



EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: Identity & Access Management Service (IAMS)

Data Controller: EC DIGIT D3

Record reference: DPR-EC-03187

Table of Contents

- 1. Introduction**
- 2. Why and how do we process your personal data?**
- 3. On what legal ground(s) do we process your personal data?**
- 4. Which personal data do we collect and further process?**
- 5. How long do we keep your personal data?**
- 6. How do we protect and safeguard your personal data?**
- 7. Who has access to your personal data and to whom is it disclosed?**
- 8. What are your rights and how can you exercise them?**
- 9. Contact information**
- 10. Where to find more detailed information?**

1. Introduction

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant 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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation "Identity & Access Management Service (IAMS)" including EU Login, undertaken by EC DIGIT D3, is presented below.

2. Why and how do we process your personal data?

Purpose of the processing operation: The European Commission's Identity & Access Management Service (IAMS) provides a common way for individuals to register or be registered for access to a number of different Commission information systems or services.

EC DIGIT D3 collects and uses your personal information to manage user populations and their rights in the context of IT systems. The main purpose is to ensure the appropriate level of security is applied in a consistent fashion across Commission IT services with the ability to identify the user of the service, authenticate that user, and / or determine his or her authorisations and roles within the context of their service. The IAMS allows not only the authentication of individual that have an employment relationship with EU Institutions (EU Staff), but also self-registered individuals can create an EU-login account worldwide.

Additional purposes for this processing operation, regarding individuals that have an employment relationship with EUIs, are the following:

- services, allowing individuals contact details to be found (e.g. e-mail address book or telephone directory)
- selection of individuals from lists, usually based on some selection criteria
- construction of lists of individuals, primarily e-mail distribution lists
- customisation of user interfaces according to users' individual characteristics

The processing is automated and performed by means of computer/machine.

Your personal data will not be used for an automated decision-making including profiling.

Individual Commission sites that rely on IAMS for commonly required personal data, may nevertheless collect additional personal data themselves. This data processing will be covered by the sites' own privacy statements.

3. On what legal ground(s) do we process your personal data

We process your personal data, because:

(a) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

The processing is necessary for the performance and support of tasks carried out by the institution as mandated by the Treaties, in particular Articles 3, 4, 5, 6, 7, 11, 17, of the Treaty of the European Union and Articles 2, 4, 67, 310, 325 of the Treaty of the Functioning of the European Union.

Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission and Information Security Policy and Internal Rules for handling ICT Information Security Incidents, the Commission Information Systems Security Policy C(2006)3602.

Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385), as last amended by Commission Delegated Regulation (EU) 2016/1611 of 7 July 2016.

This processing operation is also in line with Regulation (EU) 2018/1724 on establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 and within the scope of the EC's eGovernment Action Plan 2016-2020 on accelerating the digital transformation of governments

The above-mentioned legal basis applies to the EU-login users that have an employment relationship with the EU Institutions, agencies and Bodies (EU Staff).

The personal data of the self-registered individuals is processed based on their consent after having read, understood and agreed to this privacy statement. Consent can be withdrawn at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Which personal data do we collect and further process?

In order to carry out this processing operation EC DIGIT D3 collects the following categories of personal data:

For EU Institutions staff, IAMS is processing only identification data (to identify the individuals):

- Personal information:
 - first, middle and last name(s) as provided by the HR Systems,
 - date of birth
 - personal title
 - history of changes in the name
 - an unique number per EU Institution, Agency or Body attributed by the HR System of each entity (Personal Number)
 - an unique identification number in attributed by the Commission HR System (Per_ID)

Based on the above, IAMS generates a unique:

- username or account (based on specific rules)
- e-mail address (based on specific rules)

IAMS keeps a history of:

- name changes (to avoid creation of multiple identities for the same individual)
- password changes (to enforce regular changes (passwords are irreversibly encrypted)
- last authentication and authenticated account activity (date and time of the most recent successful and unsuccessful authentication and number of good logins and failed attempts)

This additional information is used to diagnose and resolve problems and to deal with security incidents as well as to avoid duplicated accounts. This information can help in following up any doubtful/malicious activity relating to your user account.

- Administrative data (to identify the relationship with the organization):
 - the entity where the individual is assigned
 - the job title
 - the job status
 - information related to the start and end of the contract
 - office address and phone number
 - mobile phone number (for two-factor authentication, when available into the HR System)

Based on the above and on the HR "basic entitlements policy", IAMS generates:

- access rights - information about group membership (for granting access to the intended systems)

For self-registered individuals, IAMS is processing only identification data.

- Personal information (as provided by the individual during self-registration):
 - first, middle and last name(s)
 - e-mail address
 - username
 - mobile number, when provided for two-factor authentication.

For the two-factor authentication using the EU Login mobile app, the Operating System software of the mobile device is stored as well.

Alternatively, self-registered Individuals may choose to authenticate using their social network credentials (like Facebook, Twitter, and Google) or the eID. In this case, only the Social-media/eID identifier is required. The individual may decide to provide additional information such as:

- First, last name
- e-mail address

Please note that if you choose this option, we would recommend you also read the privacy statements/notices of the related social network, since they are also applicable.

Log files for both user categories

Each time the user logs in to a site protected by EU Login, the identifier, the site and the time will be recorded in a log file. The exact time of log-out will also be recorded for security purposes.

The provision of personal data is mandatory to meet access requirement to the European Commission IT Systems. If you do not provide your personal data, the consequences is that you will not be able to get access to the mentioned IT systems.

We have obtained your personal data either from the HR system of your EU Institution, Agency or Body for the EU Institutions staff, or directly from the data subject for the self-registered individuals.

5. How long do we keep your personal data?

EC DIGIT D3 only keeps your personal data for the time necessary to fulfil the purpose of collection.

Data related to the European Institutions Staff are kept for as long as the user has a relationship with the European Commission.

However, the user's identifier (userid), personnel number, first/last name, and, to prevent errors, date of birth are retained for a longer period in order to:

- allow the reuse of the identifier, if appropriate, should the person require renewed access to Commission IT resources after a long absence or for assuming his/her rights for example while in retirement,
- to determine the real global identity of a user and prevent duplication of entries.

For other EU Institutions, Agencies and Bodies, the above-mentioned data, will be limited to the information provided by each one of them according to their Human Resources policy.

Data related to self-registered individuals are kept until the user personally deletes his/her EU-Login account or requests the deletion by our Unit, with the exception of e-mail addresses that need to be kept for further user support and assistance.

History of identity changes for the European Institutions staff is kept for as long as the user is active. However, the most recent entries of this data category should be kept longer to prevent duplication of entries and ensure security.

Log files are kept for 6 months.

6. How do we protect and safeguard your personal data?

All personal data in electronic format (databases) are stored on the servers of the European Commission. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

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

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Personal data is not shared with other recipients, or transferred to third countries or international organisations

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. What are your rights and how can you exercise them?

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) on grounds relating to your particular situation.

For self-registered individuals:

You have consented to provide your personal data to EC DIGIT D3 for the present processing operation. You can withdraw your consent at any time by notifying the Data Controller. You may also delete your account at any time. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact:

- For EU Institutions staff, your HR department; then all modifications will be automatically reflected in IAMS;
- For self-registered individuals, directly the Data Controller, at: EU-LOGIN-EXTERNAL-SUPPORT@ec.europa.eu.

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: <http://ec.europa.eu/dpo-register>.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-03187