EUROJUST
The European Union's Judicial Cooperation Unit
P.O. Box 16183 – 2500 BD The Hague • The Netherlands

# DATA PROTECTION NOTICE

## *For processing of personal data in the context of the use of the Signing Hub, e-Signature platform*

As Eurojust collects and further processes personal data, it is subject to *Regulation (EU) 2018/1725 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* ('the Regulation').

The following information is provided as per Articles 15 of the Regulation.

### 1. Context of the processing activity and Controller

Collection and processing of the administrative personal data required for the functioning of the Eurojust Signature platform is under the responsibility of the Controller, who is the Head of the Information Management Unit and can be contacted at ICTProjects2@eurojust.europa.eu

### 2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?

#### *Purpose of the processing*

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.

The data collected by the signature solution are needed for Eurojust to:

- 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,
- Create and manage the user accounts on SigningHub e-Signature platform and their access rights,
- Issue the SES for signing the electronic documents,
- Support the users when there is a need to analyse and resolve technical issues (e.g. by analysing the user action, console or application logs).

Ascertia is a provider of the digital signature workflow engine and of simple electronic signature (SES), it is a Signing Hub e-signature platform software components provider. It does not process any personal data, but might receive technical logs to support Eurojust in the investigation of bugs and issues. The logs are fully anonymised before being sent to Ascertia.

#### *Types of personal data*

The below listed personal data is stored in Eurojust premises and managed exclusively by Eurojust Information Management Unit / Digital Infrastructure Sector (DIS) authorised post-holders. The data is collected to allow access and usage of the signature solution.

The following **categories of personal data** are processed in the context of the above mentioned processing activity:

- User name,
- User Surname,
- User Middle name, if used,
- User Job title or role,
- User's Eurojust email address,
- User access time and date.

***Legal basis***

The processing is necessary for the performance of tasks carried out by Eurojust as foreseen in Eurojust Regulation (Article 2), Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, financial regulations and rules, other applicable rules, also in line with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, eIDAS.

***Technical means***

Your personal data are imported in the system by automatic synchronisation from Active Directory (AD). The data are fully stored on premises and the access is limited to authorised users only (as listed in Section 3.)

**3. Who has access to your personal data and to whom is it disclosed?**
For the purpose detailed above, access to your personal data is available to the:

- Eurojust User Support who can see the data in Active Directory (AD),
- Digital Infrastructure Sector (DIS) who can see the data both, in AD and on Signing Hub (SH), the on premise signing platform,
- Ascertia Technical Support Department and Customer Success Teams are provided only with anonymised logs, with no personal data, under the supervision of Eurojust.

**4. How do we protect and safeguard your information?**

At Eurojust appropriate technical and organisational measures are in place to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be processed, in compliance with the Eurojust best practices. 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.

Ascertia stores the logs (fully anonymised) received from Eurojust, and used for technical investigations, on its database employing encryption mechanisms. The anonymised logs stored on CRM Salesforce are hosted within the European Union in Stockholm, Sweden and the Salesforce data

center protected with security controls to mitigate risks and prevent unauthorized access to the logs database.

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. Such information is fully anonymized and is shared to support@ascertia.com email. Information exchanged via this email is hosted in United Kingdom (UK).

### 5. How can you verify, modify or delete your information?

You have the right to access your personal data and to relevant information concerning how we use your personal data. You have the right to request rectification of your personal data. You have the right to ask that we delete your personal data or restrict its use. Where applicable, you have the right to object to our processing of your personal data, on grounds relating to your particular situation. Where applicable, you have the right to your data portability. We will consider your request, take a decision, and communicate it to you. For more information, please see Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. Please note that in some cases restrictions under Article 25 of Regulation (EU) 2018/1725 may apply (see College Decision 2020-04 of 15 July 2020 on internal rules concerning restrictions of certain data subjects' rights in relation to the processing of personal data in the framework of activities carried out by Eurojust, available in the Eurojust website here).

To exercise your rights, please contact usersupport@eurojust.europa.eu

### 6. How long do we keep your personal data?

All data is kept on Eurojust premises. The retention periods are as follows:

- The Access Control Service system, an Identity Services Engine, keeps the logs for 5 days.
- After the logs are forwarded to SPLUNK and kept for 1 year, which in compliance with Eurojust log retention policy.
- User account data as they appear on Signing Hub e-signature platform are retrieved from Active Directory. This data is kept in the system (on premise) as long as the user(s) has an active account. After the post-holder(s) leaves Eurojust, the account will be disabled, and will be deleted after 7 years, as per Eurojust Policy on User Account Management.
- The Audit Logs are kept for 1 year, as defined by the Audit Log policy.

Ascertia does not store any logs automatically, only if and when they are sent by the Eurojust EJ ICT Team (DIS sector), always anonymised with request to support in resolving a technical issue. In such a case the logs stored on CRM Salesforce are retained for a period of two years from their creation.

### 7. Contact information

In case of queries regarding the processing of personal data you may also contact the Data Protection Officer of the Eurojust (dpo@eurojust.europa.eu).

### 8. Recourse

You have the right to lodge a complaint to the European Data Protection Supervisor via the email edps@edps.europa.eu or https://edps.europa.eu/data-protection/our-role-

supervisor/complaints_en if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data.