ANNEX I: CONDITIONS OF USE OF THE USER AREA

1) User Area

The User Area is the Office's sole means of electronic communication as defined in Decision No EX-20-9 of the Executive Director of the Office of 3 November 2020 on communication by electronic means.

The User Area can be accessed exclusively through the Office's website (www.euipo.europa.eu).

The User Area enables account holders to:

- 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.

2) Content of the User Area

a) Lists of files

In the User Area the account holder will find a list of all their past (closed) and present files in certain types of proceedings with the Office. This list will be provided with search facilities and will allow the account holder to enter into the detailed information of these files.

The list available in the User Area will only contain files in which the identified account holder is part of the procedure (party, representative, etc.).

b) Notification of decisions, communications and other documents by the Office

The User Area allows the Office to validly notify decisions, communications and other documents electronically.

The User Area is the sole platform through which the Office will issue notifications by electronic means including decisions, communications and other documents. While their User Area account remains active, account holders may not opt out of this means of receiving communications from the Office. So, if the account holder has a User Area account, the Office will notify all decisions, communications and documents electronically

via the User Area, unless this is impossible for technical reasons. Please see Article 4, paragraphs 1 and 2 of Decision No EX-20-9 of the Executive Director.

Account holders have the option of receiving an alert when a decision, communication or other document awaiting service is available in the User Area. The alert may consist of an email, SMS or any of the other technical means provided for that purpose. A similar alert appears as soon as the user logs in to the User Area. The alert has no legal effects. It only serves for information purposes. Please see Article 4, paragraph 3 of Decision No EX-20-9 of the Executive Director.

A decision, communication or other document, however, is deemed to have been notified on the fifth calendar day following the day on which the decision, communication or document was placed by the Office in the account holder's inbox in the User Area. Please see Article 4, paragraph 5 of Decision No EX-20-9 of the Executive Director. Account holders are advised to log in to their User Area at least once a week to consult the decisions, communications or other documents sent to them.

The date of notification of a decision, communication or other document is indicated in the User Area.

If account holders cannot access a decision, communication or other document, they should inform the Office immediately (https://euipo.europa.eu/ohimportal/en/contact-us).

The account holder will have the possibility at any time to view, print or save these notifications.

c) Applications, communications or other documents sent to the Office

The User Area allows the account holder to submit applications, communications or documents electronically.

Applications, communications or other documents sent to the Office are checked automatically to ensure that they are secure. If such checks reveal an anomaly, the documents concerned will be refused.

In the event of a malfunction during the submission of applications, communications or other documents electronically, they must be sent by one of the other accepted means of communication.

Confirmation of receipt stating, inter alia, the date of receipt will be sent to the account holder. The time of receipt of applications, communications or other documents is considered the time the receipt was validated, and is in accordance with the local time in Spain.

Confirmation of receipt is without prejudice to the procedural admissibility of the application, communication or other document.

The account holder can view, print and/or save these applications, communications or other documents at any time.

d) Back-up in case of malfunction

As seen in Article 6, paragraph 2 of Decision No EX-20-9 of the Executive Director, the Office has made two electronic communication back-up alternatives available.

When one of the electronic back-up solutions is used, it is **important to note** that the conditions laid down in Decision No EX-20-9 of the Executive Director **must be complied with**, specifically where the document submitted through the back-up solution is either the **e-filing of an EUTM or RCD application** or the **e-renewal of an EUTM or RCD registration**. For more details, see Article 6, paragraph 3 of Decision No EX-20-9 of the Executive Director.

i. 'Communication back-up' button

Within the Communications section of the User Area the 'Communication back-up' button can be used. However, it can only be used when one of the following two conditions are met:

1. no specific e-operation is available in the User Area, or;
2. a specific e-operation is available in the User Area, but this e-operation is temporarily not accessible due to a technical malfunction.

An electronic receipt of the application, communication or document sent via the 'Communication back-up' e-operation will be provided in the form of a 'sent confirmation' in the 'sent' items of the User Area.

ii. File-sharing solution

The Office will make an electronic back-up alternative available in the form of a file-sharing solution.

