Privacy statement on processing personal data in the management of log files

Protecting 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 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?

Log files are used to trace events in an information system and to help with its debugging and repair. They are part of the systems and are essential tools to provide security and efficient support when information systems are not working correctly.

Log files for the Office systems are processed in order to investigate and eliminate security incidents and malware infections on devices connected to the Office network, and/or to prevent data leaks.

Log files may also be processed for statistical purposes or to resolve users' problems accessing the Office's telecommunications systems.

2. What personal data do we process?

Log files can differ greatly in nature depending on the activity that is being logged. Activities recorded in log files can include, but are not limited to:

- visiting websites;
- accessing management stations of network components;
- connecting to databases;
- connecting to Unix/Windows computers.

Servers automatically record log files with information sent by the browser whenever a user visits a website. Log files are created to record elements that trace any operation or event on a system. These elements may include:

- user name;
- user ID;
- logical address (Internet Protocol address);
- timestamps for beginning and end of the operation / visit to a 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.

3. Who is responsible for processing the data?

Personal data processing is the responsibility of the director of the Digital Transformation Department (DTD), acting as the delegated EUIPO data controller.

Personal data is processed by DTD staff in charge of IT Operations, supported by the external service provider IECISA-ALTIA, for the purposes of managing EUIPO IT infrastructure and maintenance tasks.

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

Log files are stored automatically and nobody other than the IT security team (internal staff members) and system/network administrators (staff of the external service provider IECISA-ALTIA) have access to all of them. Log files may be processed or inspected manually when needed (in order to resolve incidents, errors, malware infections, etc.)

The permanent Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU) has been granted access to the log files related to perimeter security devices and workstation security, including:

- proxy log files;
- anti-spam / mail gateway log files;
- domain controller security log files;
- antivirus log files;
- workstation security log files;
- firewall log files.

Information is transferred to CERT-EU in order for it to carry out real-time monitoring of EUIPO systems and detect security issues. 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 these cases, personal data accessible to CERT-EU is limited to user name, IP address and timestamps for the beginning and end of the operation / visit to a website on the device where the incident was detected.

Furthermore, all information shared with CERT-EU is protected under a non-disclosure agreement (NDA).

In the case of on-going legal investigations or disciplinary processes, information may be made available to other parties, prior to approval by the data protection officer (DPO).

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.

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.

EUIPO systems and servers are password protected and require an authorised username and password to access. 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.

Regardless of stage, everybody dealing with personal data in the management of log files must sign a confidentiality declaration.

6. How can you access your personal information and, if necessary, correct it? How can you receive your data? How can you request that 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 restrict its processing or object to the same, as provided in Articles 17 to 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 DTD director.

The right to rectification only applies to inaccurate or incomplete factual data processed in the in the management of log files.

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, taking into account 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 '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 Office's information security policies.

8. How long can data be kept?

Log files are stored automatically and are kept for an agreed period of time depending on the type of information and the system it refers to. Data is stored for a maximum of 6 months, and usually between 1 week and 2 months. Log files are not archived.

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.

9. Contact information

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

Forms 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: edps@edps.europa.eu.