Data Protection Statement on the processing of personal data in the context of the EUIPO's IP Enforcement Portal (IPEP)

Protecting your privacy is of the utmost importance to the European Union Intellectual Property Office ('EUIPO'/'the Office'/'the controller'). The Office is committed to respecting and protecting your personal data and ensuring your rights as a data subject. All the data of a personal nature that identifies you directly or indirectly will be handled fairly, lawfully and with due care.

This processing operation is subject to 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.

The information in this communication is given pursuant to Articles 15 and 16 of Regulation (EU) 2018/1725.

1. What is the nature and purpose of the processing operation?

FOR THE USER MANAGEMENT:

IPEP provides three different modules or tools: the **Exchange Information** module, the **Report detentions** module and the **Report non-EU cases** module. For all three modules, personal data is processed by the EUIPO for the account creation of the different user categories.

In addition to using personal data to create the users' accounts and access credentials in IPEP, the e-mail addresses of the users are used:

- to circulate internal information about IPEP, such as information about new functionalities or updates to the current ones, or to provide new instructions for use;
- for automatically generated notifications from the system to users, for example when a new user account has been created;
- to inform users about other services or products provided by the Observatory within its legal mandate (e.g. knowledge building, awareness events, publication of studies on intellectual property rights (IPR));
- to circulate invitations to the IPEP Forum, which is celebrated every two years;
- to carry out surveys aimed at measuring the performance of the system and/or fine-tuning its applications;
- to be shared with enforcement authorities of the EU Member States, Europol and the European Anti-Fraud Office (OLAF) for enforcement operations carried out by these authorities.

FOR THE DATA ENTERED BY THE DIFFERENT CATEGORIES OF USERS:

- For the **IPEP Exchange Information** module:

  IPEP is a secure online tool that holds data on registered IP rights, contact information, supplementary product information and logistics entered by the rights holders (companies). The purpose of the **IPEP Exchange Information** module is to help enforcement authorities (e.g. police, customs, market surveillance authorities, prosecutors, Europol, OLAF and the Directorate-General for Justice's (DG JUST) Safety Gate/RAPEX team) to better identify counterfeit goods using the IPR, product and contact information entered by the rights holders.

  It allows rights holders to file and manage customs applications for action (AFAs) and to securely exchange information with the registered enforcement authorities in the form of *Suspicious Cases* and *Alerts* functions (which may contain personal data).

  The abovementioned information is introduced by companies or their representatives. Companies (rights holders) are the owners of the information and, therefore, they control the quality of the information that they introduce.

  The EUIPO authenticates users, following an authentication protocol and creates the user account. For each account there is a 'master user', who will authorise the access of other users to his account.

- **IPEP Traders Portal for COPIS** for the electronic filing and management of customs AFAs:

  The **IPEP Exchange Information** module is the EU portal (**IPEP Traders Portal for COPIS**) for rights holders to file AFAs. Rights holders can file AFAs, that contain personal data, electronically through IPEP to the European Commission's central IP database - the Anti-Counterfeit and Anti-Piracy System (COPIS) - as per Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003. The information is transferred to this central database.

  The EUIPO, through the Observatory, only acts as a processor of the data contained in the AFAs on behalf of the controllers of COPIS (i.e. the national customs authorities).

- For the **IPEP Report non-EU cases** module:

  This module features the recording of IP enforcement cases in non-EU countries. The information is used by the European Commission's Directorate-General for Trade (DG Trade) for statistical purposes. Users report, in a structured format, all data relating to cases of IPR infringements affecting EU companies in countries outside the EU and the corresponding enforcement actions of local authorities.

  The purpose of the **IPEP Report non-EU cases** module is:

  - to produce relevant statistical information to assess the level of IPR infringements in third countries;

- to provide the European Commission (DG Trade) with information about concrete IP problems faced by EU companies outside the EU, and to 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 with an overview of infringement business models and trends in enforcement, without having access to specific case details or information indicating which companies uploaded the cases to IPEP;
- for the European Commission (DG Trade) and the EUIPO to exchange information with the EU Delegations in a secure way by storing reports, briefing documents and news in IPEP.

2. What personal data do we process?

The categories of personal data processed are as follows.

- RIGHTS HOLDERS

  Rights holders in possession of the security code assigned by the EUIPO: name, surname, e-mail address and telephone number.

  Rights holders appoint their legal representatives and manage their IPEP accounts. The information they enter may include personal data (i.e. name, surname, company name, address, phone number, e-mail address).

- LEGAL REPRESENTATIVES

  Legal representatives in possession of the security code assigned by the EUIPO: name, surname, e-mail address and telephone number.

