

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

► Communication For Business Continuity Purposes

Contents

General information.....	1
Description and Purpose of the Processing	2
Data Subject's Rights.....	3
Categories of Data Subjects & Personal Data	3
Categories of Recipients & Data Transfers.....	4
Automated Decision Making.....	5
Retention Period & Security Measures.....	6

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: Corporate Support Department/ Security officer

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
<p>Personal contact details of EIOPA’s Temporary and Contract Agents, Seconded National Experts (SNEs) as well as external contractors working at EIOPA premises shall be processed and used exclusively for business continuity management purposes, i.e., to prepare exercises and respond to crises and operational disruptions affecting the normal functioning of EIOPA.</p> <p>Data are collected via EIOPA’s Extranet, in a site dedicated for business continuity to which only EIOPA staff has access after authentication. Users may only see their own entry. The information collected will be stored in the form of a list.</p> <p>Communication will take place by phone as follows:</p> <ul style="list-style-type: none"> • The Executive Director decides to communicate in times of crisis e.g., declaring business continuity role; • The Business Continuity Responsible (Security officer) contacts all Heads of Department; • Heads of Department further contact the relevant Heads of Units or Team Leaders; • Heads of Units or Team Leaders contact the rest of staff or external contractors working at EIOPA premises.
Purpose (s) of the processing
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Staff administration <input type="checkbox"/> Relations with external parties <input type="checkbox"/> Procurement and accounting <input type="checkbox"/> Administration of membership records <input type="checkbox"/> Auditing <input checked="" type="checkbox"/> Information administration <input checked="" type="checkbox"/> Other (please give details): Crisis Management – alerting in case where a major disruption affects EIOPA activities (for example, major IT disruption, fire affecting EIOPA premises, pandemics etc.)
Lawfulness of Processing
<ul style="list-style-type: none"> • Legal Basis justifying the processing: <ul style="list-style-type: none"> - Article 55 of the Staff Regulations providing that: “Officials in active employment shall at all times be at the disposal of their institution.” - EIOPA’s Business Continuity Plan of 30 November 2015 (EIOPA-15/013); rev. 2.1 of August 2021 • Processing is necessary: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> for the performance of a task carried out in the public interest – Article 5(1)(a) of the Regulation. More precisely, processing is necessary to ensure the proper management and functioning of EIOPA for the performance of its task carried out in the public interest. <input type="checkbox"/> 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 security@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

<input type="checkbox"/> Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other) If selected, please specify: <input type="checkbox"/> Providers of good or services <input type="checkbox"/> Complainants, correspondents and enquirers <input type="checkbox"/> Relatives and associates of data subjects <input checked="" type="checkbox"/> Other (please specify): external contractors working at EIOPA premises
Categories of personal data
<p>(a) General personal data: The personal data contains: <input checked="" type="checkbox"/> Personal details (name, address, phone number, email, etc.) <input type="checkbox"/> Education & Training details <input checked="" type="checkbox"/> Employment details <input type="checkbox"/> Financial details <input type="checkbox"/> Family, lifestyle and social circumstances <input checked="" type="checkbox"/> Other (please give details): First and last name; private mobile or landline number; Department/Unit/Team; business phone (if any); private/home; private email address.</p> <p>(b) Special categories of personal data The personal data reveals: <input type="checkbox"/> Racial or ethnic origin <input type="checkbox"/> Political opinions <input type="checkbox"/> Religious or philosophical beliefs <input type="checkbox"/> Trade union membership <input type="checkbox"/> Genetic or Biometric data <input type="checkbox"/> Data concerning health, sex life or sexual orientation</p>

Categories of Recipients & Data Transfers

Recipient(s) of the data
<input checked="" type="checkbox"/> Managers of data subjects <input checked="" type="checkbox"/> Designated EIOPA staff members If selected, please specify: - Business Continuity Coordinator (Security Officer); - EIOPA Senior Management / Heads of Departments / Heads of Units / Team Leaders; - EIOPA IT & Extranet (SharePoint) Administrators (who have access to Extranet, need to know basis).

Yes

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

Retention Period & Security Measures

Retention period

How long will the data be retained?

Personal details are kept for as long as the person concerned works in EIOPA.

For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:

No

Yes

Technical & organisational security measures taken

Several technical and organisational measures have been adopted 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'.