EDPS record of processing activity

Record of EDPS activities processing personal data, based on Article 31 of 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Description
	Processing of personal data in the EDPS public-key infrastructure (EJBCA)	
1.	Last update of this record	**12-10-2023**
2.	Reference number	76
3.	Name and contact details of controller	European Data Protection Supervisor (EDPS) **Postal address**: Rue Wiertz 60, B-1047 Brussels **Office address**: Rue Montoyer 30, B-1000 Brussels **Telephone:** +32 2 283 19 00 **Email:** edps@edps.europa.eu Responsible department or role: Technology and Privacy Unit, Digital Transformation Sector, EDPS IT - EDPS-IT@edps.europa.eu Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759
4.	Name and contact details of DPO	dpo@edps.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details	

Nr.	Item	Description
	of processor (where applicable)	
7.	Very short description and purpose of the processing	The EDPS IT collects and uses personal data to support the production of digital certificates attesting to the identity of the holder (the data subject). Possession of the digital certificate counts as proof of identity for the purpose of authentication in the Case Management System (CMS) application and for signing documents in electronic form, in accordance with the EDPS Acceptable Use Policy for electronic signatures for these particular digital certificates. In order for digital certificates to fulfil the aforementioned functions, the system must record information on the identity of the natural persons to whom certificates are issued. A public-key infrastructure (PKI) is used in the EDPS to identify and authenticate the person to whom the keys and certificates are issued. PKI is a system for facilitating the secure electronic transfer of information. In the EDPS, the PKI infrastructure maintained and managed by the EDPS, Technology and Privacy Unit, Digital Transformation Sector, is called "EJBCA" and the digital certificates produced are known as "CMS certificates". This PKI open source software and deployed in a Linux virtual server hosted at the European Parliament (EP), in one of the EP's private networks. It is accessible only to the EDPS staff. The software is completely stand-alone and does not establish any connection to any resource or server outside the EP's network. As mentioned above, the use cases for these digital certificates are the authentication in CMS and the signature of documents in electronic form, in accordance with the EDPS Acceptable Use Policy for electronic signatures. Every EDPS staff member is issued a CMS certificate upon joining the institution.
8.	Description of categories of persons whose data the EDPS processes and list of data categories	To generate the digital certificates, personal data of EDPS staff is processed. Personal data included in the system by the EDPS staff or automatically (e.g. for email addresses):

Nr.	Item	Description
		• Email address • Organisational entity
9.	Time limit for keeping the data	The personal data of EDPS staff members are actively processed in EJBCA for the duration of their employment relation with EDPS, for digital certificate renewal or re-issuing. Once a staff member leaves the EDPS, the digital certificate is revoked, so that it can no longer be used to access CMS; the email address of the staff member remains in EJBCA, embedded in the expired and / or revoked digital certificates, but cannot be further used for other activities. The overall time limit for which the expired and revoked certificates are kept in EJBCA is 30 years, which is the time frame in order to keep an exhaustive and secure Certificate Revocation List.
10.	Recipients of the data	N/A
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	There are no transfers outside of EU/EEA.
12.	General description of security measures, where possible.	The production environment is accessible on the basis of a username and a password, associated with a user (end entity), created for each user for the purpose of generating / renewing and downloading its own digital certificate. The digital certificate is delivered in the form of a "digital ID" file that needs to be imported onto the user's system in order to be used. This file is protected with a password and can only be imported if the user inputs it during the installation. The passwords are randomly generated by the EJBCA system and a new one is created for each time a certificate is manually issued by the EDPS IT and for each time the certificate renewal is triggered by the user. The password for accessing the EJBCA system is the same as the password for installing the digital

Nr.	Item	Description
		certificate. It (the password) is sent only to the user and the user can download the certificate only once. The digital certificate creation is triggered by the user and is not stored in the EJBCA system nor can it be recovered (re-issued with the same digital key) by the EJBCA system.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	DPN available internally.