Upon request, by contacting the Office's Information Centre (https://euipo.europa.eu/ohimportal/en/contact-us), the Office will provide the user with instructions and access to a secure file-sharing location where the application, communication or document in question can be uploaded. Access to the file-sharing back-up solution will be provided exclusively on request, to a specific account holder, for a restricted period of time, and will require user identification in the form of the User Area login credentials.

This alternative may only be used when all other methods of communication within the User Area fail.

An electronic receipt of the application, communication or document sent via the 'file-sharing solution' e-operation will be provided in the form of a 'sent confirmation' in the 'sent' items of the file-sharing solution.

e) E-operations that can be carried out via the User Area

A series of e-operations (e-filings, e-actions and other e-operations) can be carried out via the User Area. These are accessible after logging into the User Area through the 'Dashboard' or the 'Online Services' sections of the account.

In addition, the User Area also allows users, in certain *inter partes* proceedings, and when both parties are registered users of the User Area, to file joint requests that are validated (signed) electronically by the two parties.

If an account holder uses one of these standard e-operations in the User Area to file a submission, this e-operation will prevail over any subsequent statement or observation made by the account holder through other means on the same day, provided that the Office does not receive a withdrawal of the e-operation on the same day (see Guidelines Part A, Section 1, Means of Communication, Time Limits, Paragraph 3.1.6). **For example**, if an account holder withdraws an EUTM application through the User Area by selecting and submitting the corresponding e-operation, this action will prevail, irrespective of any contrary or additional observation sent by the account holder. Indeed, the account holder will **only** be deemed to have filed a request to withdraw the EUTM application indicated.

f) Management of a personalised alert system

When account holders are logged on, they can create online alerts. There are three types of alert:

- calendar alerts;
- monitoring alerts;
- watch alerts.

Alerts are notified in the User Area and can consist of emails, SMS or any other technical means provided for.

Alerts are merely of an informative nature and are not considered as notifications. If, for any reason, an alert is not sent or contains an error, neither the notification nor the relevant time limits, where applicable, are affected.

g) Access to information related to the account holder's current account with the Office

In the User Area, registered current account holders will also find all the information related to their account: balance of payment, movements, pending debits.

3) Technical requirements

Where the representation of an EUTM or RCD application is provided electronically, the detailed technical requirements for the electronic files of the representation of the trade mark and design are set out in Articles 8 and 9 of Decision No EX-20-9 of the Executive Director.

Information on the detailed technical requirements for attachments to electronic filings and communications can be found online at: https://euipo.europa.eu/ohimportal/en/help-technical-information.

4) The user account

a) Opening user accounts and sub-accounts

A user account must be created online.

During the creation process, the account holder must indicate an email address that will be used to send the password to activate the user account. The account holder must change that password when they first log on to the User Area. Thereafter, it should be changed at least once every 6 months.

Where the creation of a user account is linked to an existing EUIPO ID number with no email address, the user can provide the relevant email address through the 'Contact' form (option 'Provide email').

Account holders may open sub-accounts (or 'subprofiles'), which are dependent on the master account. The purpose of a sub-account is exclusively for the convenience of account holders to assist with case management, and can only be used directly by the registered account holder or by other members of the account holder's organisation who operate under the registered account holder's direct control, responsibility and supervision. Please see Article 3, paragraph 1 of Decision No EX-20-9 of the Executive Director.

b) Proper use of the user account

The account holder is responsible for the proper use of the account and for maintaining the confidentiality of their account, passwords, the administrative email account associated with the user account and, where appropriate, any corresponding sub-accounts. The account holder must not share their credentials for accessing the User Area with anyone. Any process carried out through the User Area using that account holder's credentials will be deemed to have been carried out by the registered account holder, who bears full responsibility for any such use. Please see Article 3, paragraph 2 of Decision No EX-20-9 of the Executive Director.

Proper use of the account and maintenance of confidentiality excludes 'prohibited disclosure'. This means that sharing or disclosing credentials, passwords or administrative email accounts with any third party, that is, any entity or individual outside its organisation, by account holders is strictly prohibited. Equally, any authorisation or consent to use the same, or create sub-accounts for any purposes other than those set out in section (a) above, are also prohibited.

