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	
The processing of personal data in the context of electronic identification of Eurojust's staff members by using Simple Electronic Signature (SES) to electronically sign documents pertaining to the administrative processes of Eurojust.		
1.	**Last update of this record**	**25/04/2024**
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 IM Unit ICTProjects2@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.	**1/ 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-employment medical checks).] **2/ Persons processing under the authority of the controller according to Article 30 of Regulation** (EU) 2018/1725 ("internal processors")	1/ Ascertia: provider of the digital signature workflow engine and of simple electronic signature (SES). Point of Contact can be reached via E: dpo@ascertia.com. The purpose is to assist Eurojust to perform relevant activities, giving the best user experience and to fulfil Eurojust business continuity needs for the signature solution. The contract has been signed between Eurojust and Ascertia. 2/ Duly authorised staff members of Digital Infrastructure Sector (DIS), IMU.
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 of personal data in the context of using the digital signature workflow engine and simple electronic signature (SES) software provided by Ascertia is to create, validate the electronic signature on electronic documents in line with the eIDAS Regulation. More specifically, **for Eurojust to ensure:** • Compliance with Eurojust eSignature policy (i.e. which user is entitled to sign with which e-signature type). • Access the SigningHub for signature workflow management, • Creation and management of the user accounts on SigningHub e-platform and their access rights, • Issuing the SES for signing the electronic documents;

Nr	Item	
		- Support to the users when there is a need to analyse and resolve technical issues (e.g. by analysing the user action, console or application logs). **For Ascertia: Ascertia** does not process any data, but might receive logs to support Eurojust in the investigation of bugs and other technical issues. The logs will be anonymised before being sent to Ascertia. For when the phase 2 will be launched, i.e. for when the Qualified Electronic Signature (QES) usage in Eurojust will be introduced, the current record of processing activity as well as any other related document will be reviewed and updated accordingly.
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.]	Data subjects with Eurojust Active Directory (AD) accounts for the use of the Signing Hub (SH) Enterprise platform (SES): 1. Enterprise Admin role(s): a Eurojust Signing Hub Enterprise account owner (Postholders belonging to the Digital Infrastructure Sector, DIS and the Information Management Unit, IMU). 2. Enterprise User role(s): all Eurojust users entitled to use the Signing Hub supported electronic signatures. Data categories collected for the data subjects above 1) and 2): - Name and surname (mandatory), populated from Active Directory (AD), stored on Eurojust premises, including middle name (if used), - Job title or role (mandatory), populated from Active Directory (AD), stored on Eurojust premises, - Eurojust Email address (mandatory), populated from Active Directory (AD), stored on Eurojust premises, - Time and date of accessing the SigningHub enterprise platform. These logs are differentiated into: Signing Hub interface and Eurojust server, stored on Eurojust premises. The above listed data are stored in Eurojust premises and managed exclusively by Eurojust / DIS authorised post-holders. Ascertia, being the software components provider, can receive only anonymised logs without personal data from on premise EJ ICT Team (DIS sector) on support cases on a case by case basis where strictly necessary in resolving the technical issues that requires the services from Ascertia.
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).]	- The Identity Services Engine (ISE) as an access control service – retention period is 5 days on ISE appliances itself. The logs however are forwarded to SPLUNK where they are kept for the duration of 1 year. - Policy on User Account Management – Signing Hub user data retrieved from Active Directory (AD), after the user account is no longer active, is retained for 7 years period in AD. - Eurojust audit log retention period is 1 year, as defined by the POLICY – Audit log, as approved by the AD 08/03/2018. Ascertia does not store any logs automatically only if and

Nr	Item	
		when they are sent by the Eurojust EJ ICT Team (DIS sector), always anonymised with request to support in resolving a technical issue. These logs are cleared periodically, after technical issue has been fixed. The logs are recorded in Ascertia CRM system for support purposes and are routinely cleared after a period of two years from their creation. The CRM database is located in Stockholm, Sweden. Logs reported to the support email address support@ascertia.com are stored on Office 365 exchange mailbox, hosted in the United, Kingdom.
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).]	Outside Eurojust: Ascertia will receive only the anonymised logs necessary to support Eurojust upon request of the EJ ICT Team (DIS sector). The data will be: 1. recorded on Salesforce system used for client relationship management (CRM). The database is located in Stockholm, Sweden 2. stored on Office 365 exchange mailbox if reported via support@ascertia.com email. The data is hosted in the United Kingdom, UK.
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.]	Yes, to United Kingdom, UK. The UK is the only destination and other sub processor is Microsoft. In limited cases, the Eurojust ICT Team (DIS sector) might sent a system specific technical support request and anonymized logs via general email to Ascertia's technical support team located in Pakistan. All information in these exchanges is fully anonymized.
12.	**General description of security measures, where possible.** [Include a general description of your security measures that you could also provide to the public.]	**Eurojust**: all data are stored on Eurojust premises in physically secure data centers. Eurojust's data centers are protected with security controls and accessible only by verified and authorised people. Eurojust has also several layers of protection in place and dedicated systems to detect and block unauthorized and/or malicious traffic. **Ascertia**: Logs (anonymised) received from Eurojust for technical investigations are stored on Ascertia database employing encryption mechanisms. This encryption ensures that data remains protected from unauthorized access or interception, thereby enhancing the confidentiality and integrity of stored information. The database operates within the European Union* and is protected with security controls to mitigate risks and prevent unauthorized access to the logs database. These controls include measures such as role-based access controls, authentication mechanisms, intrusion detection systems, and regular security assessments to identify and address vulnerabilities. * Salesforce – is Ascertia's Client Management System (CRM). It stores all technical issue data which are reviewed by Ascertia technical team. It includes email copies and their attachments. The data base is located in Stockholm, Sweden. * If anything is sent over support@ascertia.com it will be stored in a temporary Office 365 exchange mailbox hosted in the United Kingdom, UK.

Nr	Item	
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.]	Data Protection Notice https://www.eurojust.europa.eu/document/data-protection-notice-processing-personal-data-context-use-signing-hub-e-signature