RECORD OF A PERSONAL DATA PROCESSING ACTIVITY

according to Article 31 of Regulation (EU) 2018/1725

Personal data processing in the context of EFSA login - Information access management (IAM)

EUROPEAN FOOD SAFETY AUTHORITY

1) Controller(s)[1] of data processing activity (Article 31.1(a))

EFSA unit in charge of the processing activity: Corporate Services (CORSER)

EFSA Data Protection Officer (DPO): DataProtectionOfficer@efsa.europa.eu

Is EFSA a co-controller? No

If yes, indicate who is EFSA's co-controller:

2) Who is actually conducting the processing? (Article 31.1(a))

The data is processed by EFSA itself ☒

Indicate the EFSA units or teams involved in the data processing: CORSER Unit and EFSA Service Desk

The processing operation is conducted together with an external party ☐

Please provide below details on the external involvement:

3) Purpose of the processing (Article 31.1(b))

The objective of EFSA Login is to provide identified users with access to EFSA information systems in accordance with the information security principles, thus ensuring the availability, integrity and confidentiality of the information.

4) Legal basis and lawfulness of the processing (Article 5(a)–(d)):

Processing necessary for:

(a) a task carried out in the public interest or in the exercise of official authority vested in EFSA ☒

(b) compliance with a legal obligation to which EFSA is subject ☐

[1] The controller decides on the purposes and means of the data processing. In case of joint controllership (e.g. systems of the European Commission applied by EFSA or jointly with another agency), EFSA is a co-controller.

(c) performance of a contract with the data subject or to prepare such contract ☐

(d) The data subject has given consent (ex ante, explicit, informed) ☐

Further details on the legal basis:

5) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are processed?

EFSA statutory staff ☒

Other individuals working for EFSA (consultants, trainees, interims, experts) ☒

Stakeholders of EFSA, including Member State representatives ☒

Contractors of EFSA providing goods and services ☒

The general public, including visitors, correspondents, enquirers ☐

Relatives of the data subject ☐

Other categories of data subjects (please detail below) ☐

Further details concerning the data subjects whose data are processed:

EFSA Login covers all users of information systems in EFSA's operational remit, including statutory and non-statutory staff (ENDs, trainees, interim workers), scientific panel members, working group members, external experts, consultants, national representatives in the context of Pesticides Peer Review, stakeholder representatives, system administrators.

6) Type of personal data processed (Article 31.1(c))

a) General personal data

The personal data concerns:

Name, contact details and affiliation ☒

Details on education, expertise, profession of the person ☐

Curriculum vitae ☐

Financial details ☐

Family, lifestyle and social circumstances ☐

Goods and services the person provides ☐

Other personal data (please detail): ☒

b) Sensitive personal data (Article 10)
The personal data reveals:

Racial or ethnic origin of the person	☐
Political opinions or trade union membership	☐
Religious or philosophical beliefs	☐
Health data or genetic or biometric data	☐
Information regarding the person's sex life or sexual orientation	☐

Further details concerning the personal data processed:

The profile information including name, e-mail account and password as an EFSA user. Users can add other profile information such as a picture (EFSA staff only) configurable in the system by means of a self-service. The self-service also allows users to manage their access password anytime. On the basis of the profile details the integrity and non-repudiation is asserted.

Additionally the following data relating to the activity on an EFSA user account may be collected:
o date and time of most recent successful and unsuccessful authentication
o last change of password
o last password reset
o number of successful logins and failed attempts
o IP address used for login or changing password, tracked and displayed in Multi-Factor Authentication (MFA) notifications on the user's device. This information typically includes the approximate location, such as the city or region, of login attempts based on the IP address.

The information above is solely used for protecting the user identity and ensuring the integrity of the EFSA information systems accessed, allowing the diagnosis and resolution of system access problems and to deal with security incidents and/or events. Much of these relate to attempts to use an identity and thus to events that occur before a user has successfully authenticated. The IP address information may exclusively be used to ensure security by allowing follow-up to doubtful activity relating to a user account, excluding any user monitoring.

The access rights to EFSA information systems granted to individual users is managed by means of EFSA Service Desk ticketing (outsourced service) and/or coordinators assigning user rights to specific systems.

7) Recipients of the data (Article 31.1(d))

Line managers of the data subject	☐
Designated EFSA staff members	☒
Other recipients (*please specify*):	☒

- Staff of the EFSA Service Desk and coordinators of specific user groups assuming an access right management role with the aim of keeping access to EFSA systems permanently aligned with the status updates of each EFSA user ;
- The EFSA Information Security Officer and staff of the CORSER Unit including IT consultants in the context of contract outsourcing, in charge of monitoring and ensuring the functionality and security of EFSA information systems ;
- The Computer Emergency Response Team for the EU Institutions (CERT-EU) in the context of an investigation of security events.

8) Transfers to recipients outside the EEA (Article 31.1 (e))

Data are transferred to third country recipients:

Yes ☐ No ☒

If yes, specify to which third country:

If yes, specify under which safeguards:

Adequacy Decision of the European Commission	☐
Standard Contractual Clauses	☐
Binding Corporate Rules	☐
Memorandum of Understanding between public authorities	☐

9) Technical and organisational security measures (Article 31.1(g))

How is the data stored?

On EFSA's Document Management System (DMS)	☐
On a shared EFSA network drive or in an Outlook folder	☐
In a paper file	☐
Using a cloud computing solution (please detail the service provider and main characteristics of the cloud solution, e.g. public, private)	☒
On servers of an external service provider	☐
On servers of the European Commission or of another EU Institution	☐
In another way (*please specify*):	☐

Please provide some general information on the security measures applied:

EFSA Login (IAM) is based on 'Microsoft Entra ID' (formerly Azure Active Directory), a cloud computing application of the SaaS (Software as a Service) model, complying with

EFSA's standards on processing of personal data by means of cloud computing.EFSA' service contract with Microsoft provides that EFSA content will be stored solely on servers located inside the European Economic Area (EEA = 27* EU countries + Iceland, Liechtenstein, Norway) + Switzerland and that Microsoft consultants providing on-line assistance are subject to strict confidentiality undertakings.

Further special contract conditions related to information security and personal data protection in the context of the use of a cloud computing system are applicable, including provisions regarding any data transfers outside the European Economic Area and related to sub-processing, auditing, personal data breaches, access to information by law enforcement bodies (non-exhaustive list).

10) Retention period (Article 4.1 (e))

EFSA user profile information is kept in the system as long as access rights are enabled. Maximum six months after the de-provisioning and withdrawal of all access rights to EFSA information systems, the user profile information shall be deleted from the system.

11) Consultation with the Information Security Officer

Was the ISO consulted on the processing operation ?

Yes ☒ No ☐

If yes, please provide some details on the consultation with the ISO:

12) Information given to data subjects (Articles 15 and 16)

Has information been provided to data subjects on the way their data is processed including how they can exercise their rights (access, rectification, objection, data portability)? Usually this information is provided in a Privacy Statement, specifying the controller's contact details. As possible, please provide a link to the relevant Privacy Statement or a description.

EFSA users can consult their profile by logging in using the authentication credentials (http://myapps.microsoft.com). For further information on the provisioning of specific access rights and any rectifications thereto, the EFSA Service Desk shall be contacted (servicedesk@efsa.europa.eu).
Users can verify all data about their account, including information on any unauthorized use or access or attempts thereto.

Last update of this record: 22/04/2025

Reference: DPO/GOV/8