

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

► ESAS INFORMATION SYSTEM

Contents

General information.....	1
Description and Purpose of the Processing	2
Categories of Data Subjects & Personal Data	4
Categories of Recipients & Data Transfers.....	6
Retention Period & Security Measures	6
Privacy statement	7

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)
Executive Director Westhafenplatz 1, 60327 Frankfurt am Main, Germany fausto.parente@eiopa.europa.eu
Contact Details of the Data Protection Officer
Westhafenplatz 1, 60327 Frankfurt am Main, Germany dpo@eiopa.europa.eu
Contact Details of the responsible EIOPA Team/Unit/Department
<i>EIOPA's Oversight Department</i> <i>Affected National Competent Authorities have been also informed</i>
Contact Details of External Processor(s) / Joint Controller(s)

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.

☒ External processor(s):

Microsoft EU
 One Microsoft Place
 South County Business Park
 Leopardstown
 Dublin 18 D18 P521 Ireland
 Telephone: +353 (1) 706-3117
[Link to Privacy Documentation](#)

☒ Joint controller(s):

- European Banking Authority (EBA), Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France
- European Securities and Markets Authority (ESMA), 201-203 Rue de Bercy, 75012 Paris, France

☐ N/A

Description and Purpose of the Processing

Description & essential elements of processing

➤ General Description and purpose of processing

The European Supervisory Authorities (hereinafter “ESAs”), i.e. the European Banking Authority (hereinafter “EBA”), the European Insurance and Occupational Pensions Authority (hereinafter “EIOPA”) and the European Securities and Markets Authority (hereinafter “ESMA”) are developing and managing in collaboration with the European Central Bank and the National Competent Authorities falling within the ESAs’ remit (hereinafter the two latter individually or collectively referred to as “CA” or “CAs”) a system for the exchange of information relevant to the assessment of the fitness and propriety of holders of qualifying holdings, directors and key function holders of financial institutions (hereinafter “persons of interest”) performed by CAs (hereinafter all together “ESAs Information System”).

The ESAs Information System has been established by the ESAs as mandated in Article 31a of the ESAs Founding Regulations.

The ESAs Information System is hosted by the EIOPA and consists of a cross-sectoral database aiming at facilitating the timely exchange of information between the CAs on the persons mentioned above.

Employees of the CAs and the ESAs in charge of fitness and propriety assessments have access to the ESAs Information System to further facilitate the exchange of such information. Access of those employees is strictly defined on a need-to-know basis.

The data added to the System belongs to the CAs. In particular, the ESAs Information System allows the CAs to easily insert, update, or delete data in total autonomy. Strictly agreed datasets are used and a limited amount of free text and open fields is available. End users do not have access to the whole list of persons of interest that have been added to the System, but only to the result of their specific search (if any).

Once the search results are displayed, the end-user can select one (or several) record(s) and send via the ESAs Information System request(s) to the CA(s) that performed or is in the process of performing the assessment(s). The CA(s) that performed the assessment can view the request(s) in the ESAs Information System but shall provide the requested information outside of the system.

Finally, the ESAs will contribute to the information exchange by producing statistics and/or identifying issues in the information exchange. This is in line with the ESAs' tasks, and in particular promoting the convergence of supervisory practices and enhancing the information exchange among the CAs, as referred to in the ESAs Founding Regulations.

Following all the above, the ESAs act as "Joint Controllers" pursuant to article 28 of the Regulation, while the CAs act as separate controllers.

➤ **Essential elements of processing**

A. Essential elements of joint processing by the ESAs:

1. Granting access to the ESAs Information System

1. *Categories of data subjects - Users/End-users of the ESAs Information System (ESAs, and CAs staff members)*
2. *Categories of personal data - Contact data (name, professional e-mail address)*
3. *Legal basis - Necessary for the performance of a task carried out in the public interest (Article 5(1)(a) of the Regulation, in combination with Articles 2(4), 31a and 35 of the ESAs Founding Regulations).*
4. *Recipients/Categories of recipients/processors - ESAs as owners of the system; EIOPA's IT Unit as processor of personal data related to the hosting and use of the ESAs Information System.*
5. *Retention period of personal data of System users - Until the ESAs or CAs staff member is no longer appointed as the respective authority's representative for the ESAs Information System.*
6. *Joint Controllers - Joint Controllership between the ESAs*
7. *Primary Contact Point of the Joint Controllers – EIOPA (EIOPA DPO contact details mentioned above)*

