies and reports deemed necessary for each project's framework;• use of social media linked to each project;• sending newsletters based on subscription.
Data Subjects	Natural persons whose name, official contact, photo and/or image and voice in multimedia items may be processed. Moreover natural persons whose email address is processed for sending a newsletter based on subscription.
Description of categories of persons whose data EUIPO processes and list of data categories	The categories/types of personal data processed are as follows: <ul style="list-style-type: none">• personal names and official contacts;• official photos of events;• multimedia items showing the people participating in official events, their image, voices, statements, opinions, etc.;• news in social media, including pictures, and on the web;• email addresses for the purposes of sending newsletters.



Retention period	<p>Personal data will be kept only for the time needed to achieve the purpose for which it is processed. All data related to the projects will be stored for the duration of the project. This is normally 7 years. Information will be shared on the website and in the media and is stored for as long as the European Commission considers it appropriate to achieve the purpose of transparency.</p> <p>After the data subject unsubscribes from the newsletter, his/her email address will be deleted automatically without delay.</p> <p>In the event of a formal appeal, all data held at the time of the appeal will be retained until the completion of the appeal process.</p>
Recipients of the data	<p>Personal data is published on the websites and social media and available to the general public.</p> <p>Information concerning the people shown in multimedia, photos or any other audiovisual item or whose name is displayed in a document produced within the scope of EU-funded projects, and - if the data subject decides to subscribe to the newsletter - his/her email address, will only be shared with those people required to implement such measures on a need-to-know basis. Personal data is not used for any other purposes or disclosed to any other recipient.</p> <p>The projects social media will be managed by the project management teams, in particular by the project Awareness and Communication Officer who will be based in the region/country of the project, the EU-funded Communication Officers in the EUIPO International Cooperation Service and the Communication Service.</p>
Are there any transfers of personal data within EU, subject to Regulation (EU) 2016/679 and Directive 2016/680?	NO
Are there any transfers of personal data to third countries or international organisations?	NO
General Description of security measures	<p>We take appropriate technical and organisational measures to safeguard and protect the personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.</p> <p>All personal data related to the projects' procedures is stored in secure IT applications according to the Office's security standards, as well as in specific electronic folders accessible to authorised recipients only. Appropriate levels of access are granted individually only to the above mentioned recipients.</p> <p>The database is password-protected under a single sign-on system and connected automatically to the user's ID. E-records are held securely to safeguard the confidentiality and privacy of the data therein.</p> <p>Regardless of the stage, everybody dealing with personal data in the context of the projects' procedures, and in particular the Awareness and Communication Officer appointed for each project, must sign a confidentiality declaration.</p>
For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Privacy statement: https://euiipoef.eu/en/privacy-statement
EDPS Prior consultation	NO