  Legal representatives are appointed by the rights holders. They can manage the account, create cases and file AFAs in IPEP on behalf of their rights holders. The information they enter may include personal data (i.e. name, surname, company name, address, phone number, e-mail address).

- CONTACT POINTS

  In the **IPEP Exchange Information** module, contact points are the contacts entered by the rights holders or their legal representatives for the registered enforcement authorities of the Member States. The personal data recorded are: name, surname, address, e-mail address, telephone and fax numbers, countries covered, products covered, languages, whether the contact can answer technical or legal questions, and identify if the contact is the main contact of the company.

  The contact points can reply to Suspicious Cases sent by the authorities.

In the **IPEP Report non-EU cases** module, rights holders can enter the details of contact points, specifically the name, surname and email address of the person within the company in charge of the file, although this information is not mandatory. This personal data can be uploaded by different types of users as defined in the 'IP Enforcement Portal Terms and Conditions', and it is stored and processed when they log in to the database with the appropriate credentials. A contact point can be assigned for specific countries and their access to the information in the **IPEP Report non-EU cases** module can be limited to the countries assigned. Users can search for their own cases and edit the information at any time. However, a user cannot access any information uploaded by other users if they have not been authorised to do so by an administrator or a company master user (i.e. a rights holder or legal representative acting as master user on behalf of the rights holder).

- ASSOCIATIONS

  In the **IPEP Report non-EU cases** module, associations such as helpdesks or EU Delegations can enter the following case information on behalf of the rights holders: name, surname, e-mail address and telephone number.

- ENFORCEMENT AUTHORITIES

  In the **IPEP Exchange Information** module, for the creation of the profiles of authorities not accessing through the Common Communication Network (CCN), the personal data processed are: name, surname, name of the authority, professional e-mail address and the static IP addresses of the relevant enforcement authorities.

  The enforcement authorities can send Suspicious Cases and Alerts.

  In doing so, officers of law enforcement authorities, national IP offices and other institutions and agencies active in the protection of IP can voluntarily share their individual professional contact details with specific rights holders through the tool.

- EUROPEAN COMMISSION (DG TRADE)

  For the **Record of Non-EU cases**, no personal data is utilised in the statistics used by the European Commission (DG Trade).

As stated in the Terms and Conditions, the EUIPO is not responsible for information uploaded to IPEP by the users. Users should take all reasonable steps to ensure that personal data that is inaccurate, incomplete or outdated is not entered in IPEP.

3. Who is responsible for processing the data?

In the **IPEP Exchange Information** module, for the processing of AFA information to and from COPIS, the EUIPO acts as the processor of data entered in IPEP by the rights holders, such as product, IPR and contact information. This information can be included in the AFA information transmitted to the Directorate-General for Taxation and Customs Union (DG TAXUD) and the EU Member States, and can be used in the Alerts and Suspicious Cases exchanged with the enforcement authorities registered in IPEP.

The same applies to the information in the Alerts and Suspicious Cases exchanged entered by enforcement authorities and to the IPR-infringing goods detention data of the Member States that is related to the AFA information and reported in the **IPEP Report Detentions** module.

4. Who has access to your personal data and to whom is it disclosed?

Personal data is disclosed to the following recipients.

FOR THE DATA COLLECTED FOR USER MANAGEMENT:

For the purposes of creating and maintaining the accounts, data is disclosed to the IPEP team, a limited number of the EUIPO's Customer Department staff and the system's administrators on a strict need-to-know basis.

The EUIPO only has access to the users' information needed for account creation, both for rights holders and for enforcement authorities that access IPEP from a secure static IP address (i.e. name, surname, company/authority and e-mail address).

FOR THE DATA ENTERED BY THE DIFFERENT CATEGORIES OF USERS:

- For the **Exchange Information** module:
    - The EUIPO:
        - With regard to the rights holder accounts and the information included therein, the EUIPO's access is limited to the information entered under 'Company Information' and to the 'Product Information' relating to products shared by the rights holder with the EUIPO's IPEP team for the purpose of training the enforcement authorities.
    - Outside the EUIPO:
        - Rights holders' master users and sub-account users, and right holders' authorised legal representatives and contact points have access to data related to their respective companies.
        - Registered enforcement officials with access to IPEP can view the contact points and product information of the rights holders registered in IPEP.

- For the **Report non-EU cases** module:
    - The EUIPO:
        - EUIPO information technology (IT) operators and the system administrator can only use data for the purposes of resolving technical issues or performing technical maintenance.

- The EUIPO's IPEP team can access, in read-only mode, the personal data of companies' contact points for cases that have been uploaded in IPEP.

- Outside the EUIPO:

  - Rights holders, legal representatives and associations (IPR helpdesks): Master users can create, modify and delete their own companies' contact points. Sub-account users can create their own companies' contact points, but are not allowed to modify or delete existing ones.

