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
	Creation of private keys using Uanataca Registry System	
1.	Last update of this record	**12-10-2023**
2.	Reference number	77
3.	Name and contact details of controller	European Data Protection Supervisor (EDPS) and Uanataca Trust Service Provider are joint controllers for this processing activity. **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	dpo@edps.europa.eu

Nr.	Item	Description
	of DPO	
5.	Name and contact details of joint controller (where applicable)	**Uanataca Trust Service Provider** **Email:** info@uanataca.com
6.	Name and contact details of processor (where applicable)	
7.	Very short description and purpose of the processing	Uanataca provides technology services to the EDPS, in order for the EDPS to be constituted as the Registration Authority within Uanataca's Public Key Infrastructure or so that UANATACA directly issues qualified certificates for the EDPS staff, upon demand of the EDPS. Under the scenario where the EDPS is constituted as the Registration Authority within Uanataca's Public Key Infrastructure, Uanataca designates, on a non-exclusive basis, the EDPS as Registration Authority, for the latter to act as Uanataca's intermediary in providing the EDPS staff with electronic certification services. The EDPS IT, serving as the Registry Operator, processes personal data to support the production of digital certificates attesting to the identity of the holder (the data subject). Two main types of certificates can be produced, with different purposes: • Advanced S/MIME (email) certificates • Qualified certificates Possession of the qualified digital certificate counts as proof of identity for the purpose of signing documents in electronic form, in accordance with the EDPS Acceptable Use Policy for digital signatures. Possession of the advanced S/MIME certificates counts as proof of identity for the purpose of guaranteeing the authenticity and confidentiality of electronic mails, in accordance with the EDPS Acceptable Use Policy for the Exchange of Encrypted Email Messages. In order for the digital certificates to fulfil the aforementioned functions, the system must record information on the identity of the natural persons to whom certificates are issued. In addition, there must be a procedure to validate this identity information against the physical person. A public-key infrastructure (PKI) is used to

Nr.	Item	Description
		create and manage the digital certificates. PKI is a system for facilitating the secure electronic transfer of information. The PKI used for the production of these digital certificates is maintained and managed by Uanataca. As mentioned above, the applications include the encryption and the signature of electronic messages. The digital certificates used for this purpose are a tool which allows staff to exchange encrypted e-mail messages within the EDPS or with third parties. The exchange of encrypted messages must comply with the EDPS Acceptable Use Policy for the Exchange of Encrypted Email Messages. Every EDPS staff member can request one advanced S/MIME certificate. One qualified certificate will be issued to each of the following EDPS Managers: • EDPS Supervisor • Secretary-General • Head of the EDPS HRBA Unit • Head of the EDPS Finance Sector
8.	Description of categories of persons whose data the EDPS processes and list of data categories	In order to generate the digital certificates, personal data of the following data subjects will be processed: • EDPS staff The following personal data categories will be processed • First and last name; • Date of birth; • ID card number; • Copy of ID card; • Professional email address; • Professional address; • Professional phone number; • Job position

Nr.	Item	Description
9.	Time limit for keeping the data	The personal data of EDPS staff members are kept in a registry maintained by the EDPS IT and actively processed in the Uanataca Registry and PKI, for the duration of the user's possession of the digital certificates, for the digital certificate issuing and renewal. Once a staff member renounces the use of the digital certificate or leaves the EDPS, the digital certificate is revoked so that it can no longer be used; the personal data of the staff member remains in the EDPS registry and Uanataca's PKI registry for the duration of the retention period, which is 15 years. The retention period is the minimum required by law for an eIDAS trusted service provider.
10.	Recipients of the data	Uanataca processes the aforementioned personal data of EDPS staff members, with the exception of the copy of ID card, to issue certificates for the EDPS staff members.
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 to the EDPS IT, acting as Registry Operator, on the basis of a password protected electronic certificate, for the purpose of creating and approving certificate requests and revoking certificates. The S/MIME certificate is generated by the user and 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 chosen by the user and can only be imported if the user inputs it during the installation. The qualified certificate (qualified signature) is generated by the EDPS IT, acting as Registry Operator, and delivered in a USB/Bluetooth secure token. The qualified certificate (advanced signature) is generated by the user and 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 chosen by the user and can only be imported if the user inputs it during the installation. The EDPS IT will keep a secure backup of all the certificates delivered in the form of a "digital ID" file. The certificates are not stored, nor can they be recovered (re-issued with the same digital key) by the PKI.

Nr.	Item	Description
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	Data Protection Notice available internally.