Privacy Statement on the processing of personal data in relation to the collection of misleading invoices addressed to the users of the IP systems

The protection of your privacy is of the utmost importance to the European Union Intellectual Property Office ('EUIPO' or 'us' or 'the controller'). The Office is committed to respecting and protecting your personal data and ensuring your rights as a data subject. All data of a personal nature, namely data that can identify 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 provided pursuant to Articles 15 and 16 of Regulation (EU) 2018/1725.

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

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 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.

The purposes of the processing operation are to:

- 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 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.

Your personal data is not intended to be used for any automated decision making, including profiling.

2. What personal data do we process?

No special categories of data are processed (sensitive personal data). The data processed is:

- **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.

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.

3. Who is responsible for processing the data?

Processing of the personal data is carried out under the responsibility of the Customer Department director and the International Cooperation and Legal Affairs Department director, acting as the delegated EUIPO data controllers within their respective competence.

This processing activity is ensured by the joint cooperation of the teams led by the Head of the Customer Management Service, the Digital Transformation Department (DTD) director, the Communication Service department and the Service Manager of the external service provider eXTEL Contact Centre, which acts on behalf of the EUIPO as data processor.

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

Personal data is disclosed to the following recipients.

- 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.

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.

Personal data such as name and address of the user reporting a misleading invoice and any other identification data contained in the 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.

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).

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.

5. How do we protect and safeguard your information?

We take appropriate technical and organisational measures in order to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.

All personal data related to the management of user interactions, including reports on misleading invoices and emails received from the user are processed by integrated customer relationship management software.

The Office also uses other systems/databases in which data is stored in a secure environment according to the 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 abovementioned recipients.

The database is password protected under a single sign-on system and automatically connected to the user ID. The e-records are held securely to safeguard the confidentiality and privacy of the data therein.

Everyone who deals with personal data in the context of the management of user interactions, at any stage, signs a confidentiality declaration.

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 that your personal data be erased, or restrict / object to its processing?

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

The right of rectification only applies to inaccurate or incomplete factual data processed within the management of user interactions.

If you would like to exercise any of these rights, please send a written query explicitly specifying your request to the delegated data controllers at the address specified in question 9.

Your request will be answered free of charge and without undue delay, and usually within 1 month of receipt of the request. However, according to article 14(3) of Regulation (EU) 2018/1725, that period may be extended by 2 months where necessary, taking into account the complexity and number of the requests. We 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 on the basis of Article 5(1)(a) of Regulation (EU) 2018/1725, which states that ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body’.

Personal data is collected and processed in accordance with the following legal instruments.

- Articles 151(1)(a) and (b) of Regulation (EU) 2017/1001 which stipulate that ´the Office shall have the following tasks: administration and promotion of the EU trade mark system; administration and promotion of the European Union design system´.
- Article 151(2) of Regulation (EU) 2017/1001 which stipulates that ´the Office shall cooperate with institutions, authorities, bodies, industrial property offices, international and non-governmental organisations in relation to the tasks conferred on it´.
- Joint Statement on an Expert Cooperation Charter in the Area of Anti-Scam which envisages information-sharing on instances of suspected fraud and compilation of a register of examples of malicious practices and of entities involved in such practices.

8. How long do we store your data?

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 until the closure of legal proceedings on the basis of misleading invoices reported to EUIPO.

9. Contact information

Should you have any queries on the processing of your personal data, please address them to the data controller, the Customer Department director, at the following email address: DPOexternalusers@euipo.europa.eu .

You may also consult the EUIPO data protection officer by sending an email to: DataProtectionOfficer@euipo.europa.eu.

Form of recourse:

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