

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

► Breach of Union law

Contents

General information	1
Description and Purpose of the Processing	2
Data Subject's Rights	3
Categories of Data Subjects & Personal Data.....	4
Categories of Recipients & Data Transfers.....	5
Automated Decision Making.....	6
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: Legal Unit, legal@eiopa.europa.eu

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>Management of breach of Union law (BUL) proceedings under Article 17 of Regulation (EU) No 1094/2010, including the establishment of the BUL Panel.</p> <p>If BUL proceedings are triggered by an external complaint, EIOPA may collect and process the following:</p> <ul style="list-style-type: none"> • Personal data of complainants or their representatives (e.g. names and contact details), who send a complaint by e-mail to or mail to EIOPA against a national competent authority or a financial market participant; • Personal data of other data subjects, if mentioned in the complaint or accompanying documentation, and deemed relevant for the assessment of the BUL complaint (it cannot be foreseen what other data apart from names might be concerned); <p>In the context fo establishment of BUL Panel, the following processings of personal data might take place:</p> <ul style="list-style-type: none"> • The CVs of the candidates for becoming member of the common pool / BUL Panel are collected and shared with the BoS for appointment; • The names and contact details of the members of the BUL Panel, as well as the representatives of the competent authorities concerned are collected. <p>More precisely, these names might appear in:</p> <ol style="list-style-type: none"> (a) emails exchanged in the context of a case / documents submitted by competent authorities; (b) the minutes taken during Panel meetings; (c) the report/decision communicated by the Panel to the BoS, or the decision of the BoS; (d) the declarations of non-conflict of interest signed by the Panel members.
Purpose (s) of the processing
<p><input type="checkbox"/> Staff administration</p> <p><input checked="" type="checkbox"/> Relations with external parties</p> <p><input type="checkbox"/> Procurement and accounting</p> <p><input type="checkbox"/> Administration of membership records</p> <p><input type="checkbox"/> Auditing</p> <p><input type="checkbox"/> Information administration</p> <p><input type="checkbox"/> Other (please give details): Management of breach of Union law (BUL) proceedings, including the establishment of the BUL Panel.</p>
Lawfulness of Processing
<ul style="list-style-type: none"> • Legal Basis justifying the processing: <ul style="list-style-type: none"> - Articles 17 and 41(2) of Regulation (EU) No 1094/2010

<p>- Rules of Procedure on investigations regarding breach of Union law (EIOPA-BoS-11-017-rev4)</p> <ul style="list-style-type: none">• 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<input type="checkbox"/> for compliance with a legal obligation to which the Controller is subject<input type="checkbox"/> 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<input type="checkbox"/> in order to protect the vital interests of the data subject or of another natural person <p>Or</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Data subject has given his/her unambiguous, free, specific and informed consent – Article 5(1)(d) of the Regulation: the complainants’/representatives’ personal data are shared with concerned NCA(s) based on such consent

Data Subject’s Rights

Information on how to exercise data subject’s rights
<p>Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018.</p> <p>Data subjects have the right to:</p> <ul style="list-style-type: none">• 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. <p>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.</p> <p>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 legal@eiopa.europa.eu or DPO@eiopa.europa.eu.</p> <p><u>Complaint:</u></p> <p>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).</p>

Categories of Data Subjects & Personal Data

Categories of Data Subjects
<input checked="" type="checkbox"/> EIOPA permanent staff, Temporary or Contract Agents <input checked="" type="checkbox"/> 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 checked="" type="checkbox"/> Complainants, correspondents and enquirers, and their representatives <input type="checkbox"/> Relatives and associates of data subjects <input checked="" type="checkbox"/> Other (please specify): Relevant staff of the concerned NCAs, BUL Panel Members
Categories of personal data
<p>(a) General personal data:</p> <p>The personal data contains:</p> <input checked="" type="checkbox"/> Personal details (name, address etc) <input checked="" 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): The personal data collected mostly include contact details (such as last name, first name, telephone/fax, full address, email address) and CVs of the candidates that responded to a call for interest for a member position in the BUL Panel. It cannot be foreseen what other types of personal data may be revealed in the context of an external complaint.
<p>(b) Special categories of personal data</p> <p>The personal data reveals:</p> <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

Categories of Recipients & Data Transfers

Recipient(s) of the data
<input type="checkbox"/> Managers of data subjects <input checked="" type="checkbox"/> Designated EIOPA staff members If selected, please specify: designated staff of the Legal Unit and other relevant departments (e.g. Oversight Department, Consumer Protection Department); EIOPA’s Senior Management, <input type="checkbox"/> Relatives or others associated with data subjects <input type="checkbox"/> Current, past or prospective employers <input type="checkbox"/> Healthcare practitioners <input type="checkbox"/> Education/training establishments <input type="checkbox"/> Financial organisations <input type="checkbox"/> External contractor <input type="checkbox"/> Other (please specify): - BoS Members; - Board of Appeal in the case of an appeal; - With regard to external complaint: with concerned NCA(s), based on explicit consent by data subject
Data transfer(s)
<input checked="" type="checkbox"/> Within EIOPA or to other EU Institutions/Agencies/Bodies If selected, please specify: Within EIOPA, to the Board of Appeal, as applicable. <input checked="" type="checkbox"/> To other recipients within the EU (e.g. NCAs): with regard to external complaints, personal details of complainants/representatives, based on their explicit consent <input type="checkbox"/> To third countries If selected, please specify: Whether suitable safeguards have been adopted: <input type="checkbox"/> Adequacy Decision of the European Commission ² <input type="checkbox"/> Standard Contractual Clauses (SCC) <input type="checkbox"/> Binding Corporate Rules (BCR) <input type="checkbox"/> Administrative Arrangements between public Authorities (AA) <input type="checkbox"/> 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: N/A

² Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions \(europa.eu\)](https://european-council.europa.eu/media/e3000420/1/16222_en.pdf).

Automated Decision Making

Automated Decision-making, including profiling
<p>A decision is taken in the context of this processing operation solely on the basis of automated means or profiling:</p> <p><input checked="" type="checkbox"/> No</p> <p><input type="checkbox"/> Yes</p> <p>In case of an automated decision-making or profiling, please explain:</p>

Retention Period & Security Measures

Retention period
<p>How long will the data be retained?</p> <p>1. Elections:</p> <ul style="list-style-type: none"> - CVs of non-elected candidates: 1 year after the election. - CVs of elected candidates: Until the end of the mandate of each BUL Panel member <p>2. BUL cases:</p> <ul style="list-style-type: none"> - The documents in a BUL proceedings, i.e. documents submitted by NCAs / emails exchanged / meeting minutes / reports and decisions / declarations of interest: 5 years after the case was closed. <p>3. External complaints:</p> <ul style="list-style-type: none"> - complaints, email correspondence, accompanying documentation: 5 years after the case was closed. <p>If the BUL case is subject to an appeal with the Board of Appeal and/or an action before the Court of Justice of the EU, the 5-year period only starts after the Board of Appeal has decided on the appeal and/or the Court’s judgment has gained the status of res judicata. This is needed to allow for a comparison between similar cases and ensure uniformity and consistency in the handling of BUL cases. Thereafter, transfer to the historical archive.</p>
<p>For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:</p> <p><input checked="" type="checkbox"/> No</p> <p><input type="checkbox"/> Yes</p>
Technical & organisational security measures taken
<p>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 II a).</p>