



PRIVACY STATEMENT

Processing of personal data in the context of Microsoft 365 access for external users

1. Introduction

The protection of your personal data is of high importance to the Smart Networks and Services Joint Undertaking (SNS JU). SNS JU is committed to respecting and protecting your personal data and ensuring your rights as a data subject.

All personal data processed in the context of Microsoft 365 (M365) services are handled fairly, lawfully and with due care, taking into account the specific risks related to cloud-based services.

This processing operation is subject to Regulation (EU) 2018/1725. The present privacy statement is provided pursuant to Articles 15 and 16 of that Regulation.

2. Controller

The controller for this processing operation is:
Smart Networks and Services Joint Undertaking (SNS JU)
Avenue de la Toison d'Or 56-60
1060 Brussels, Belgium
Email: data-protection@sns-ju.eu

SNS JU has appointed a Data Protection Officer (DPO), who can be contacted at the same address.

3. Purpose of the processing

Personal data are processed for the provision, administration and secure use of Microsoft 365 services, including:

- provision and management of user accounts and identities (e.g. Microsoft Entra ID)
- access to collaboration tools (e.g. Outlook, Teams, SharePoint, OneDrive)
- communication, document management and collaboration activities
- management of access rights and permissions
- monitoring, security and incident detection

- ensuring integrity, availability and confidentiality of IT systems and data
- compliance with internal policies, security requirements and legal obligations

4. Categories of data subjects

The processing concerns:

- SNS JU staff and management
- external users granted access (e.g. experts, contractors, partners)
- individuals whose personal data are included in content stored or exchanged via M365

5. Personal data processed and legal basis

5.1 Categories of personal data

SNS JU may process the following categories of personal data within the M365 environment:

a) User and account data

- name, surname, user ID
- professional email address and contact details
- role, function and access rights

b) Content data (Customer Data)

- emails, documents, files and communications created, stored or shared by users
- personal data contained in such content

c) Technical and usage data

- log data (login, access, activity history)
- device and connection data (IP address, identifiers)

d) Service-generated and diagnostic data

- metadata and telemetry data generated through the use of M365 services
- diagnostic data (Required or Optional) transmitted to Microsoft for service operation, security and improvement

e) Security-related data

- alerts, incident reports, suspicious access attempts

In specific cases, personal data may include special categories of data where processed by users within M365 tools. SNS JU does not intentionally process such data through M365 unless necessary and subject to safeguards.

5.2 Legal basis

Processing is based on:

- Article 5(1)(a) of Regulation (EU) 2018/1725 (task carried out in the public interest)
- Article 5(1)(b) of Regulation (EU) 2018/1725 (compliance with legal obligations)

Processing is necessary for the functioning of SNS JU and compliance with:

- Council Regulation (EU) 2021/2085 establishing SNS JU
- EU Financial Regulation and internal control requirements
- applicable IT security, data protection and administrative rules

Where applicable, processing of special categories of data is carried out in accordance with Articles 10 and 11 of Regulation (EU) 2018/1725.

6. Roles and responsibilities

SNS JU acts as **data controller** for personal data processed in the context of its use of M365 services.

Microsoft acts primarily as **data processor**, providing cloud services under contractual arrangements (including the Interinstitutional Licensing Agreement and Data Processing Agreement).

However, for certain processing activities (in particular related to diagnostic data, service-generated data or connected services), Microsoft may act as an **independent or joint controller**.

SNS JU is not responsible for processing operations carried out by Microsoft in its capacity as independent or joint controller. Data subjects are invited to consult Microsoft's privacy documentation for further information: <https://privacy.microsoft.com/>

7. Source of the data

Access to personal data is granted on a need-to-know basis to:

- authorised SNS JU staff responsible for IT, administration and security
- European Commission services providing IT infrastructure and support
- Microsoft, as provider of M365 services
- authorised contractors supporting IT systems, under appropriate safeguards

In specific cases, data may be disclosed to:

- audit, control or security authorities
- competent EU bodies (e.g. OLAF, European Court of Auditors)
- judicial or law enforcement authorities where required by law

8. Recipients of the data

Access to personal data is granted on a need-to-know basis to:

- authorised SNS JU staff responsible for IT systems and administration
- European Commission services where relevant for IT infrastructure
- Microsoft, as service provider of Microsoft 365

- other authorised contractors or service providers supporting IT operations, under appropriate safeguards.

9. Transfers to third countries

Personal data processed within M365 may be transferred outside the European Economic Area (EEA), in particular in the context of:

- support services
- diagnostic and service-generated data
- sub-processors used by Microsoft

Such transfers are governed by contractual arrangements concluded at EU level (including the Interinstitutional Licensing Agreement and applicable safeguards).

SNS JU monitors these transfers and relies on appropriate safeguards in accordance with Articles 46–49 of Regulation (EU) 2018/1725, including standard contractual clauses and additional safeguards where required.

10. Data retention

Personal data are retained according to their category and purpose:

- account data: for the duration of access and up to **1 year** after deactivation
- logs and technical data: up to **6 months**, unless required longer for security or audit purposes
- content data: in accordance with SNS JU document management and retention policies
- incident-related data: for the duration necessary to investigate and follow up incidents

Retention rules are defined in SNS JU internal policies and aligned with applicable retention schedules.

11. Security measures

SNS JU implements appropriate technical and organisational measures, including

- role-based access control and authentication mechanisms
- secure configuration of M365 services and environments
- monitoring and logging of access and activity
- incident detection and response procedures
- contractual safeguards with Microsoft and its sub-processors
- periodic review of security measures and compliance

Microsoft implements technical and organisational measures as processor, as described in its contractual commitments.

12. Handling of personal data breaches

SNS JU has procedures in place for the detection, reporting and management of personal data breaches.

In the context of M365, incidents involving Microsoft are handled in coordination with the service provider and relevant EU services.

Where required, SNS JU will notify the European Data Protection Supervisor (EDPS) and affected data subjects in accordance with Regulation (EU) 2018/1725.

13. Rights of Data subjects

Under Regulation (EU) 2018/1725, you have the right to:

- access your personal data
- rectify inaccurate or incomplete data
- request restriction of processing
- object to processing

Requests can be addressed to: data-protection@sns-ju.eu

Data subjects may also access certain personal data directly through Microsoft tools (e.g. account settings), where applicable.

Certain rights may be restricted in accordance with Article 25 of Regulation (EU) 2018/1725, in particular to ensure security, confidentiality or the proper functioning of IT systems.

14. Complaints

If you consider that your rights have been infringed, you may contact the SNS JU DPO.

You also have the right to lodge a complaint with the European Data Protection Supervisor (EDPS):

European Data Protection Supervisor

Rue Wiertz 60

B-1047 Brussels

Email: edps@edps.europa.eu

13. Further information

Further information on Microsoft's data processing activities is available at:

<https://privacy.microsoft.com/>

The SNS JU public register of processing activities is available at:

<https://smart-networks.europa.eu/data-protection-declaration/>