PRIVACY STATEMENT

Processing of personal data in the context of IT Systems, network access and security

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 framework of the selection, appointment and management of external experts and evaluators are handled fairly, lawfully and with due care.

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 ensuring the secure and efficient operation of SNS JU IT systems and infrastructure, including:

- provision and management of user accounts and access rights
- administration of network access and authentication mechanisms
- operation and maintenance of IT systems and applications
- monitoring and logging of system usage and access
- detection, prevention and management of security incidents
- ensuring integrity, availability and confidentiality of systems and data

- technical support and troubleshooting
- compliance with security, audit and internal control requirements

4. Categories of data subjects

The processing concerns:

- SNS JU staff and management
- external users with access to SNS JU systems (e.g. contractors, experts)
- visitors or users interacting with SNS JU IT infrastructure

5. Personal data processed and legal basis

Personal data processed

SNS JU may process the following categories of personal data:

- identification data (name, surname, user ID)
- contact details (email address, telephone number)
- account and authentication data (usernames, roles, access rights)
- technical data (IP address, device identifiers, system logs)
- usage data (login history, activity logs, system interactions)
- security-related data (incident reports, alerts, access attempts)
- Processing does not aim at monitoring individuals but may involve logging activities for security purposes.

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 to ensure compliance with:

- Council Regulation (EU) 2021/2085 establishing SNS JU
- EU Financial Regulation and internal control requirements

applicable IT security and data protection rules.

6. Source of the data

Personal data are:

- provided directly by users
- generated automatically by IT systems and security tools
- provided by SNS JU services or partner organisations for access management

7. Recipients of the data

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

- authorised SNS JU IT and administrative staff
- European Commission services providing IT infrastructure or support
- contractors and service providers supporting IT systems, under appropriate safeguards
- audit, control or security authorities where required European Anti-Fraud Office (OLAF)

- other competent EU bodies or authorities

In specific cases, data may be shared with judicial or law enforcement authorities where required.

8. Transfers to third countries

In principle, personal data are processed within the European Economic Area (EEA).

Where transfers to third countries occur (e.g. when an applicant is located outside the EEA), they are carried out in compliance with Regulation (EU) 2018/1725.

9. Data retention

Personal data are retained according to their category:

- account data: for the duration of access and up to 1 year after deactivation
- system and access logs: up to 6 months, unless required longer for security or audit purposes
- incident-related data: for the duration necessary to investigate and follow up the incident

At the end of the retention period, data are securely deleted.

10. Security measures

SNS JU implements appropriate technical and organisational measures, including:

- role-based access control
- secure storage and handling of sensitive information
- confidentiality obligations for staff and stakeholders
- monitoring and protection of IT systems

Enhanced safeguards are applied where sensitive data are processed.

11. Rights of data subjects

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

- access your personal data
- rectify inaccurate or incomplete data
- request erasure of your data
- request restriction of processing
- object to processing
- withdraw your consent at any time (where applicable)
- not be subject to automated decision-making

Requests can be addressed to: data-protection@sns-ju.eu
SNS JU will reply within one month, which may be extended in complex cases.
Restrictions to these rights may apply in accordance with Article 25 of Regulation (EU) 2018/1725.

12. 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

The SNS JU public register of processing activities is available at:
https://smart-networks.europa.eu/data-protection-declaration/