If the Office is informed or suspects that prohibited disclosure has occurred, based on documentary evidence submitted to it, it will take immediate measures to ensure that any illegal acts resulting from this disclosure are discontinued. This would particularly be the case where use of the user account by non-qualified third parties circumvents the requirements concerning professional representation within the meaning of Articles 119 and 120(1) EUTMR or Articles 77 and 78(1) CDR or amounts to a data breach within the meaning of (Article 4(12) of Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) or Article 3(16) 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 (EU Data Protection Regulation).

For this reason, the Office will investigate the relevant facts and, where appropriate, invite the account holder to comment on the evidence and explain its actions. If the investigations lead the Office to reasonably believe that prohibited disclosure occurred, it may apply the following sanctions, depending on the kind and severity of the irregularity concerned:

- temporarily or permanently suspend the relevant user account upon written notice to ensure that the prohibited disclosure comes to an immediate end and is discontinued for the future;
- in the event of a suspected breach of the requirements relating to professional representation, require the account holder to submit authorisation(s) signed by the relevant person(s) pursuant to Article 74(1) EUTMDR and Article 62(1) CDIR -; failure to comply may entail the consequences provided for in Article 74(3) EUTMDR and Article 62(4) CDIR respectively;
- where the prohibited disclosure infringes national law or administrative rules, inform the competent national authorities (including the central industrial property offices of the Member States, the account holder's professional body or law enforcement authorities) about the committed acts; and/or
- in the event of acts amounting to a threatened or committed data breach, initiate proceedings under the General Data Protection Regulation or the EU Data Protection Regulation, or inform the competent data protection supervisory authorities, as the case may be.

c) Deactivating a user account

Account holders may request the deactivation of their user account at any time. The deactivation will be effected as soon as technically possible. Until the definitive deactivation of the user account, all provisions related to the User Area are valid and fully applicable.

A user account that remains unused for a period of 3 years may be deactivated. The user account can be reactivated on request.

d) Use of administrative and contact email addresses

Account holders must inform the Office promptly of any change to the **administrative** email address they provided when opening their User Account. The administrative email address will not be published by the Office, nor made available to third parties, with the exception of administrative cooperation (Article 117 EUTMR and Article 75 CDR.

Account holders may also provide the Office with a **contact** email address that is different from the administrative email address. When an account holder indicates their contact email address, they will have the choice to opt out if they do not want the Office to send them EUIPO and IP-related information by email, such as news on trade marks or designs, or invitations to seminars and workshops.

The purpose of the above information is strictly to inform and update users on EUIPO and IP-related topics and news, including general or specific surveys.

For more information on the use of email addresses and the processing of personal data within the framework of the EUIPO's tasks, as laid down in Regulation (EU) 2017/1001 and Regulation (EC) No 6/2002, see the EUIPO's dedicated data protection page at https://euipo.europa.eu/ohimportal/en/data-protection.

e) Managing the public profile in the user account

The account holder's contact email address, phone and fax numbers will not be made publicly available or searchable via eSearch plus, TMview and DesignView unless they have given their express consent (opt-in) in the User Area options menu.

5) Disclaimers

The Office is not liable for any loss or damage arising from interference, omissions, interruptions, computer viruses, telephone faults or disconnections in the operational functioning of this electronic system brought about by causes beyond the Office's control. These include any delays or blockages in the use of the system caused by faults in, or overloading of, the Office's communication lines or servers, the internet system or other electronic systems, or any damage caused by third parties as a result of unlawful intrusion beyond the Office's control.

The Office is also not liable for any data breaches caused by the intentional or negligent behaviour of the account holder. This would include any failure to use their account properly or maintain the confidentiality of their account, passwords, administrative email account or sub-accounts, in particular when an account holder has knowingly shared their credentials for accessing the User Area with third parties outside of their organisation.

Any action performed via the User Area must comply with the applicable rules. Where, due to a technical malfunction or any other equivalent reason, the User Area allows actions that do not comply with the applicable rules to be performed, these actions may be invalidated by the Office. In such an event, the account holder will be informed accordingly.

6) Encryption and non-repudiation

The Office has advanced and secure systems for guaranteeing the identity of account holders when connected and for certifying the content of messages sent. It also guarantees the authenticity of the server to which account holders are connected, thus preventing the server being supplanted by third parties. The Office's server has been certified by an international certifying authority (Verisign Inc.), which guarantees that account holders have in fact connected to the Office. All information transmitted via the internet is encrypted using SSL protocol.