2. Setting up, functioning and maintenance of the ESAs Information System

1. *Categories of data subjects - Potentially: Persons of interest subject to fit and proper assessments (data inserted by the CAs) and Users/End-users of the ESAs Information System*
2. *Categories of personal data - Potentially: (a) The information inserted in the ESAs Information System by the CAs, i.e. identification data (first name(s), surname/family name, date of birth, place of birth, birth name, other names used by the person); (b) Contact data of the users of the ESAs Information System; (c) Log files identifying authorised users having accessed the ESAs Information System (for more details please see below).*
3. *Legal basis - Necessary for the performance of a task carried out in the public interest (Article 5(1)(a) of the Regulation, in combination with Articles 2(4), 31a and 35 of the ESAs Founding Regulations).*
4. *Recipients/Categories of recipients/processors - ESAs as owners of the system; EIOPA's IT Unit as processor of personal data related to the hosting and use of the ESAs Information System*

<p>5. <i>Retention period – (a) For the information inserted in the ESAs Information System: Fifteen years (15); Shorter retention periods may apply in line with applicable legislation. (b) For the contact data of the users of the ESAs Information System: until the ESAs or CAs staff member is no longer appointed as the respective authority’s representative for the ESAs Information System.</i></p> <p>6. <i>Joint Controllers - Joint Controllership between the ESAs</i></p> <p>7. <i>Primary Contact Point of the Joint Controllers - EIOPA</i></p> <p>B. Essential elements of independent processing by the <u>CAs as separate controllers</u>, outside the joint controllership of the ESAs:</p> <p>1. <i>Categories of data subjects - Persons of interest subject to fit and proper assessment</i></p> <p>2. <i>Categories of personal data - identification data (first name(s), surname/family name, date of birth, place of birth, birth name, other names used by the person)</i></p> <p>3. <i>Legal basis - National and EU laws, as applicable, providing for the collection of information on fitness and propriety; ECB’s Founding Regulation</i></p> <p>4. <i>Recipients/Categories of recipients/processors - Relevant CA; Potentially: the ESAs</i></p> <p>5. <i>Retention period - Fifteen years (15) - shorter retention periods may apply in line with applicable national legislation</i></p> <p>6. <i>Joint Controllers – No. Separate controllership for each of the CAs</i></p> <p>7. <i>Primary Contact Point - CAs) that initially created the data input into the ESAs Information System</i></p>

Categories of Data Subjects & Personal Data

Categories of Data Subjects
<p><input checked="" type="checkbox"/> EIOPA Temporary or Contract Agents, SNEs or trainees: <i>on a need-to-know-basis</i></p> <p><input type="checkbox"/> Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other) If selected, please specify:</p> <p><input type="checkbox"/> Providers of good or services</p> <p><input type="checkbox"/> Complainants, correspondents and enquirers</p> <p><input type="checkbox"/> Relatives and associates of data subjects:</p> <p><input checked="" type="checkbox"/> Other (please specify): - <i>Users/End-users of ESAs Information System (ESAs, and CAs staff members)</i> - <i>Persons of interest subject to fit and proper assessment</i></p> <p><i>For more information, please see above under essential elements of processing.</i></p>
Categories of personal data
<p>(a) General personal data: The personal data contains:</p>

- ☒ Personal details (name, address etc)
- ☐ Education & Training details
- ☒ Employment details
- ☐ Financial details
- ☐ Family, lifestyle and social circumstances
- ☒ Other (please give details):

The following categories of personal data will be concerned by this processing activity:

