Eurojust record of processing activity

Record of processing personal data activity, 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

Part I –Article 31 Record (this part is publicly available)

Nr.	Item	Description
Dencrypt Connex Service – Secure Mobile Communication App		
1.	**Last update of this record**	
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	
3.	**Name and contact details of controller** [Use functional mailboxes, not personal ones, as far as possible - this saves time when updating records and contributes to business continuity.]	Head of Information Management Unit (mchanfreau@eurojust.europa.eu)
4.	**Name and contact details of DPO**	dpo@eurojust.europa.eu
5.	**Name and contact details of joint controller (where applicable)** [If you are jointly responsible with another EUI or another organisation, please indicate so here (e.g. two EUIs with shared medical service). If this is the case, make sure to mention in the description who is in charge of what and whom people can address for their queries.]	N/A
6.	**Name and contact details of processor (where applicable)** [If you use a processor (contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-	Frontex Head of Digital Services Unit HoU.DIG@frontex.europa.eu

Nr.	Item	Description
	employment medical checks).]	
7.	**Purpose of the processing** [Very concise description of what you intend to achieve; if you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).]	The purpose of the processing is to provide a secure and encrypted communication app for mobile phones for voice calls and message exchanges between designated JITs members, Eurojust, and Frontex.
8.	**Description of categories of persons whose data are processed and list of data categories** [In case data categories differ between different categories of persons, please explain as well.]	**Mobile App users** 1) First name 2) Last name 3) Email account used to register in the app 4) Organisation name 5) Address book name (e.g. a descriptive text of who the user can communicate to) 6) User device IP address The voice calls content and text messages content exchanged between users are not kept at central server. Technical log contains information whether communication setup between parties took place or is being initiated (user device IP, email account)
9.	**Time limit for keeping the data** [Indicate your administrative retention period including its starting point; differentiate between categories of persons or data where needed (e.g. in selection procedures: candidates who made it onto the reserve list vs. those who did not).]	Administrative identification data for all users is kept for the time when access to Dencrypt is valid. Validity period is regulated by issuance of a service request directed to DIG Service Desk. Data in backup and technical log will be held for 11 years, according to Frontex Data Management Policy. (The voice calls content and text messages content exchanged between users are not covered by the backup)
10.	**Recipients of the data** [Who will have access to the data within Eurojust? Who outside Eurojust will have access? Note: no need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).]	1) Frontex and Eurojust Back Office users having access to the Dencrypt Connex mobile application have access to contact information within the assigned addressbook (searchable address book, seeing other Frontex and non Frontex personnel identified by first and last name / assigned address book only). 2) Dencrypt system Frontex administrators and Eurojust Back Office to manage service. 3) App users have access only to an address book with

Nr.	Item	Description
		the list of contact they can exchange messages with (point 5) of section 8) Dencrypt system administrators in Frontex and Eurojust, share also technical logs with Dencrypt – Denmark – technical support. These logs do not include any users related data and only contain technical information.
11.	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** [E.g. processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult DPO for more information on how to ensure safeguards.**]**	No
12.	**General description of security measures, where possible.** [Include a general description of your security measures that you could also provide to the public.]	End to end encryption between parties is in place for both text messages and calls. The system is hosted in FRONTEX premises, in a dedicated infrastructure for Eurojust.
13.	**For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:** [While publishing the data protection notice is not strictly speaking part of the record, doing so increases transparency and adds no administrative burden, since it already exists.]	https://www.eurojust.europa.eu/document/data-protection-notice-processing-personal-data-context-use-dencrypt-connex-app