



## PRIVACY STATEMENT

### Assignment of electronic qualified signature to EASA staff members Ref 84

#### 1. What personal data do we collect?

To enable EASA Authorising Officers the possibility of signing documents electronically, the following data is processed

**From users requesting the qualified electronic signature service:**

- Name, Surname (as per IAMS)
- Commission generated User ID of the requestor (as per IAMS)
- professional e-mail address (as per IAMS)
- data present on the signing certificate for users of the remote signing functionality (defined by the issuer; it can be/but not limited to: fist/last name, Date of Birth, ID Number, membership, title/role)

**From users requesting for “remote” qualified certificate for electronic signature service (for issuance):**

- Given Name(s), Surname(s) as per the ID document
- ID document type
- ID document number
- Country issuer of the ID document
- issuance end expiration date of the ID document
- copy of the ID document
- nationality
- mobile phone number
- data related to the organization the user works for





FO Personal data processing records and compliance checklist - Public	Ref 084 Assignment of electronic qualified signature to EASA staff members
---	--

This data is deleted from the EU Sign database once the certificate is validated and issued.

[From users granted a remote qualified certificate for electronic signature \(after issuance\)](#)

- Commission generated User ID of the requestor (as per IAMS)
- date of certificate request
- date of the certificate issue
- information about certificate validity
- encrypted information related to the certificate (e.g. public key, certificate alias, etc.)

**2. For which purpose do we collect personal data and on which legal basis?**

The data processed is necessary to provide EASA Authorising Officers and their delegates the possibility of signing documents electronically. The extent and nature of data may vary depending on the type of certificates requested, as detailed above.

The processing operations are held under Article 5, 1 (a) of Regulation (EU) 2018/1725 for the performance of a task carried out in the exercise of official authority vested in the Union institution or body, as established by Regulation (EU) 2018/1139 and its responsibilities laid down in Chapter V, Article 75.

**3. Who may receive your personal data?**

**List of AOs**

EASA staff members responsible for keeping the list up to date in accordance with the internal designation/revocation process and the designated staff members to liaise with the processor for the issuance/revocation of certificates. The list of EASA staff members to whom the electronic qualified signatures are due will be sent by the EASA responsible for liaising with EU-Sign services.

**Data processed for issuance, maintenance and revocation of EU-Sign certificates**

Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle. Each designated staff member will then be individually invited to provide the personal data needed to initiate the issuance of the certificate. The EU-Sign service provider will be the sole recipient of such data. Remote certificates for qualified signature are also sent to the EU Sign’s Partner Qualified Trust Service Provider.





#### 4. How long are your personal data kept?

The extent and nature of personal data being processed depends on the action and the type of certificate requested, therefore different retention periods apply, as follows:

[Data processed by EASA to maintain the list of Authorising Officers \(AOs\):](#)

##### **5 years**

In accordance with EASA internal policy “Use of electronic documents & electronic identification means – PO.IMS.00118-003”

[Data processed by the processor \(EU-Sign\) as qualified electronic signature service provider:](#)

##### **25 months**

- Personal data related to the user of the electronic signature service
- Administrative data related to the user of the electronic signature service and
- Technical data related to the usage events of electronic signature service
- history of all operations performed by an individual

##### **Up to maximum 5 days**

- ID documentation data required to grant remote certificate for qualified electronic signature

##### **6 months**

- Personal information contained in the eSignature certificate, after revocation/withdrawal of the certificate
- logs

#### 5. What are your rights?

You have the right to request from EASA access to and rectification or erasure of your personal data or restriction of processing. You also have the right to object to processing of your personal data.





FO Personal data processing records and compliance checklist - Public	Ref 084 Assignment of electronic qualified signature to EASA staff members
---	--

Data subjects should however be aware that objection to provide the data required for the issuance of the certificates will prevent their issuance as well as the data subjects use of a qualified electronic signature.

EASA should provide information on actions taken on a data subject's request within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

A breach concerning your personal data should be communicated to you under certain circumstances. EASA should also ensure the confidentiality of electronic communications.

#### 6. Who is the data controller and how to exercise your rights?

EASA should exercise the tasks of the data controller for the purpose of these processing operations.

To exercise the mentioned rights, you can contact the controller by sending an email to: [ed-office@easa.europa.eu](mailto:ed-office@easa.europa.eu)

If you consider your data protection rights have been breached, you can always lodge a complaint with the EASA's Data Protection Officer ([dpo@easa.europa.eu](mailto:dpo@easa.europa.eu)) or with the European Data Protection Supervisor: [edps@edps.europa.eu](mailto:edps@edps.europa.eu).

