ACER
European Union Agency for the Cooperation of Energy Regulators

Data Protection Notice

EU- Sign services

(9.11.2021)

1. Introduction

This privacy statement explains the use of personal data by the EU Sign service provided by the European Commission's Directorate-General for Informatics (DIGIT) to the European Union Agency for the Cooperation of Energy regulators ("ACER").

This privacy statement explains how and why EU Sign processes, collects, handles and ensures protection of personal data provided and what rights you may exercise in relation to this data: the right to access, rectify, block, etc.

The European institutions are committed to protecting and respecting your privacy. As this service/application collects and further processes personal data, Regulation (EC) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, is applicable (here after the EUDPR).

The following information is provided as established in Articles 15 and 16 of Regulation (EC) 2018/1725.

2. Who are the controllers?

The controllers are ACER and the European Commission's Directorate-General for Informatics (DIGIT).

The Commission Data Protection Officer publishes the register of all operations processing personal data. You can access the Commission's register on the following link: http://ec.europa.eu/dpo-register and this specific processing has been notified to the Commission's DPO with the following reference: DPO-3848.

3. Why do we process your data?

ACER and DIGIT (referred to hereafter as the Data Controller) collect and use some basic personal information in order to provide a service to create, validate and extend electronic signatures and electronic seals and in order to operate the service efficiently (including maintaining usage statistics for service planning and billing purposes).

The personal data collected and further processed are:

- for the creation of a qualified signatures: full name, work email, mobile phone, document ID, country issuer of the document ID, nationality
- The requester's UserID.
- when applicable: The requester's Sysper JobID (only for European Commission users with specific EU Sign application roles).
- EU Login domain.
- The requester's Organisation.

- In the case of PDF signatures:
- Signer Name.
- Signer Contact.
- The subject's distinguished name(s) of the certificate(s) used to sign/seal.
- This personal data is connected to the following transactional data:
- Time of the signature request.
- Type of operation requested (sign, verify, extend).
- Which policy was applied to the operation (e.g. EC-internal, Seal, Qualified Electronic Signature)).
- Which rights you have within the EU Sign service.
- Hashes of the documents on which the operation was performed. The hash is unique to the document, but the original document cannot be derived from the hash.
- The certificate used to sign/seal, as well as the chain of CA certificates for the issuer of that certificate.
- Any time-stamps present.
- In the case of PDF signatures:
- Signer Reason.
- Signer Location.

The following personal data is collected and processed during the process of signing, sealing, validating or extending, but not stored after completion of the process:

- Any additional personal data that may be contained in the certificate used to sign/seal and the certificates of its chain.
- Any additional personal data contained in the document that is being signed, sealed, validated or extended.
- Any personal data included in the certificate used to sign/seal are those provided by you to the issuer of the certificate at the time of enrolment (e.g. at the time of purchase).
- A log of your EU Sign activity (signature and seal creations, verifications, or extensions) is kept for usage statistics and problem analysis by DIGIT. The system may use it to check your request against limits to prevent service abuse (unintentional or otherwise). This log is also available – only to you – as part of the EU Sign service. If your organisation (or DG) has subscribed to the seal service and has given you sealer status (meaning that you may use your organisation's seal), then your organisation's Seal Authorizing Officer (SAO) and Seal Supervisors can also view your seal usage log.
- Some of your personal information (UserID, Sysper JobID, EU Login domain, organisation, DG) is used to determine if you are authorized to use the electronic seal of your organisation, or if you have any specific administrative roles (e.g. seal authorizing officer or seal supervisor).
- The documents and signatures you provide with your requests are processed for the duration of your request and, unless stated otherwise elsewhere in this document, are not stored after the completion of your request.
- A persistent cookie may be created for your convenience to save your EUSign preferences, e.g. to keep default signature types (PAdES/XAdES/CAdES, enveloped/enveloping/detached).

