RECORD OF PERSONAL DATA PROCESSING ACTIVITY according to Article 31 of Regulation (EU) 2018/1725

Contents
- General information .......................................................................................................................... 1
- Description and Purpose of the Processing ...................................................................................... 2
- Data Subject’s Rights .......................................................................................................................... 2
- Categories of Data Subjects & Personal Data .................................................................................. 3
- Categories of Recipients & Data Transfers .................................................................................... 4
- Automated Decision Making .......................................................................................................... 5
- Retention Period & Security Measures ........................................................................................... 5

General information

Introduction

EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) No 2018/1725 (further referred as the Regulation)¹.

Contact Details of Data Controller(s)

Fausto Parente, Executive Director
Westhafenplatz 1, 60327 Frankfurt am Main, Germany
fausto.parente@eiopa.europa.eu

Contact Details of the Data Protection Officer

Eleni Karatza
Westhafenplatz 1, 60327 Frankfurt am Main, Germany
dpo@eiopa.europa.eu

Contact Details of Processor

EIOPA’s Team/Unit/Department responsible for the processing:
Legal Team

---

¹ 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.
**Description and Purpose of the Processing**

### Description of Processing

Based on the Working Instructions on External Whistleblowing policies, EIOPA reacts to possible violations of EU insurance and occupational pensions law by national competent authorities provided and raised by external whistleblowers.

The whistleblowing reports submitted to EIOPA's facilities may contain information and personal data pertaining to the whistleblower or other persons.

Verification of whistleblowers’ contact details occurs during the initial assessment of the report. Whistleblowers’ personal data are anonymized before the information received is further disseminated.

### Purpose (s) of the processing

- [ ] Staff administration
- [x] Relations with external parties
- [ ] Procurement and accounting
- [ ] Administration of membership records
- [ ] Auditing
- [ ] Information administration
- [x] Other (please give details): Monitoring compliance by competent authorities with EU law in the insurance and pensions sector

### Lawfulness of Processing

- **Legal Basis justifying the processing:**
  
The legal basis for the purpose of processing the data acquired is set out in Article 17a Regulation (EU) No 1094/2010

- **Processing is necessary:**
  
  [x] for the performance of a task carried out in the public interest – Article 5(1)(a) of the Regulation
  
  [ ] for compliance with a legal obligation to which the Controller is subject
  
  [ ] for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  
  [ ] in order to protect the vital interests of the data subject or of another natural person
  
  Or
  
  [ ] Data subject has given his/her unambiguous, free, specific and informed consent

### Data Subject’s Rights

- Information on how to exercise data subject’s rights
Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018.

Data subjects have the right to:

- access their personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate.
- request the erasure of their personal data, as well as object to or obtain the restriction of their processing.
- withdraw their consent to the processing of their personal data at any time in case such processing is based solely on their consent.

For the protection of the data subjects’ privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.

Should data subjects wish to access/rectify/delete their personal data, or receive a copy of them/have it transmitted to another controller, or object to/restrict their processing, please contact Whistle Whistle@eiopa.europa.eu or DPO@eiopa.europa.eu.

**Complaint:**
Any complaint concerning the processing of the data subjects’ personal data can be addressed to EIOPA’s Data Protection Officer (DPO@eiopa.europa.eu). Alternatively, data subjects can also have at any time recourse to the European Data Protection Supervisor (www.edps.europa.eu).

### Categories of Data Subjects & Personal Data

#### Categories of Data Subjects

- [ ] EIOPA permanent staff, Temporary or Contract Agents
- [ ] SNEs or trainees
- [ ] Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other)
  
  If selected, please specify:

  - [ ] Providers of good or services
  - [ ] Complainants, correspondents and enquirers
  - [ ] Relatives and associates of data subjects
  - [x] Other (please specify):
    - Whistleblowers: Any person who voluntarily provides EIOPA with intelligence about possible violations of EU insurance and occupational pensions law.
    - Individuals mentioned in the whistleblowing reports.
### Categories of personal data

