



EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Services offered by the eDelivery building block (obtaining digital certificates and publishing service metadata)

Data Controller: European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT), Unit H.4

Data Processors: PKI Domain Owners¹

Record reference: [DPR-EC-05967.2](#)

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 The PKI Domain Owner is the organisation deciding which other organisations can be issued certificates that allow them to operate in a given eDelivery message exchange network.

1. Introduction

The European Commission (hereafter ‘the Commission’) is committed to protecting your personal data and to respecting 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 “*Services offered by the eDelivery building block (obtaining digital certificates and publishing service metadata)*” undertaken by the European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT), Unit H.4, is presented below.

The eDelivery building block helps public administrations exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. To this end, in addition to providing software and specifications, eDelivery offers a range of ancillary services for establishing an eDelivery secure exchange network and/or technical support and some of these may involve the processing of personal data.

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

Purpose of the processing operation: Unit H.4 collects and processes your personal information to provide you with the PKI Service and the SML Service offered by the eDelivery building block. To provide these services, Unit H.4 requires the services of Directorate-General for Informatics (DG DIGIT, Unit B.3).

The purpose of the processing for the two aforementioned specific services is as follows:

PKI Service: The purpose of the PKI Service is to provide digital certificates to organisations. Digital certificates are special computer files that can be used by IT systems to encrypt data and/or validate digital signatures (see https://en.wikipedia.org/wiki/Public_key_certificate for further details).

Your personal data is processed:

- if, as authorised representative of an organisation, you request a digital certificate for your organisation, or

- if, on behalf of the 'PKI Domain Owner'², you approve a request for a certificate.

In both cases, these personal data are processed as part of the procedure that the European Commission must follow to have a digital certificate issued.

Once a certificate is issued, the personal data used in the issuing process is retained to serve as proof that the process steps were duly followed, to contact you regarding events linked to the certificate management lifecycle (e.g., when the certificate is about to expire) or to authorise further requests linked to the issued certificate (e.g., requests to revoke the certificate).

An organisation asking for a certificate must submit to the internal service provider (DIGIT B.3) a signed Application Form to authorise the Commission services to manage (issue, renew, block) digital certificates. The Application Form contains personal data of the representative of the organisation. The scanned signed Application Form is stored as part of the process required for issuing certificates. The organisation must also send a file called "certificate signing request", which is uploaded in CommisSign (this file should not contain personal data in principle – however, personal data included by the organisation would be processed as described in DPR-EC-00678 "PKI CommisSign – Creation and preservation of private keys").

When an organisation requests a certificate, personal data pertaining to the certificate request is sent by the European Commission to the PKI Domain Owner for the latter to be able to approve or reject the request.

SML Service: The SML (Service Metadata Locator) Service is an IT system used to publish and look up the technical details needed to connect to other IT systems of interest.

The Commission does not require any personal data to provide or operate the service. However, it (DG DIGIT, Unit B.3) will process personal data:

- if a user publishes identifiers of natural persons (e.g., national identification numbers) instead of identifiers of organisations;
- if the digital certificates used to authorise an entity to publish data contain personal data.

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

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

Processing your personal data to carry out both services is undertaken on the basis of **Article 5(1)(a) of Regulation 2018/1725**: the processing of personal data 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.

Under the Connecting Europe Facility (CEF) Programme, your personal data was processed on the basis of Article 4 (4) of the Regulation (EU) No 1316/2013 of the European Parliament and of

² The PKI Domain Owner is the organisation deciding which other organisations can be issued certificates that allow them to operate in a given eDelivery message exchange network.

the Council, of 11 December 2013, establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, according to which *“In the telecommunications sector, the CEF shall support actions that pursue the objectives specified in a Regulation on guidelines for trans-European networks in the area of telecommunications infrastructure.”* In addition to that, according to the Article 6 (3) and Annex (Section 1.1) of the Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC, *“Building blocks essential for, and with demonstrable prospects of being used in, the development, deployment and operation of other digital service infrastructures as listed in Section 1.1 of the Annex, shall be given top priority for funding.”*, and *“The building blocks identified to be included in the work programmes, subject to Article 6 (1) and (3), are the following:[...] b) Electronic delivery of documents: this refers to services for the secure, traceable cross-border transmission of electronic documents.”*