4. How long do we keep your data?

The Data Controller only keeps the data for the time necessary to fulfil the purpose of collection or further processing. For the purpose of good administration and incident management, the retention period is 25 months in order to make it possible to compare one full year against the previous one. After 25 months the data is either deleted or anonymised.

5. How do we protect your data?

All data in electronic format are stored either on the servers of ACER, of the European Commission or of its contractors, the operations of which abide by the European Commission's security decision of 16 August 2006 [C(2006) 3602] concerning the security of information systems used by the European Commission.

ACER's and 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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The transmission of requests between your device and the server of the European Commission is done over a secure connection (TLS) to prevent interception or tampering.

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

Access to your data is provided to authorised staff of the European Commission only according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The same is applicable to the staff of the ACER.

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.

On the user/customer side, Seal Authorising Officers (SAOs) and Seal Supervisors have access to all usage details of the seals under their responsibility. Each user of the service can also access his/her own usage details. You can view a log of your own past activity on EU Sign by navigating to "My EU Sign" section.

EC DIGIT IT personnel (especially those teams operating the web application hosting, database hosting, hardware, network and EU Sign services) may have access to your data for operational reasons in accordance with the applicable provisions of the General Data Protection Regulation. For service administration and incident management purposes, they, in the discharge of their duties, can access log files, and investigate possible issues for a specific user.

For accounting and billing requirements SAOs, Seal Supervisors and DIGIT D service administration have access to usage statistics. These are normally aggregated but may also be on an individual user level.

For your personal EU Login information, please refer to EU Login.

Users must be aware that any personal data contained in documents to be signed/sealed will be contained in the signed/sealed document. Additionally, the signed/sealed document will contain the certificate(s) used to sign/seal. The signed/sealed document will not be stored by EU Sign after the finalization of the signing/sealing process, but users must be aware that any personal data in the document itself or in the certificate

used to sign/seal it, will be disclosed to any party to whom the signed/sealed document is provided. In most cases, the personal data contained in the signing/sealing certificate will include the signatory/sealer's name or email address; and usually an identifier of the signatory/sealer. In some cases (e.g. signing certificates provided through the Belgian eID), additional personal data are included in the signing/sealing certificates, such as year of birth or gender.

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

In case you wish to access your personal information processed in this context, you can contact the ACER Data Protection Officer at dpo@acer.europa.eu. You can, if need be, rectify any inaccurate personal data by sending a written request to the above mentioned email address. You may make a request for erasure of your personal data if you are in one of the situations laid down by Article 19 paragraph (1) of Regulation (EU) 2018/1725. In this case, you should send a written request to the same email address mentioned under section "Access". We will respond to your request without undue delay and at the latest within one month.

You could further request cancellation of your application and deletion of all linked personal data by making use of the contact information mentioned above.

You may make a request for restricting the processing of your personal data if you are in one of the situations laid down by Article 20 of Regulation (EU) 2018/1725 for the following reasons. In this case, you should send us a written request to the same email address mentioned under section "Access". You have the right to receive the personal data processed by ACER in this context in a structured, commonly used, and machine-readable format, and you may also request us to transmit this data to any other controller under the conditions of Article 22 of Regulation 2018/1725. In this case, you should send us a written request to the same email address mentioned under section "Access". You may object at any time to processing of your personal data under the conditions laid down by Article 23 of Regulation (EU) 2018/1725, on grounds relating to your particular situation. In this case, you should send us a written request to the same email address mentioned under section "Access".

8. Contact information

If you have comments or questions, any concerns or a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller using the following contact information:

For ACER: acer@dpo.europa.eu by indicating 'Data Protection' in the subject and explicitly specifying your request.

For The European Commission's Directorate-General for Informatics (DIGIT): EC-ESSI-SERVICE@ec.europa.eu

You may also contact:

The Data Protection Officer (DPO) of the Commission: DATA-PROTECTION-OFFICER@ec.europa.eu

Please note that you have the right to submit a complaint at any time to the European Data Protection Supervisor at edps@edps.europa.eu.