

# GUIDELINES ON WHISTLEBLOWING

## Record of processing activity

|  |  |
|--|--|
| Title  | Guidelines on Whistleblowing   |
| Name and contact details of controller       | ENISA, Policy Office, po@enisa.europa.eu   |
| Name and contact details of DPO              | dataprotection@enisa.europa.eu   |
| Name and contact details of Joint Controller | N/A  |
| Name and contact details of processor        | N/A  |
| Purpose of the processing                    | The purpose of the processing operation is to enable the reporting of fraud, corruption or other serious professional wrongdoing in ENISA. This requires establishing reporting channels for whistleblowers, managing and following-up reports, and ensuring protection and adequate remedies for whistleblowers. Articles 22(a), 22(b) and 22(c) of the Staff Regulations, as well as the Conditions of Employment of Other Servants of the European Union provide the rules on whistleblowing.   |
| Description of data subjects                 | Anyone working at ENISA, including statutory staff members, seconded national experts, trainees and interims. Depending on the case, the data subject may be a whistleblower, an alleged wrongdoer, a witness or third party.  |
| Description of data categories               | Personal data relating to any person implicated in a whistleblowing report, including potentially data on suspected offenses, offenses, criminal convictions and security measures, as well as data on professional conduct and behaviour.<br><br>Special categories of data may appear in an ad-hoc basis in the context of a whistleblowing report. In such cases, any information that is not clearly of interest or relevance to the allegations will be immediately deleted and not further processed.  |
| Time limits (for the erasure of data)        | Different conservation periods apply depending on the information in the report and how the case is dealt with.<br><br>Firstly, personal information that is not relevant to the allegations should not be further processed.<br><br>Secondly, when an initial assessment is carried out but it is clear that the case should not be referred to OLAF or is not within the scope of the whistleblowing procedure the report will be deleted as soon as possible. In any case, personal information will be deleted no later than two months of completion of the initial assessment.<br><br>Thirdly, if it is clear after the initial assessment that a report should be transferred to OLAF, ENISA will carefully monitor what actions OLAF takes. If OLAF starts an investigation, it is not necessary for ENISA to keep the information for a longer period. In case OLAF decides not to start an investigation, the information should be deleted without delay. |

|   |  |
|---|--|
|   | (Point 9 of EDPS guidelines on whistleblowing of 17/12/2019).  |
| Data recipients                         | <p>Recipients include specific persons within ENISA (Heads of Unit, Heads of Department, the Executive Director) to whom a whistleblowing report is submitted. They may also involve other persons within ENISA who are directly or indirectly implicated in a whistleblowing case.</p> <p>External recipients include primarily OLAF. In some cases a whistleblowing report might need to be transmitted to other recipients, such as judicial authorities, in the course of a disciplinary or other procedure.</p> |
| Transfers to third countries            | N/A  |
| Security measures - General description | Clearly defined reporting channels, as well as roles and responsibilities; access based on need-to-know principle; security of electronic communication channels; security of paper-based records; access logs; strict retention periods; training of staff.   |
| Privacy statement                       | Available on intranet for all ENISA staff members.   |

