



European Union Aviation Safety Agency

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

Nr.	Item	Explanation
Assignment of electronic qualified signature to EASA staff members		
1.	Last update of this record	21.03.2023
2.	Reference number	084
Part 1 – Article 31 of Regulation (EU) 2018/1725 - Record (recommendation: Publicly available)		
3.	Name and contact details of the controller and of the staff member responsible	Controller: European Union Aviation Safety Agency (EASA) Staff member responsible: Head of ED Office Contact: ed-office@easa.europa.eu
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	EU-SIGN EU-SIGN-SERVICE@ec.europa.eu
7.	Purpose of the processing	Provide EASA Authorising Officers and their delegates the possibility of signing documents electronically, as provided for EASA Policy on “Use of electronic documents & electronic identification means” PO.IMS.00118-003. The register of all individuals entitled to hold signature powers in accordance with the above policy is kept and maintained by the ED Office in cooperation with the Legal Department and the Finance Department. This register will be used for the purposes of requesting EU-Sign the issuance or revocation of the electronic signature certificates.





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

8.	Description of categories of persons whose data are processed by EASA and list of personal data categories	<p>Categories of persons whose data are processed by EASA: EASA staff members designated as Authorising Officers and their delegates, in accordance with PO.IMS.00118-003.</p> <p>Categories of personal data processed from users requesting the qualified electronic signature service:</p> <ul style="list-style-type: none">- 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) <p>Additional categories of personal data processed from users at the time of the request for “remote” qualified certificate for electronic signature service:</p> <ul style="list-style-type: none">- 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 <p>This data is deleted from the EU Sign database once the certificate is validated and issued.</p> <p>Categories of personal data processed from users after the remote qualified certificate for electronic signature is granted:</p> <ul style="list-style-type: none">- Commission generated User ID of the requestor (as per IAMS)- date of certificate request
----	--	---





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

		<ul style="list-style-type: none">- date of the certificate issue- information about certificate validity- encrypted information related to the certificate (e.g. public key, certificate alias, etc.)
9.	Time limit for keeping the data	<p>The list of Authorising Officers (AOs) and its review is handled in accordance with the EASA internal processes under which AOs are designated. These lists are kept in accordance with the retention periods applicable to the process and personal data deleted as soon as the AO is replaced or designation withdrawn.</p> <p>Data processed by the processor in EU Sign observe the following time limits</p> <p>25 months</p> <ul style="list-style-type: none">- 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 <p>Up to maximum 5 days</p> <ul style="list-style-type: none">- ID documentation data required to grant remote certificate for qualified electronic signature <p>6 months</p> <ul style="list-style-type: none">- Personal information contained in the eSignature certificate, after revocation/withdrawal of the certificate- logs
10.	Recipients of the data	<p>List of AOs</p> <p>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.</p> <p>Data processed for issuance, maintenance and revocation of EU-Sign certificates</p> <p>Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle.</p>





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

		Remote certificates for qualified signature are also sent to the EU Sign's Partner Qualified Trust Service Provider.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
12.	General description of security measures, where possible.	<p>EASA staff accessing the AO lists are assigned to maintain the list in accordance with documented processes. Access is restricted to users according to pre-defined and authorised roles.</p> <p>All personal data held by the processor in electronic format (databases) are stored on the servers of the European Commission.</p> <p>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.</p> <p>The processor responsible staff abide by statutory, and when required, additional confidentiality agreements.</p>
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the below privacy statement.	See Privacy Notice

