

DATA PROTECTION NOTICE

regarding the processing of personal data in the context of whistleblowing proceedings

1. Context and Controller

As Eurojust collects and further processes personal data in the context of whistleblowing proceedings, 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.

Collection and processing of personal data in the context of whistleblowing proceedings are under the responsibility of the Controller, who is the Administrative Director of Eurojust and can be contacted at adconfidential@eurojust.europa.eu.

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

Legal basis of the processing

The legal bases for the processing activities are:

- Article 5(1)(b) of Regulation EU 2018/1725: processing is necessary for compliance with a legal obligation to which the controller is subject;
- Articles 22a and 22b of the Staff Regulations
- College Decision 2019-02 on Eurojust guidelines on whistleblowing by members of its staff, Staff Regulations (Art 22(c))
- AD Decision 2017-48 adopting Eurojust's Guide on Ethics and Conduct of 21 September 2017
- College Decision of 13 July 2004 on the implementation of Regulation (EC) No 1073/1999 concerning investigations conducted by OLAF in accordance with Article 38(4) EJD
- Eurojust Decision on general implementing provisions on the conduct of administrative inquiries and disciplinary procedures of 23 September 2013.

Purpose of the processing

The purpose of the processing is to carry out the procedure defined by the College Decision 2019-02 on Eurojust guidelines on whistleblowing by members of its staff.

Technical means

Technical measures include storing the files electronically in a restricted area of the Document Management System. All processing operations are carried out pursuant to existing policies describing access control to different Eurojust applications. Limited amount of staff with a legitimate 'need to know' for the purposes of this processing operation have access to your

personal data. Organisational measures include the use of locked closets, confidential settings in the emails and printing with badging.

Types of personal data

The data which will be used only for that processing are the relevant documents necessary to manage the whistleblowing procedure:

- surname and first name (should the whistle-blower chooses to disclose it)
- e-mail address (should the whistle-blower chooses to disclose it)
- date and signature (should the whistle-blower chooses to sign the report)

The whistleblowing report where all unnecessary data will be erased

3. To whom is your personal data disclosed?

The recipients of the data depend on the option that a staff member chooses to report a serious irregularity and it could be:

Internal whistleblowing

- the staff member's immediate superior
- the Administrative Director
- the President of the College
- OLAF

In any case, the recipient of the information is in turn obliged to transmit the information thus received without delay to OLAF.

External whistleblowing

Upon receipt of the information reported internally, OLAF or Eurojust must give the whistle-blower within 60 days of receipt of the information an indication of the period of time that it considers reasonable and necessary to take appropriate action. If no action is taken within that period of time, or if the whistle-blower can demonstrate that the period of time set is unreasonable in light of all the circumstances of the case, he or she may make use of the possibility of external whistleblowing by bringing his concerns to the attention of the President of either the Commission, the Council, the Parliament or the Court of Auditors, or to the Ombudsman.

In case the Administrative Director decides to launch an administrative inquiry, data may be disclosed to the Disciplinary Board, the investigator, the staff member responsible for the inquiry and other persons involved in the inquiry.

If the staff member concerned contests the disciplinary decision, the disciplinary file may be referred to the Court of Justice of the European Union. Data may be sent to the Ombudsman, if the staff member concerned addresses a complaint.

In addition, data recipients can also be the HR unit contact point to provide confidential and impartial guidance on, for example, whether the information in question is covered by the whistleblowing rules, which reporting channel may best be used for the information concerned, and which alternative procedures are available if the information concerned does not qualify for whistleblowing ('signposting').

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

You have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict their use. You have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. 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.

If you wish to exercise your data subject rights, any such request should be directed to the Administrative Director of Eurojust at adconfidential@eurojust.europa.eu.

You may also contact the Data Protection Officer at Eurojust at dpo@eurojust.europa.eu.

5. How long do we keep your personal data?

Upon the closing of an initial investigation led by Eurojust, the data gathered to build the investigation will either be sent to OLAF if it concerns fraud or if not relating to fraud, dealt with through the appropriate channels within Eurojust.

If a case is sent to OLAF and an investigation is opened, there is no need for Eurojust to keep the information for a longer period and Eurojust will delete the information without delay.

For files on the basis of which an administrative inquiry or disciplinary procedure is opened by Eurojust, the information should be kept for a maximum of 10 years after the closure of the case in order to allow a harmonised application of the Staff Regulations.

When the investigation has dismissed a report of whistleblowing, the data gathered to build the investigation will be retained for a period of 2 months after the final decision has been issued to all the parties involved.

6. Contact information

You have the right to access, rectify or erase or restrict the processing of your personal data or, where applicable, the right to object to processing or the right to data portability in line with Regulation (EU) 2018/1725.

Any such request should be directed to the Controller, by using the following email address:

adconfidential@eurojust.europa.eu, and by explicitly specifying your request.

You may also contact the Data Protection Office of the Eurojust (dpo@eurojust.europa.eu).

7. Recourse

You have the right to lodge a complaint to the European Data Protection Supervisor (https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en) if you consider that your rights under the Eurojust Regulation and/or Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data or seek a judicial remedy before the Court of Justice.