

Record of processing activity

ESAs Information System

Record of EBA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 (EUDPR)

Part 1 - Article 31 Record (publicly available)

1	Last update of this record	28/01/2025
2	Date of next review	28/01/2027
3	Reference number	EBA/DPR/2024/8
4	Name and contact details of controller	<p>Controller: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France</p> <p>Responsible Department at EBA: Prudential Regulation and Supervisory Policy</p> <p>Contact: info@eba.europa.eu (state in the subject "Data Protection Enquiry")</p>
5	Contact details of DPO	<p>dpo@eba.europa.eu, or alternatively send a letter to the postal address of the EBA (address above) marked for the attention of the DPO of the EBA.</p> <p>Primary contact point DPO: dpo@europa.eu</p>
6	Name and contact details of joint controller (where applicable)	<ul style="list-style-type: none"> The European Insurance and Occupational Pensions Authority, Westhafenplatz 1, 60327 Frankfurt am Main, Germany (EIOPA); The European Securities and Markets Authority, 201-203 Rue de Bercy, 75012 Paris, France (ESMA)
7	Name and contact details of processor (where applicable)	<p>Microsoft</p> <p>One Microsoft Place</p> <p>South County Business Park</p> <p>Leopardstown</p> <p>Dublin 18 D18 P521 Ireland</p>

Part 1 - Article 31 Record (publicly available)

Telephone: +353 (1) 706-3117

<https://aka.ms/privacyresponse>

[Link](#) to Privacy Documentation

8 Short description and purpose of the processing activity

The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) manage 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 by competent authorities (hereinafter “ESAs Information System”) in collaboration with the ECB and the National Competent Authorities under the ESAs remit (hereinafter individually or collectively referred to as “CA” or “CAs”). The ESAs Information system is hosted by the EIOPA. The ESAs Information System has been established by the ESAs pursuant to their mandate as described in Article 31a of their Founding Regulations.

The ESAs Information System consists of a cross-sectoral database aiming at facilitating a timely exchange of information between the CAs. 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 information. Access of such employees is strictly defined on a need-to-know basis.

The data belongs to the CAs, so the ESAs Information System allows the CAs to maintain it easily by inserting, updating, or deleting data in total autonomy, manually or in an automated way depending on the volume of information (but also considering the CAs’ IT and staff resources). Strictly agreed datasets is used, and a limited amount of free text and open fields are available.

The end users would not have access to the whole list of persons of interest but only to the result of their specific search (if available) when entering the above-requested information.

Once the search result list is displayed, the end-user can select one (or several) record(s) and send via 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 and should in response provide information on its assessment outside of the system.

Part 1 - Article 31 Record (publicly available)

Additionally, the ESAs will contribute to the information exchange by providing direct added value, such as producing statistics and identifying issues in the information exchange. This is in line with ESAs tasks, in particular promoting the convergence of supervisory practices and enhancement of information exchange referred to in ESAs Regulation.

The ESAs are “Joint Controllers” of this processing activity pursuant to article 28 of EUDPR.

A. Essential elements of processing by the ESAs:

1. Granting access to the ESAs Information System

1. Categories of data subjects - Users/End-users of 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 compliance with a legal obligation (Articles 2(4), 31a and 35 of the ESAs Regulation); Necessary for the performance of a task carried out in the public interest (Article 5(1)(a) of EUDPR)
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 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 Controllorship between the ESAs
7. Primary Contact Point - EIOPA

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 ESAs Information System
2. Categories of personal data - Potentially: 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

Part 1 - Article 31 Record (publicly available)

name, other names used by the person); Contact data of the users of the ESAs Information System

3. Legal basis - Necessary for compliance with a legal obligation (Articles 2(4), 31a and 35 of the ESAs Regulation); Necessary for the performance of a task carried out in the public interest (Article 5(1)(a) of EUDPR)
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 - For the information inserted in the ESAs Information System: Fifteen years (15); Shorter retention periods may apply in line with applicable legislation; For the contact data of the users of the ESAs Information System, the retention period explained in 1. above
6. Joint Controllers - Joint Controllership between the ESAs
7. Primary Contact Point - EIOPA

B. Essential elements of independent processing by the CAs as separate controllers, outside the joint processing by the ESAs:

1. Categories of data subjects - Persons of interest subject to fit and proper assessment
2. 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)
3. Legal basis - National and EU laws, as applicable, providing for the collection of information on fitness and propriety; ECB's Founding Regulation
4. Recipients/Categories of recipients/processors - Relevant CA or the ECB
5. Retention period - Fifteen years (15) - shorter retention periods may apply in line with applicable legislation
6. Joint Controllers - Separate controllership for the ECB and each of the CAs
7. Primary Contact Point - CAs (ECB or CAs) that initially created the data input into the ESAs Information System

9 Description of categories of persons whose data the EBA

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

Part 1 - Article 31 Record (publicly available)
processes and list of data categories

- Identification data of natural and legal persons who were assessed or are in the process of being assessed for F&P by the CAs, as listed in the section “Data input into the ESAs Information System” point 7 of the Joint Guidelines;
- Additional categories of data: the date of entry of the information related to the F&P assessment, 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.

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.

10 Special categories of personal data processed (as defined in Article 10 EUDPR)	No special categories of personal data are specifically required for this processing activity.
11 Time limit for keeping the data	The information regarding the persons of interest (both individuals and legal persons) entered in the ESAs Information System will be kept for a maximum period of 15 years from the date of entry by a CA and then be deleted from the ESAs Information System. Based on a regular assessment of the need to keep it, personal data may be deleted by CAs before the end of that maximum period, on a case-by-case basis, when required for compliance with EU and/or national legislation.

Part 1 - Article 31 Record (publicly available)

12 Recipients of the data	<p>1. Relevant staff members of the Joint Controllers, on a need-to-know basis:</p> <ul style="list-style-type: none"> • EBA: in its capacity as European Supervisory Authority on the basis of the statutory duties under the EBA Founding Regulation. • ESMA: in its capacity as European Supervisory Authority on the basis of the statutory duties under the ESMA Founding Regulation. • EIOPA: In its capacity as European Supervisory Authority on the basis of its statutory duties under the EIOPA Founding Regulation. <p>2. CAs:</p> <ul style="list-style-type: none"> ○ National competent authorities ○ ECB <p>3. EU entities:</p> <ul style="list-style-type: none"> ○ EBA acting in its capacity as direct supervisor ○ ESMA acting in its capacity as direct supervisor
13 Are there any transfers of personal data to third countries or international organisations?	<p>There will be no transfers of personal data to third countries in the context of the ESAs Information System.</p>
14 General description of security measures, where possible	<p>With regard to the maintenance and operation of the ESAs Information System by EIOPA, it will be hosted within the authority's data centre, located within the EU, and the database will be subject to strict security measures, including conditions of access by users and logs, which will be defined once the IT solution has been developed.</p> <p>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.</p>
15 For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	<p>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.</p> <p>Joint Guidelines on the exchange of information relevant to fit and proper assessments - EIOPA</p>