EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: CEF eDelivery Digital Service Infrastructure (DSI)

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

Record reference: DPR-EC-05967.1

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 "CEF eDelivery Digital Service Infrastructure (DSI)" undertaken by Head of Unit H.4, Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission is presented below.

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

Purpose of the processing operation: DG CNECT H.4 collects and processes your personal information to provide you with vertical business processes offered by the CEF eDelivery DSI, specifically PKI service and SML service.

eDelivery DSI 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.

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

PKI service: In a general sense, Public Key Infrastructure (PKI) is a set of roles, policies, procedures and systems defined by a Certification Authority needed to create, manage, distribute, store and revoke digital certificates. The CEF eDelivery PKI service enables issuance and management of the digital certificates used by the users of the service on deployed eDelivery components to ensure confidentiality, integrity and non-repudiation of the data moving across systems. Two user roles are relevant with respect to the service: the organisation deciding which other organisations can be issued certificates to operate in a given message exchange network (hereinafter referred to as 'PKI Domain Owner') and the organisations participating in the message exchange network (hereinafter referred to simply as 'organisation') for that domain.

As the service is operated through the CEF building blocks technical support, please refer to the technical support DPMS record DPR-EC-06847.1 as a baseline, which defines how non-specific, non-required personal data (e.g., email signatures) is handled when communicating with our technical support. To deliver the PKI service, we process specific personal data where required in the certificate management lifecycle (e.g., to issue, retrieve, revoke a certificate) or to contact you regarding events linked to the certificate management lifecycle. Furthermore, when the organisation asking for a certificate is external to the European Institutions, it must submit a signed Power of Attorney (PoA) to establish the legal framework for the services of the European Commission to be able to manage digital certificates on its behalf. The scanned signed PoA is sent by the organisation to the Commission (to the internal data processor (DG DIGIT

D.3), who both stores it and provides it to the external data processor – the Certification Authority – as part of the process required for issuing certificates). Finally, when the organisation requests a certificate, the full request, possibly including personal data (such as the name of the requestor that may be present in the email signature accompanying the request), may be sent by the internal data processor to the PKI Domain Owner in order for the latter to be able to approve or reject it.

SML service: The Service Metadata Locator (SML) is the key component that enables dynamic discovery of participants in message exchange networks. To do so, it provides a technical way for privileged administrator organisations (hereinafter referred to as 'SMP Owners'), designated by the organisation(s) (hereinafter referred to as 'SML Domain Owners') operating the message exchange network, to create data entries in the SML service, for that domain, that link a unique identifier of a participant with the Internet address (URL) where metadata about the services supported by that participant can be found. In addition to the data entries being stored in an internal database of the Commission, to provide the service the data entries (i.e., the unique identifier of a participant and the Internet address where metadata about the services supported by that participant can be found) are also replicated in the DNS system, where they are publicly accessible by design.

As the service is operated through the CEF building blocks technical support, please refer to the technical support DPMS record DPR-EC-06847.1 as a baseline, which defines how non-specific, non-required personal data (e.g., email signatures) is handled when communicating with our technical support. The Commission does not require any additional personal data to operate the service. In particular, identifiers of participants should identify organisations, but the internal data processor cannot control if the users of the service unilaterally decide to publish identifiers of natural persons (e.g., national identification numbers). Users of the service are duly informed that this is not allowed, but there are no technical means to prevent it. Where the SMP Owners themselves are concerned, the internal data processor identifies them by means of digital certificates in which no personal data is requested.

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

Lawfulness for the processing of personal data for the provision the services is identified under 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. According to the Article 4 (4) of the Regulation (EU) No 1316/2013 of the European Parliament and of 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, "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."

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

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

- Name (first and last name);
- Organisation name;
- Unique identifier for organisation (e.g., public register number or VAT number);
- Position in company;
- Contact details (address of company, email address, phone number);
- Hand signature (of the Power of Attorney document);
- Date of signature;
- 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).

In order to carry out this processing operation, DG CNECT H.4 collects the following categories of personal data for the **SML service** (personal data is not requested, but may be present in):

- Certificates which may contain personal data (email address, first and last name, postal address, organisation name);
- Business-specific identifier (that should designate an organisation, but the data processor cannot exclude cases where it might be traceable to a natural person) 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 (i.e., the PoA document) 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 data processor is notified that the domain no longer requires the service.
- Personal data pertaining to the representative of the organisation requesting the certificate (i.e., the PoA document) 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 (All data should refer to legal entities and not natural persons, however it is possible that some of the data processed contain personal data such as email address, first and last name, postal address, organisation name.):

Retention period:

- Data pertaining to SMP Owners (i.e., certificates which should not include personal data) is retained as longs as the SMP system they own is operational in the domain.
- The retention period for data pertaining to the participants (legal entities) is decided by SML Domain Owner. The internal data processor 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 data processor removes data pertaining to SMP Owners and/or the participants (legal entities) 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 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.

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.

We also share your information with contractors (internal – DG DIGIT D.3, and external - Deutsche Telekom Security GmbH/PKI Domain Owners) and authorised technical and support staff of the Commission to fulfil the provision of services, described in this privacy statement. Data collected from users of the PKI Service is also shared with the PKI Domain Owners and the

Certification Authority that issues the certificates for the PKI service (outside of the EU organisation but based in the EU).

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. No international data transfers to third countries take place.

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**.