Under the Digital Europe (DEP) Programme, your personal data is processed on the basis of Article 8 (1) of the Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, which states that the Union shall pursue objectives such as *“[...] (b) deploy, operate and maintain trans-European interoperable state-of-the-art digital service infrastructures across the Union, including related services, in complementarity with national and regional actions; (c) support the integration and use of trans-European digital service infrastructures and of agreed European digital standards in the public sector and in areas of public interest to facilitate cost-efficient implementation and interoperability; (d) facilitate the development, update and use of solutions and frameworks by public administrations, businesses and citizens, including of open-source solutions and the re-use of interoperability solutions and frameworks; [...] (g) support the design, testing, implementation, and deployment and maintenance of interoperable digital solutions, including digital government solutions, for public services at Union level which are delivered through a data-driven reusable solutions platform aiming to foster innovation and establish common frameworks in order to unleash the full potential of the public administrations’ services for citizens and businesses; [...]”*

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

In order to carry out this processing operation, Unit H.4 collects the following categories of personal data for the **PKI Service**:

- First and last name
- Function in organisation
- Organisation name
- Organisation VAT number
- Organisation address
- Hand or electronic signature
- Date of signature
- Email address
- Phone number

- Emails concerning the certificate management process (e.g., in which a PKI Domain Owner approves the issuing of a certificate for a specific organisation, in which an organisation requests the revocation of its certificate).

While providing the **SML Service**, Unit H.4 might process the following categories of personal data if they are present):

- Contact details (email address, first and last name, postal address, organisation name) that may be included in certificates
- Unique identifier (Business-specific identifier) linked to the Internet address where metadata about the services supported by the participant designated by that identifier can be found
- Log data about the performed operations for troubleshooting and security auditing purposes.

5. How long do we keep your personal data?

The Commission only keeps your personal data for the time necessary to fulfil the purpose of collection. The retention periods of the services covered by this privacy statement are as follows:

PKI Service:

Retention period:

- Personal data pertaining to the PKI Domain Owner is retained as long as the service is provided for that domain.
- Personal data pertaining to the representative of the organisation requesting the certificate is retained as long as the issued certificate has not expired or has not been revoked.
- Emails are retained for five years.

Start date description: Personal data is retained as of the moment it is made available by the user.

End date description:

- Personal data pertaining to PKI Domain Owners is deleted once the internal service provider is notified that the domain no longer requires the service.
- Personal data pertaining to the representative of the organisation requesting the certificate is deleted when:
 - a) The certificate has expired and the owner did not request a renewal, or
 - b) The certificate has been revoked and the owner did not request another certificate
- Emails are deleted five years after they were received.

SML Service:

Retention period:

- Certificates that contain personal data are retained as long as they are valid and as long as the SMP system is operational in the domain.
- The retention period for the unique identifiers that refer to natural persons is decided by the SML Domain Owner.

The internal service provider will remove the data at the latest once the service is no longer provided for the domain.

Start date description: Data is retained as of the moment it is made available by the user / uploaded by SMP Owners.

End date description:

- The internal service provider removes data pertaining to SMP Owners and/or the participants in a domain either on request or at the latest once the service is notified that the domain no longer requires the service.
- Certificates are deleted once they expire.

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

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the Commission and the PKI Domain Owners. 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.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States (['GDPR' Regulation \(EU\) 2016/679](#)).

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. 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 basis 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.

Data collected from users of the PKI Service is also shared with the relevant PKI Domain Owner that must approve the issuing of the certificate.

The information we collect will not be given to any other third party than mentioned above, except to the extent and for the purpose we may be required to do so by law. There are no international data transfers.

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) of Regulation (EU) 2018/1725 on grounds relating to your particular situation.

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 the Data Controller, European Commission, DG CNECT, Directorate-General for Communications Networks, Content and Technology, eGovernment and Trust (CNECT.H.4), CNECT-H4@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-05967](#).