DATA PROTECTION NOTICE

on the use of Microsoft 365

Last updated: 13 May 2025

Eurofound, who acts as the data controller, embraces the need to protect your personal data. We, therefore, undertake to process it, as data controller, with respect to the applicable law[1].

If after reading this notice you still have questions on the processing of your data, please contact us at dataprotectionofficer@eurofound.europa.eu. We will reply to you within one month.

Who is the data processor?

The data processor is Microsoft Ireland Operations Limited[2], which can be contacted at Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

Who are the data subjects?

Data subjects of this processing operation include:

- Eurofound's staff members,
- Staff members of other EU Institutions, Bodies and Agencies, and
- Any natural person whose personal data is being processed using M365 (e.g., a participant in a Teams call, an email recipient, a participant in a survey).

Why do we process your personal data?

In line with the European Commission's Digital Workplace Strategy (adopted in 2017) and to fulfil its "Any place, Any time, Any (corporate) device" promise, Eurofound uses the cloud-based solution called Office 365 provided by Microsoft (or M365). This enables

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 (or the EUDPR).

[2] Microsoft Ireland, an affiliate of Microsoft Corporation, acts as Eurofound's data processor. Appropriate agreements have been concluded to regulate this relationship.

Eurofound

Eurofound's staff to work on any (corporate) device and facilitates collaboration with internal and external stakeholders.

M365 is used transversally across Eurofound to enable security functions, data analyses, project work, real-time communication, social networks, among others. Given the broad spectrum of M365 use, it is difficult to list all purposes of use. Nonetheless, Eurofound processes your personal data for a variety of different purposes, namely:

- Creation of all M365 accounts;
- Communication and collaboration using Teams[3];
- Collaboration on documents using Microsoft SharePoint Online and OneDrive;
- Sending and receiving emails using Microsoft Outlook Online;
- Use of integrated Office 365 functionality within these tools;
- MS Forms for contact forms on website and events registration; and
- Management of projects planned in the Programming Document.

Ultimately, Microsoft processes your personal data to deliver the agreed-upon services[4].

Please note that none of these purposes carried out by Eurofound involves the need to make a decision solely by automated means and without any human intervention.

Which personal data do we collect and process?

The personal data processed by Eurofound includes:

- any personal data which Eurofound elects to include in Customer Data, i.e., all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Eurofound through use of the M365. It includes, but is not limited to, the following data:
    - Identification data: e.g. title, name, email address, birthday, profile photo (if applicable);

[3] For more information, please read the applicable data protection notice.
[4] The services provided by Microsoft consist of (i) delivering functional capabilities as licensed, configured, and used by Eurofound and its users, including providing personalised user experiences and processing data as necessary to fulfil contractual obligations to Eurofound or to otherwise comply with law; (ii) troubleshooting (preventing, detecting, and repairing problems affecting the operation of online services); and (iii) ongoing improvement (installing the latest updates and capabilities, and making improvement to user productivity, reliability, efficacy, and security).

- Contact details: e.g. office telephone number, mobile and home telephone number (optional);
- Personal characteristics: e.g. gender, hobbies and interests, skills and expertise, school and education (all optional);
- Professional data: e.g. current position and unit, line manager, current responsibilities / projects involved;
- Contacts data (Third party contacts are processed in Outlook and MS Teams);
- Electronic communications data: e.g. IP addresses, cookies and connection data;
- User patterns: e.g. media utilisation, methods of communication;
- Content data: any data content generated and controlled by Eurofound staff members, including chat messages (one-to-one as well as group messages) and any other personal information, voluntarily posted on the platform; and
- Multimedia: e.g. image and sound recording.

- any personal Data that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of Eurofound's use of service-based capabilities or obtained by Microsoft from locally installed software. This includes:
  - Diagnostic data[5], which is a category of data collected or obtained by Microsoft from software installed by Eurofound on local devices used in connection with Online Services;
  - Service-generated data, which is a category of data generated or derived by Microsoft through the operation of the Online Services. Service generated data record events that occur in-cloud services by capturing activities within Microsoft computing environment, whether these activities are initiated by the user or by the tenant administrators. he following data fields are common for service-generated data.
    - User Principal Name
    - Activity ID such as copy, delete, mark as read.
    - Timestamp

[5] Does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office.

- Client ID
- User ID in hexadecimal pseudonymous identifiers
- Session ID
- Version
- Tenant Name
- Net ID
- Workload
- Source User ID
- Target User ID – as relevant/appropriate for event type
- Event timestamp (Date & Time)
- Event details (e.g. type, outcome (success/failure), detail information – defined per event type)
- Source & Target Hostname – as relevant/appropriate for event type; and
- Source & Target network addresses and protocols – as relevant/appropriate for event type.

In some specific procedures special categories of personal[6] data may be processed by Eurofound.

What is the legal basis for processing your personal data?

The processing of your personal data is necessary for the Agency to carry out its mandate[7] and, therefore, for the day-to-day functioning and management of the Agency and for the performance of tasks that Eurofound, as an EU Agency, carries out in the public interest[8].

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

Access to your personal data will be given to the following categories of recipients:

[6] As defined in Article 10(1) of the EUDPR: *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.
[7] According to Article 1 of Regulation (EU) 2019/127 of the European Parliament and of the Council of 16 January 2019 establishing the European Foundation for the improvement of living and working conditions (Eurofound), and repealing Council Regulation (EEC) No 1365/75.
[8] Article 5(1) (a) and recital (22) of the EUDPR.

