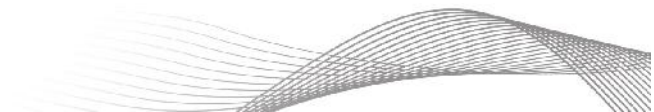# EDPS record of processing activity

Record of EDPS activities processing personal data, 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.

| Nr. | Item | Description |
|---|---|---|
| | | **Whistleblowing procedure** |
| 1. | Last update of this record | **26-11-2018** |
| 2. | Reference number | **07** |
| 3. | Name and contact details of controller | European Data Protection Supervisor (EDPS) <br> **Postal address**: Rue Wiertz 60, B-1047 Brussels <br> **Office address**: Rue Montoyer 30, B-1000 Brussels <br> **Telephone:** +32 2 283 19 00 <br> **Email:** edps@edps.europa.eu <br><br> Responsible department or role: <br> *HRBA* <br><br> Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759 |
| 4. | Name and contact details of DPO | edps-dpo@edps.europa.eu |
| 5. | Name and contact details of joint controller (where applicable) | N/A |
| 6. | Name and contact details of processor (where applicable) | N/A |

| Nr. | Item | Description |
|---|---|---|
| 7. | Very short description and purpose of the processing | The purpose of the processing is to carry out the procedure defined by the EDPS decision of 14 June 2016 adopting rules regarding whistleblowing by members of its staff. |
| 8. | Description of categories of persons whose data the EDPS processes and list of data categories | The rules apply to every staff member working in the EDPS's Secretariat, irrespective of their administrative position or status, involved in a wistleblowing episod.

It can also apply to every person who enters into a contract with the EDPS (Article 17 of the EDPS decision).

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

- surname and first name
- personal number
- assignment
- office address & tel
- office e-mail address
- date and signature

The whistleblowing report where all unnecessary data will be erased |
| 9. | Time limit for keeping the data | . The time for which the complaint files may be kept is the following: upon the closing of an initial investigation led by the EDPS, 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 the EDPS. **If a case is sent to OLAF and an investigation is opened, there is no need for the EDPS to keep the information for a longer period**. In cases OLAF decides not to start an investigation, the EDPS will delete the information without delay. Files on the basis of which an administrative inquiry or disciplinary procedure is opened by the EDPS, the information should be kept in line with the retention periods foreseen for those files. . **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.** |

| Nr. | Item | Description |
|---|---|---|
| 10. | Recipients of the data | The recipients of the data are:<br>- the Human Resources Unit, the officer in charge of personal files.<br>- the AIPN (the EDPS Director)<br>- the Supervisor where necessary<br>- the Ethics officer where necessary for guidance and support<br>- OLAF where needed<br>- the EPDS DPO, the IAS, the Court of auditors and the Court of Justice where necessary |
| 11. | Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards? | No |
| 12. | General description of security measures, where possible. | - Paper files stored in locked cupboard (in a specific paper file for background information and secure USB key for electronic files). The final decision will be filed in the personal file in Sysper and paper version. The security measures will be adapted once a new information security risk assessment is conducted. |
| 13. | For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice: | *Link to data protection notice* |