<table>
<thead>
<tr>
<th>(a) <strong>General personal data:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The personal data contains:</td>
</tr>
<tr>
<td>☑ Personal details (name, address etc)</td>
</tr>
<tr>
<td>☐ Education &amp; Training details</td>
</tr>
<tr>
<td>☑ Employment details</td>
</tr>
<tr>
<td>☑ Financial details</td>
</tr>
<tr>
<td>☐ Family, lifestyle and social circumstances</td>
</tr>
<tr>
<td>☐ Other (please give details):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) <strong>Special categories of personal data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The personal data reveals:</td>
</tr>
<tr>
<td>☐ Racial or ethnic origin</td>
</tr>
<tr>
<td>☐ Political opinions</td>
</tr>
<tr>
<td>☐ Religious or philosophical beliefs</td>
</tr>
<tr>
<td>☐ Trade union membership</td>
</tr>
<tr>
<td>☐ Genetic or Biometric data</td>
</tr>
<tr>
<td>☐ Data concerning health, sex life or sexual orientation</td>
</tr>
</tbody>
</table>

### Categories of Recipients & Data Transfers

<table>
<thead>
<tr>
<th>Recipient(s) of the data</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Designated EIOPA staff members</td>
</tr>
<tr>
<td>☐ Managers of data subjects</td>
</tr>
<tr>
<td>☐ If selected, please specify:</td>
</tr>
<tr>
<td>EIOPA’s Executive Director, Head of Corporate Affairs Department, Head of Oversight Department, Whistleblowing officer (member of the Legal team), and other EIOPA staff on a need-to-know basis</td>
</tr>
<tr>
<td>☐ Relatives or others associated with data subjects</td>
</tr>
<tr>
<td>☐ Current, past or prospective employers</td>
</tr>
<tr>
<td>☐ Healthcare practitioners</td>
</tr>
<tr>
<td>☐ Education/training establishments</td>
</tr>
<tr>
<td>☐ Financial organisations</td>
</tr>
<tr>
<td>☐ External contractor</td>
</tr>
<tr>
<td>☑ Other (please specify): Other competent EU institutions and bodies, National competent authorities</td>
</tr>
</tbody>
</table>
Data transfer(s)

☑ Within EIOPA or to other EU Institutions/Agencies/Bodies
   If selected, please specify: The EU institution(s), agency or body, that is competent to act upon the information.

☑ To other recipients within the EU (e.g. NCAs): NCA(s) concerned
   If selected, please specify:
   Whether suitable safeguards have been adopted:
   - [ ] Adequacy Decision of the European Commission
   - [ ] Standard Contractual Clauses (SCC)
   - [ ] Binding Corporate Rules (BCR)
   - [ ] Administrative Arrangements between public Authorities (AA)

☐ To third countries
   If selected, please specify:
   - [ ] Whether suitable safeguards have been adopted:
   - Adequacy Decision of the European Commission
   - Standard Contractual Clauses (SCC)
   - Binding Corporate Rules (BCR)
   - Administrative Arrangements between public Authorities (AA)

☐ To international organisations
   If selected, please specify the organisation and whether suitable safeguards have been adopted:
   - Data subjects could obtain a copy of SCC, BCR or AA here:

Automated Decision Making

Automated Decision-making, including profiling

A decision is taken in the context of this processing operation solely on the basis of automated means or profiling:
☒ No
☐ Yes

In case of an automated decision-making or profiling, please explain:

Retention Period & Security Measures

Retention period

2 Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions (europa.eu)]
<table>
<thead>
<tr>
<th>How long will the data be retained?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files which do not lead to the opening of an inquiry will be kept for 2 years.</td>
</tr>
<tr>
<td>Files relating to cases brought before the EU/national courts will be kept for up to 2 years following conclusion of proceedings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ No</td>
</tr>
<tr>
<td>☑ Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical &amp; organisational security measures taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Several technical and organisational measures have been adopted in order to ensure the optimum security of the documents and personal data collected in the context of the procedures described under section “Description and purpose of the processing”.</td>
</tr>
</tbody>
</table>