- Eurofound staff members on a need-to-know basis. Staff abide by statutory confidentiality obligations;
- Eurofound's M365 administrators for configuration purposes;
- Eurofound's contractors for configuration and troubleshooting purposes. Contractors' staff abide by contractual confidential obligations; and
- Eurofound's processors, including Microsoft and Microsoft's processors[9].

No other third parties will have access to your personal data, except if required by law.

How long do we keep your personal data?

The following retention periods by Eurofound apply:

a) Your personal data (e.g., name, e-mail address and profile photo) will be replicated to M365 from on-premise Active Directory (AD) and will be deleted when the replication is stopped, or the account is deactivated from AD after departure from the Agency;
b) For retention periods applied to the processing of personal data on meetings in MS Teams please read the specific data protection notice available here;
c) For retention periods applied to the processing of personal data in events read the specific data protection notice available here;
d) Content data will be kept until it is necessary to fulfil the purpose of collection or further processing. Additional information is provided under the specific data protection notices available here; and
e) Log data will be kept for 90 days.

Microsoft will retain personal data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft deletes the data.

[9] A list of Microsoft processors is available here.

How do we protect and safeguard your data?

Microsoft has implemented appropriate security measures to ensure the protection of your personal data, including, but not limiting to:

- Microsoft personnel are subject to confidentiality obligations;
- Microsoft maintains an inventory of all media on which Customer Data or Personal Data is stored. Access to the inventories of such media is restricted to the Microsoft personnel authorised in writing to have such access;
- Microsoft limits access to facilities where information systems that process Customer Data or Personal Data are located to identified authorised individuals;
- Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference; and
- Microsoft is certified in the following ISO standards:
    - ISO/IEC 20000-1: Information technology — Service management; Part 1: Service management system;
    - ISO 22301: Business Continuity Management Standard requirements;
    - ISO/IEC 27001: Information Security Management Standards;
    - ISO/IEC 27017: Code of Practice for Information Security Controls;
    - ISO/IEC 27018: Code of Practice for Protecting Personal Data in the Cloud;
    - ISO/IEC 27701: Privacy Information Management;
    - ISO/IEC 42001: Artificial intelligence management system; and
    - ISO 9001: Quality management systems — Requirements.

Eurofound has a documented Electronic Information Security Policy, which defines the generic ICT infrastructure security measures that are in place. Eurofound permits guest users and has disabled all third-party apps. We also have a contract with external consultants to understand, configure and document all governance and security decisions related to Microsoft365 implementation, including the use of SharePoint. Staff are advised to ensure that any devices that access the information from the SharePoint site or on which information is downloaded are appropriately encrypted and possess appropriate network security safeguards, such as up-to-date virus protection, firewalls and security patches.

Do we transfer any of your personal data to third countries or international organisations (outside the EU/EEA)?

Pursuant to the Inter-institutional Licensing Agreement signed between the EU institutions and agencies and Microsoft[10]:

- Customer Data and Personal Data is stored and processed in data centres in the EU and EFTA[11];
- Stored service generated logs from the Microsoft 365 In-Scope Services takes place in the EU, Norway, and the following adequate countries: Canada, Israel, Japan, New Zealand, Switzerland, United Kingdom, United States, and Uruguay;
- Access to the limited Customer Data and pseudonymised personal data for security operations may take place in the EU, Norway, adequate countries (Canada; Israel; Japan; New Zealand; Switzerland; United Kingdom; United States; Uruguay), Australia, India, and the United Arab Emirates;
- Microsoft Online Services are highly automated and designed to operate without human intervention. Accordingly, if an Online Service is down or broken, the first level of repair is fully automated. In exceptional cases where automation is unable to remediate an issue and Microsoft human engineers need access to the production infrastructure. Processing may take place in EU, adequate countries (Canada; Israel; Japan; New Zealand; Switzerland; United Kingdom; United States; Uruguay), Australia, Brazil, Chile, Colombia, Costa Rica, Egypt, El Salvador, Georgia, India, Jordan, Kenya, Malaysia, Mexico, Peru, Philippines, Serbia, Singapore, South Africa, Taiwan, and Vietnam; and
- Microsoft personnel and approved staff augmentation vendors who support internal platform services upon which M365 is dependent may process data in the EU, adequate countries (Canada; Israel; Japan; New Zealand; Switzerland; United Kingdom; United States; Uruguay), Australia, Brazil, Costa Rica, Egypt, India, Jordan, Malaysia, Serbia, Taiwan, Türkiye, and United Arab Emirates.

Please note that Microsoft does not control or limit the regions from which the customer or its end users may access or move customer data. Therefore, in case a staff member travels outside the EU/EEA and uses the services, personal data may be processed

[10] Which will enter into force on 1 June 2025.
[11] Iceland, Liechtenstein, Norway, and Switzerland.

outside the EU/EEA to enable the user access to the online services from their location. Staff members should refrain, as much as possible, from accessing Microsoft functionalities, for work purposes, outside the EU/EEA area.

10. What are your rights as a data subject and how can you exercise them?

Within the limits set by the EUDPR, you have the right to access, rectify, erase and/or port your personal data, to restrict or object to the processing of your personal data, and to withdraw your consent (if obtained). Just note that withdrawal of your consent does not affect the lawfulness of processing while your consent was valid.

You may contact the ICT sector (ICT@eurofound.europa.eu) with your request. Your request is free of charge. However, if it is manifestly unfounded or excessive, Eurofound may refuse to act on it.

You also have the right to raise a complaint with the European Data Protection Supervisor should you consider that this processing is in violation of the law. You will find more information here.