- *Identification data of natural and legal persons assessed or are in the process of being assessed for fitness and propriety by the CAs, as listed in the section "Data input into the ESAs Information System" point 7 of the Joint Guidelines published by the ESAs on the topic²;*
- *Additional categories of data: the date of entry of the information related to the fitness and propriety assessments, the legal basis on which the assessment was or is being performed according to the relevant sectoral act, and a reference number for an underlying record held by the CA;*
- *Identification data of the contact points in the CA;*
- *Log files identifying authorised users having accessed the ESAs Information System.*

In particular, the data to be provided by the CAs into the ESAs Information System should include the following information as concerns the persons of interest:

- *[Mandatory] First name(s) of the person of interest: Identification of the applicant;*
- *[Mandatory] Surname/family name of the person of interest: Identification of the person of interest;*
- *[Mandatory] Date of birth of the person of interest: Identification of the applicant, would be used to segregate homonyms as well;*
- *[Mandatory] Place of birth (city and country): Identification of the person of interest, would be used to segregate homonyms as well;*
- *[where available] Other names used by the applicant (AKA names), including, where available, birth name of the applicant;*
- *[when mandatory data points are not available and only for historical data] social security number, identification number of the person of interest.*

(b) Special categories of personal data

The personal data reveals:

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Genetic or Biometric data
- ☐ Data concerning health, sex life or sexual orientation

² [Joint Guidelines on the exchange of information relevant to fit and proper assessments - EIOPA](#)

Categories of Recipients & Data Transfers

Recipient(s) of the data
<p>Personal data collected will be disclosed to the following recipients:</p> <ol style="list-style-type: none"> 1. <i>Relevant staff members of the Joint Controllers, on a need-to-know basis:</i> <ul style="list-style-type: none"> • EBA: in its capacity as ESA on the basis of the statutory duties under the EBA Founding Regulation • ESMA: in its capacity as ESA on the basis of the statutory duties under the ESMA Founding Regulation • EIOPA: In its capacity as ESA on the basis of its statutory duties under the EIOPA Founding Regulation. 2. <i>Relevant staff members of the CAs (as defined above), on a need-to-know basis:</i> 3. <i>Relevant staff members of relevant EU entities, on a need-to-know basis:</i> <ul style="list-style-type: none"> ○ EBA acting in its capacity as direct supervisor ○ ESMA acting in its capacity as direct supervisor
Data transmissions and transfer(s)
<p><input checked="" type="checkbox"/> Other EU institutions/agencies/bodies (as explained above, EBA/ESMA/ECB)</p> <p><input checked="" type="checkbox"/> Other recipients within the EU (as explained above, CAs)</p> <p><input type="checkbox"/> To third countries</p> <p><i>There will be no transfers of personal data to third countries in the context of the ESAs Information System.</i></p> <p>If selected, please specify:</p> <p>Whether suitable safeguards have been adopted:</p> <p><input type="checkbox"/> Adequacy Decision of the European Commission³</p> <p><input type="checkbox"/> Standard Contractual Clauses (SCC)</p> <p><input type="checkbox"/> Binding Corporate Rules (BCR)</p> <p><input type="checkbox"/> Administrative Arrangements between public Authorities (AA)</p> <p><input type="checkbox"/> To international organisations</p> <p>If selected, please specify the organisation and whether suitable safeguards have been adopted:</p>

Retention Period & Security Measures

Retention period
<p>How long will the data be retained?</p> <p><i>Please see above under essential elements of processing by the ESAs and the CAs.</i></p>

³ Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions \(europa.eu\)](https://european-council.europa.eu/media/e300123/16714/1/EN/adequacy-decisions-2023-2024.pdf)

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

General description of technical & organisational security measures taken

Several technical and organisational measures have been adopted in order to ensure the optimum security of the personal data collected in the context of the procedures described under section 'Description and Purpose of the Processing'.

In particular, state-of-the-art security measures are applied to protect the integrity and confidentiality of the data processed. These measures include encryption, access controls, and regular security audits to mitigate risks and ensure compliance with data protection requirements on data security.

Privacy statement

The related privacy statement is available on the webpage of the ESAs Information System, as well as on EIOPA's webpage dedicated to the topic:

[Joint Guidelines on the exchange of information relevant to fit and proper assessments - EIOPA](#)