# RECORD OF A PERSONAL DATA PROCESSING ACTIVITY

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

| Title |
|---|
| **Processing of health data** |

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

EFSA unit in charge of the processing activity: Human Capital Unit (HuCap)

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:*

The processing operation is conducted together with an external party **X**

*Please provide below details on the external involvement:*

EFSA medical adviser and Medical center, both outsourced services currently provided by the company Medlavitalia

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

To carry out the pre-employment medical check-up and to monitor the state of health of statutory staff working at EFSA by means of annual medical check-ups in line with the applicable provisions of the Staff Regulations

## 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 **X**

(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:*

Legal basis: Art 28, 33, 59 SR and Art. 12, 13, 83 CEOS

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

*Whose personal data are processed?*

| | |
|---|---|
| EFSA statutory staff | **X** |
| 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:*

Data subjects: statutory staff (Officials, TAs, CAs) as well as ENDs

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

**a) General personal data**

The personal data concerns:

| | |
|---|---|
| Name, contact details and affiliation | **X** |
| Details on education, expertise, profession of the person | ☐ |
| Curriculum vitae | ☐ |
| Financial details | ☐ |
| Family, lifestyle and social circumstances | **X** |
| 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 | **X** |
| Information regarding the person's sex life or sexual orientation | ☐ |

*Further details concerning the personal data processed:*

Identification data
Surname, forename, personnel number, data and place of birth, nationality, language, sex, civil status, children, family history, postal address, e-mail address, telephone numbers, name of family doctor, education, languages, position held, type of contract.

Medical data
Medical history, objective examination, results of laboratory tests, x-rays, ECGs, results of other medical examinations (ophthalmic, audiometric, etc.) necessary for a particular individual, medical certificates, periods of absence and other medical records.

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

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

The EFSA Medical Adviser manages the medical file.
For a staff member requesting to be recognized as suffering from an occupational disease, the data will be sent to the Accidents and Occupational Diseases Department of the Sickness Insurance Fund.

Certain administrative details may be disclosed to:
• The Legal and Assurance Services Unit, to allow it to prepare the defense in the event of an action before the ECJ or
• ECJ judges at their request, or
• The European Ombudsman, at his request, or
• The European Data Protection Supervisor

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

Data are transferred to third country recipients:

Yes ☐ No **X**

***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*): | **X** |

*Please provide some general information on the security measures applied:*

Medical records are kept in a separate file for each individual and stored in secure archives only accessible to the EFSA Medical Adviser.
As a complement, since 2016 the EFSA Medical Adviser imports the data in the electronic medical file 'ERMES'. This system ensures a quick overview of the health status of the patient and his/her medical history, to elaborate metabolic trends, to automatically generate reports, certificates and communications, etc. The system can also be used to record specific information needed for the procedures carried out by the Medical Service, such as medical examinations, the administration of absences on medical grounds and check-ups, invalidity procedures and occupational accidents. The system also facilitates the monitoring of procedures by automatically generating the various notes and letters required for these procedures. ERMES as complement electronic file represents a measure of data security, e.g. in case of a physical disaster occurring at EFSA infirmary (i.e. fire), a backup of the electronic system is kept out of the infirmary in EFSA. The medical file is processed by and accessible solely to Medlavitalia as provider of the EFSA Medical Adviser service (two medical doctors & a nurse) taking account of the instructions from the data controller.
A security plan and data protection impact assessment of the ERMES Electronic medical file for EFSA is provided in annex

## 10) Retention period (Article 4.1 (e))

Medical files are retained for a period of 30 years after ceasing of work at EFSA. In the case of persons exposed to carcinogens or mutagens, files are kept for 40 years after the last exposure incident or, in any event, until reaching the age of 75.

The original medical file of a staff member who carried out his/her pre-employment medical visit at the Medical Service of the European Commission in Brussels shall be transferred to the Medical Service of the European Commission on termination of employment at EFSA.

The pre-recruitment files of candidates who have not been recruited are destroyed after one year. Where a negative medical opinion is given, the file will be destroyed after five years, if no claim took place.

## 11) Consultation with the Information Security Officer

Was the ISO consulted on the processing operation ?

Yes **X** No ☐

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

The ISO was specifically consulted on the ERMES electronic file management system of the Medical Adviser.

## 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.*

Information on the EFSA medial files management provided on the Intranet portal (to be updated)

Last update of this record: 24/02/2020

Reference: DPO/HR/8