Data Protection Statement on the processing of personal data in the context of EUIPO events/training and stakeholders' feedback using the Office 365 application 'Forms' (Microsoft Forms)

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(s) of the processing operation?

As part of the operational activities of the Office, we use the Microsoft Office 365 application 'Forms' (Microsoft Forms) to create registration forms and satisfaction surveys in the context of online, face-to-face and hybrid training sessions, meetings and events organised by different EUIPO departments with external stakeholder participation.

Microsoft Forms is also used to collect feedback from EUIPO stakeholders to better understand their needs, expectations and experience with EUIPO products and services, as well as to identify opportunities for improvement ([1]).

When national intellectual property offices (NIPOs) take part in an event's organisation, personal data gathered from these processes may, with the consent of the data subject, be shared with the co-organising NIPO for further analysis and record-keeping purposes.

This processing is not intended to be used for any automated decision making or profiling.

2. What personal data do we process?

Depending on the type of activity, event or training in question, and the type of participant (speaker or attendee), we may process some or all of the following data for each external participant:

Registration form:

- title,
- name and surname,

([1]) See, for example, the processing of personal data for immediate feedback and other surveys.

- email address,
- telephone number,
- organisation,
- position,
- city,
- country,
- user association,
- education (degree, field of study, institution, date of completion),
- professional experience (job title, company organisation, employment dates and duration, description of responsibilities),
- level of English,
- motivation letter,
- referrals (source where the user heard about the event/training),
- user training preferences,
- electronic identifying information: IP address, cookies, connection data and access times,
- EUIPO user account.

In face-to-face events, the following additional personal data may be processed:

- passport or ID number,
- representative ID number,
- accommodation and travel details,
- financial data (bank account details / credit card details, VAT number),
- health data (dietary restrictions).

For surveys:

- related to events or training sessions: these surveys are anonymous, no personal data is processed apart from electronic identifying information: IP address, cookies, connection data and access times;

- related to stakeholders' feedback: these surveys may be anonymous (as mentioned above) or, if necessary for the purpose of the survey, a limited amount of the respondents' personal data may be collected.

For the stakeholder feedback surveys, the categories of personal data collected will depend on the survey (e.g. name, surname, title, country, any personal data provided by the respondent within the form), etc. For more information on the type of personal data that may be collected, please refer to the relevant activity's data protection statement ([2]).

([2]) For example, for personal data collected in the context of customer feedback, please see the relevant data protection statement.

3. Who is responsible for processing the data?

Personal data processing is the responsibility of the head/director of the EUIPO department or service that is organising the activity, training or event, acting as the delegated EUIPO data controller.

Personal data is processed by the Digital Innovation Department (DID) staff in charge of IT operations as the internal processor.

In addition, Fujin (the external service provider) and Microsoft (the service provider) are involved as external processors.

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

Personal data is disclosed to the following recipients.

- Personal data will be accessible to the EUIPO staff members responsible for the management of training and events or for handling the EUIPO stakeholders' feedback.

- In the context of specific events organised by the Business Development Department, with the help of the NIPOs, access to the personal data of participants (their name, surname, profession, country, NIPO and email address) may be shared with the contact points of the other NIPOs involved.

- The Digital Innovation Department (DID) staff in charge of IT operations, supported by the external service provider Fujin, may also have access to your personal data.

- As regards Microsoft, in principle, the majority of the service operations are automated to reduce the need for human access. Microsoft engineers and support staff do not have access to customer data by default. They are only granted access if and when it is required for maintenance purposes. The information is stored in Microsoft Datacenters located in the EU, although information may be made available to subcontractors in other countries, depending on the maintenance or support requirements and availability of this expertise. Nevertheless, if access is granted, it is always temporary and is strictly limited to the information required for the specific maintenance or support procedure being carried out.

- The Workplace Solutions DepartmentI, and their external processors, Vitel S.A. and Zoom, may be given access to your personal data to be able to organise the training sessions and events.

- The Communication and Media Relations Service in order to record, film and take photos during training sessions and other events for promotional purposes.

The information processed through the registration form and/or post-event survey will only be shared with those required to implement these measures and only on a need-to-know basis. Personal data is not used for any other purposes or disclosed to any other recipients.

The information in question will not be communicated to third parties, except where necessary for the purpose(s) outlined above.

The information will be stored in Microsoft Datacenters located in the EU. Nonetheless, as indicated in DPR-2018-003, information may be made available to subcontractors in other countries, depending on the maintenance or support requirements and availability of this expertise. However, if access is granted, it is always temporary and is strictly limited to the information required for the specific maintenance or support procedure being carried out.

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.

EUIPO systems and servers are password protected and require an authorised username and password for access. The information is stored securely to safeguard the confidentiality and privacy of the data therein.

Microsoft Datacenters are certified in several security standards, most notably 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, unauthorised access, or any other type of unlawful activity.

  Microsoft has implemented a list of over 700 security controls in its systems, servers and datacentres. This includes security controls against accidental or unlawful destruction, loss, unauthorised 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. Information is encrypted while at rest and in transit. As mentioned above, information may be made available to subcontractors in other countries, depending on the maintenance or support requirements and the availability of this expertise. Nevertheless, if access is granted, it is always temporary and is strictly limited 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 Data Privacy Framework.

- Microsoft requires sub-processors to join the Microsoft Supplier Security and Privacy Assurance Program.

  This program is designed to standardise 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 sub-processors.

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 restrict and 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 EUIPO department director of the department that is organising the training or event or that handles the stakeholders' feedback activity).

The right to rectification only applies to inaccurate or incomplete factual data processed through Microsoft Forms within the registration procedure for a training or event organised by the EUIPO.

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)(d) (consent) of Regulation (EU) 2018/1725. Participants and speakers in training and events organised by the EUIPO confirm their consent to the processing of their personal data before they submit a registration form or survey through Microsoft Forms.

For more information on the processing of personal data in the context of EUIPO stakeholders' feedback, please refer to the legal basis indicated in the relevant data protection statement ([3]).

([3]) For example, for personal data collected in the context of customer feedback, please see the relevant data protection statement.

8. How long do we store your data?

Your personal data will only be kept for the time necessary to achieve the purpose(s) for which it will be processed.

Registration forms and surveys are deleted in Office 365 3 months after the date of the event. Data extracted from Office 365 is kept in the EUIPO's content management system (Sharedox) in the following ways.

- Part of the data (name, surname, title, signature, email, bank details, fiscal code and address if applicable) is stored for accountancy purposes for a maximum of 7 years.
- Health-related data is stored for a maximum of 1 month after the event, unless the participant has withdrawn their consent. If consent is withdrawn, the data will be deleted without undue delay. If a health-related incident is reported after the event, health-related data is stored until the closure of any legal proceedings or for a maximum of 5 years following the event.
- The rest of the data is stored for a maximum of 6 months after the event.
- Contact details can be kept as part of a contact details database for a maximum of 10 years or until consent is withdrawn. These details may be shared internally among the EUIPO departments to invite the data subjects to future meetings/events.

For the storage duration of personal data collected in the context of EUIPO stakeholders' feedback, please refer to the relevant data protection statement ([4]).

In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.

9. Contact information

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

You may also consult the EUIPO Data Protection Officer at: DataProtectionOfficer@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.

([4]) For example, for personal data collected in the context of customer feedback, please see the relevant data protection statement.