



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
		Filing and sorting of digital files of Eurojust staff (Temporary Agents and Contract Agents) and SNEs. The implementation started in 2022 with the testing of the system and the go-live is planned in Q2 2023.
1.	Last update of this record	04/07/2023
2.	Reference number	HRU-18 (July 2023)
3.	Name and contact details of controller	Head of Human Resources Unit hohrconfidential@eurojust.europa.eu
4.	Name and contact details of DPO	dpo@eurojust.europa.eu
5.	Name and contact details of joint controller	N/A
6.	Name and contact details of processor	HR Admin staff, in the Human Resources unit, who file, by sorting and categorising, digital files belonging to a staff member' and SNEs' personal files. Dedicated staff in DG HR and DIGIT providing troubleshooting support, upon request from Eurojust. HR-NDP-INTERINSTITUTIONAL@ec.europa.eu Dedicated staff in the Paymaster's Office processing Staff members' salaries and producing the Payslips. PMO-SALARIES-BASIC-SLA@ec.europa.eu
7.	Purpose of the processing	Data is processed with the purpose of electronically managing the personal files of Eurojust staff (Temporary and Contract agents), and SNEs, in compliance with the Personal Files Policy. Once categorised and filed, the files belonging to a staff member' or SNE's digital personal file can be published (by the Human Resources Unit staff member processing the data), becoming

Nr.	Item	Description
		<p>available for consultation via SYSPER.</p> <p>Likewise, payslips are processed and published by the PMO and become available for the staff member via SYSPER – not applicable for SNEs.</p>
11.	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p>	No
12.	<p>General description of security measures, where possible.</p>	<p>The data are stored at the Commission's Computing Centre in Luxembourg and are therefore protected by the numerous security measures implemented by the Directorate-General for Informatics to protect the integrity and confidentiality of the Institution's electronic assets. The European Commission's data centre compliance includes the following certifications: ISO 14001, ISO 22301, ISO 27001, ISO 50001, ISO 9001, PCI DSS, PFS, Tier Rating Compliant : Tier IV, Uptime Institute rating: Tier IV.</p> <p>Access to personal data is protected by the management of access rights which are strictly limited to the principle of "need to know" according to the tasks assigned to access holders. The access rights are linked to the 'Purpose' stated in chapter 7 and assigned to user groups mentioned in chapter 6. The login and password are managed by the European Commission's Common Authentication Services (EU Login).</p> <p>Accesses, as well as any modifications performed on the data, are logged to ensure traceability of these actions. These logs include who modified the data, when, and what modifications were done, including previous values and new values.</p> <p>The overall responsibility for the implementation of the data protection rules rests with the "controller", i.e. the Head of Human Resources Unit. It is the "controller" who determines who has what access right(s) to which part(s) of the system.</p>
13.	<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</p>	<p>Data Protection Notice</p>

