Specific Privacy Statement on the processing of personal data in the procedure of Office 365.

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 the purpose(s) of the processing operation?

Office 365 is a cloud based package of applications (Word, Excel, PowerPoint, Outlook, OneNote, OneDrive, Teams, and more) provided to users with the aim to offer more flexibility and improve communications, collaborations, as well as the availability of resources.

The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the above-mentioned services.

The processing is not intended to be used for any automated decision making, including profiling.

2. What personal data do we process?

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

- 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)

3. Who is responsible for processing the data?

The processing of the personal data is carried out under the responsibility of the Director of the Digital Transformation Department, acting as delegated EUIPO data controller.

Personal data is processed by DTD's external service provider, such as Microsoft, for the following activities:

- 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.

In you wish to see more information regarding the processing of personal data by Microsoft, please access their Microsoft Privacy Statement.

4. Who has access to your personal data and to whom are they disclosed?

The personal data is disclosed to the following recipients:

DTD Department, Microsoft and IECISA ALTIA (DTD Operations external service provider) involved in the data processing necessary to provide the service.

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. The following safeguards are implemented.

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.

5. How do we protect and safeguard your information?

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.

Office 365 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.

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.

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 restriction or 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 you data, in the cases foreseen by Articles 17 to 24 of the Regulation (EU) 2018/1725.

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

The right of rectification can only apply to inaccurate or incomplete factual data processed within the Office 365 procedure.

Your request will be answered free of charge and without undue delay, and in any event within one month of receipt of the request. However, according to article 14 (3) of Regulation (EU) 2018/1725 that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

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

Processing is based on Article 5.1 (a) of the Regulation (EU) 2018/1725.

The personal data are collected and processed in accordance with the EUIPO Information security policies.

8. How long do we store your data?

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.

In the event of a disciplinary or criminal investigation, or formal appeal that involves information included in emails, all data held at the time of the formal appeal or investigation should be retained until the completion of the process.

9. Contact information

Should you have any queries/questions concerning the processing of your personal data, please address them to the data controller, Director of the Digital Transformation Department under the following mailbox: UserFeedback@euipo.europa.eu

You may consult EUIPO Data Protection Officer: 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.