  - EU Delegations: Neither master users nor sub-account users can create, modify or delete contact points. 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 in which they operate.

  - DG Trade: Neither master users nor sub-account users can create, modify or delete contact points. DG Trade users can access, in read-only mode, the personal data of companies' contact points for cases that have been uploaded in the tool.

5. How do we protect and safeguard your information?

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.

Safeguards are ensured by the EUIPO's general security policy. In the framework of its Information Security Management Policy, the EUIPO is certified to ISO 27001 standards.

All personal data is stored in secure IT applications on the EUIPO's servers 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 abovementioned recipients.

The IPEP 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.

Furthermore, the creation of an account in IPEP is based upon a security code assigned by the EUIPO. Additionally, security is ensured for the exchange of information between IPR holders and enforcers as follows.

- Enforcers' profiles are created in the secure CCN of the European Commission. Communication via the CCN is based on identification, authentication and authorisation under the control of a responsible national authority.

- Enforcement authorities that are not able to connect using the CCN can access via a static IP address. In such cases, profiles are created by the EUIPO system administrators under the control of a single point of contact from the enforcement authority.

- For companies, the system offers two levels of protection: password and PIN-SAFE.

- Rights holders / users do not see the information of the other accounts. They only have access to their own account.

Moreover, in order to ensure the highest level of security in its IT systems, including IPEP, the EUIPO is certified with Service Organisation Control (SOC) 2 standards. The SOC 2 report focuses on a business's non-financial reporting control, based upon the internationally recognised 'trust service principles' of security, availability, processing integrity, confidentiality and privacy. This ensures, in particular, that systems:

- are logically and physically protected from unauthorised access;
- are available for committed or agreed use;
- are complete, accurate, timely and authorised in processing;
- protect information that is designated 'confidential' as committed or agreed;
- collect, use, retain and disclose personal information conforming to the commitments of the entity's privacy notice and with international privacy standards.

SOC 2 certification is a recurrent process, with the EUIPO being subject to a yearly independent audit. Therefore, the EUIPO ensures that the highest standards of security are applied to IPEP.

6. How can you obtain access to information concerning you and, if necessary, rectify it? How can you receive your data? How can you request your personal data be erased, or restrict or object to its processing?

You have the right to access, rectify, erase and receive your personal data, as well as to restrict or object to its processing, as provided in Articles 17-24 of Regulation (EU) 2018/1725.

If you would like to exercise any of these rights, please send a written query explicitly stating your request to the delegated data controller, the Director of the Observatory.

Your request will be answered without undue delay, and in any event within 1 month of receipt of the request. However, according to Article 14(3) of Regulation (EU) 2018/1725, this period may be extended by up to 2 months where necessary, considering the complexity and number of requests. The Office will inform you of any such extension within 1 month of receipt of the request, together with the reasons for the delay.

7. What is the legal basis for processing your data?

Personal data is processed in accordance with Article 5(1)(a) of Regulation (EU) 2018/1725, which states that it is lawful when necessary for the performance of tasks in the public interest attributed by EU legislation.

Regulation (EU) No 386/2012 ([1]) entrusts the EUIPO with tasks related to the enforcement of IPR, including the assembling of public and private stakeholders as an Observatory on infringements.

Through the Observatory, the EUIPO must engage in providing mechanisms that help to improve the online exchange between Member States' authorities working in the field of IPR, providing information relating to the enforcement of such rights, and fostering cooperation with and between those authorities.

For the personal data contained in the AFAs for the further processing of detention data reported by the Member States in COPIS, Implementing Regulation (EU) No 1352/2013 ([2]) provides the relevant legal basis.

8. How long can your data be kept?

Given the purpose of IPEP, the personal data will be stored in the database as long as it is not deleted by the users, or by the system administrators on their behalf. Any information included in AFAs, Alerts and Suspicious Cases that have been exchanged with enforcement authorities cannot be deleted by the user. They will have to be deleted by the system administrators on their behalf.

9. Contact information

Should you have any queries on the processing of your personal data, please address them to the data controller, the Observatory Director at: DPOexternalusers@euipo.europa.eu.

You may also consult the EUIPO data protection officer (DPO) at: DataProtectionOfficer@euipo.europa.eu.

Forms of recourse
If your request has not been responded to adequately by the data controller and/or the DPO, you can lodge a complaint with the European Data Protection Supervisor at: edps@edps.europa.eu.

([1]) Regulation (EU) No 386/2012 of the European Parliament and of the Council of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights, including the assembling of public and private-sector representatives as a European Observatory on Infringements of Intellectual Property Rights Text with EEA relevance.
([2]) Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights