



Record¹ of processing activities regarding a whistleblowing procedure at the EIT

Nr	Item	Description
1	Reference number	DPO-56
2	Name of the data controller, the data protection officer and processor ² , if applicable and contact details	<p>The data controller is the EIT Director.</p> <p>Contact e-mail: eit-antifraud@eit.europa.eu</p> <p>Contact e-mail of the Data Protection Officer: EIT-DPO@eit.europa.eu</p>
3	Purposes of the processing	<p>The purposes of processing personal data are:</p> <ul style="list-style-type: none"> - to enable reporting of fraud or irregularities via established whistleblowing channels; - to identify the whistleblowers aiming to avoid the abuse of the procedure and ensure further confidentiality of the whistleblower; - to analyse and assess the acquired information regarding potential irregularity or fraud in order to decide on the further actions that have to be taken; - to inform whistleblower about the time needed to take appropriate action.

¹ In line with 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

² For more information., please see below (categories of data recipients).



		<p>Please be informed that in case EIT decides to take further actions and transmit the received information to OLAF, your data will be processed according to the Privacy Statement regarding management of OLAF cases.</p> <p>Data processing operations include collecting, recording, organization, storage, consultation, use, disclosure by transmission, erasure, and destruction of personal data.</p>
4	Categories of data subjects	The data subjects are persons who reported irregularity or fraud (whistle-blowers) and alleged wrongdoers, third parties, and witnesses, mentioned in the whistle-blower's report.
5	Categories of the personal data processed	<p>The following types of personal data may be processed for the above-mentioned purposes in accordance with the Regulation:</p> <ul style="list-style-type: none"> - identification and contact information of the whistle-blower (name, surname, phone number/email address); - any relevant information mentioned in the report describing the relevant circumstances of the case, facts, and evidence, such as <ul style="list-style-type: none"> • personal data including name and contact information of the suspected entities/persons; • reasons for suspicions of fraud or irregularity; • identification of the procedure (contract/procurement or recruitment, etc); • references and dates of call for proposals/call for tender/etc; • amounts involved; • relations between the reporting person and the suspected entities/persons; • risks that further operations are concerned; • precautionary measures that are taken; • the sources of acquired information, etc. <p>The personal data that is not relevant to the allegations will not be further processed.</p>



6	<p>Categories of data recipients</p>	<p>Within the EIT:</p> <p>The personal data of data subjects are processed by the EIT authorized staff depending on the channel for reporting chosen: line manager (Head of Unit/Department), Anti-Fraud Coordinator, the EIT Director, Chairman of the Governing Board or the European Anti-Fraud Office (OLAF); and the Head of Administration Unit in case of ‘staff matters’³.</p> <p>The data collected will only be disclosed to the absolute minimum of persons involved on a need-to-know basis in particular to Head/s of Units and other advisory functions who may be consulted in order to assess the reported information. Also responsible staff of the Human Resources section and the Legal officer(s) assigned may be involved.</p> <p>Please, be aware that EIT guarantees confidentiality of whistleblower’s identity. This means that whistleblower’s name will not be revealed to the person(s) potentially implicated in the alleged wrongdoings, or to any other person without a strict need to know, unless the whistleblower personally authorises the disclosure of his/her identity or this is a requirement in any subsequent criminal law proceedings. In all other cases, the EIT is committed to keeping the identity of the whistleblower confidential.</p> <p>Within the Commission and other EU institutions/bodies/agencies:</p> <p>Access to your personal data may be given on a need-to-know basis and in compliance with the relevant current legislation for audit control or investigation purposes to the Court of Auditors, Internal Audit Service of the European Commission, and European Anti-Fraud Office (OLAF).</p> <p>Access to the personal data may be granted also to the European Ombudsman and the European Data Protection Supervisor upon request, the General Court, and the European Court of Justice to the extent necessary for handling the review procedure and litigation.</p>
---	---	--

³ e.g. psychological or sexual harassment;



		Personal data of the reporting persons will not be revealed to the person(s) potentially implicated in the alleged wrongdoings, or to any other person without a strict need to know unless the whistle-blower personally authorizes the disclosure of his/her identity, or this is a requirement in any subsequent criminal law proceedings. In all other cases, the EIT is committed to keeping the identity of the whistle-blower confidential.
7	Time limit storage	The EIT keeps your personal data contained in files related to whistleblowing for 2 years. In case the reported information is transmitted to OLAF, your personal data will be stored according to the Privacy Statement on management of OLAF cases.
8	If applicable, transfers of personal data to a third country or to international organization (if yes, the identification of that third country or international organization and the documentation of suitable safeguards)	No
9	General description of the technical and organisational security measures	Technical and organisational measures: access to personal data is restricted to recipients specified above, in particular, all case related documents are stored in dedicated folders on Share Point with restricted access.
10	For more information, including how to exercise rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Please see the privacy statement annexed to the record. Please consult the Data Protection page on the EIT's website: https://eit.europa.eu/who-we-are/legal-framework/data-protection

Signature of the data controller

(Approval is given via a workflow in ARES in place of a handwritten signature)

