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

▸ TIME MANAGEMENT – LEAVES, ABSENCES, FLEXITIME, WORKING TIME AND TELEWORKING

Contents

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: ……HR UNIT……………………………………………………………………………………………

---

[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.

Handling instructions for documents with security markings:
https://www.eiopa.europa.eu/sites/default/files/publications/other_documents/summary_eiopa_information.pdf

Description and Purpose of the Processing

Description of Processing
The purpose of processing the data subject's personal data is the time management related to presences and absences in accordance with the EU Staff Regulations, the Conditions of Employment of other servants and the implementing provisions on working hours, part-time work, leave, flexitime and teleworking. These covers: • Working time • Flexitime • Annual leave, sick leave, leave on personal grounds/unpaid leave, parental leave, family leave, maternity leave, special leave including travelling time due to special leave • Working pattern, like part-time work • Teleworking, including teleworking from abroad. For flexitime, the data is collected to keep a record of the hours worked by the staff in the context of 40 hours/week. This gives flexibility for the staff to decide, within the interest of the service and the defined bandwith, when they start and finish work. For leave, the data is managed by the HR Unit for the purpose of leave management. Such data may also be further processed in case of an invalidity procedure.

Purpose (s) of the processing
☒ Staff administration ☐ Relations with external parties ☐ Procurement and accounting ☐ Administration of membership records ☒ Auditing ☒ Information administration ☐ Other (please give details): ………………………………………………………………………………………………………

Lawfulness of Processing
• Legal Basis justifying the processing: -   Regulation (EEC) No 31 laying down the Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (CEOS) and the Implementing Rules thereof, in particular title IV of SR -   Decision of the Management Board EIOPA-MB-14-004 of 14 January 2014 adopting implementing rules to Staff Regulations by analogy, in particular Commission Decision C(2013)9051 on leave -   Decision of the Management Board EIOPA-MB-16-057 adopting Implementing Rules to the Staff Regulations by analogy, in particular Commission Decision C(2015)9720 on article 55a of the SR and Annex IVa concerning part time work.

- Decision of the Management Board EIOPA-MB-20-104 of 9 November 2020 on the application by analogy of the Commission Decision C(2020) 1559 final of 16.3.2020 amending Decision C(2013) 9051 of 16 December 2013 on leave.

- Decision of the Management Board EIOPA-MB-23-070 of 5 September 2023 on the adoption of the model decision on working time and hybrid working.

- Decision of the Executive Director EIOPA-23-695 of 5 September 2023 on implementing rules for applying the model decision on working time and hybrid working.

- Processing is necessary:

☒ for the performance of a task carried out in the public interest

☐ for compliance with a legal obligation to which the Controller is subject

☐ 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

☐ in order to protect the vital interests of the data subject or of another natural person

Or

☐ Data subject has given his/her unambiguous, free, specific and informed consent

Data Subject's Rights

Information on how to exercise data subject's rights
Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018.

Data subjects have the right to:

- 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.

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.

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 human.resources@eiopa.europa.eu] or DPO@eiopa.europa.eu.

Complaint:

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).

Restrictions:

Without prejudice to the above, rights might be restricted in accordance with EIOPA's decision on the restriction of data subject's rights (EIOPA-MB-19-056).

Categories of Data Subjects & Personal Data

Categories of Data Subjects
☒ EIOPA permanent staff, Temporary or Contract Agents ☒ SNEs or trainees ☐ Visitors to EIOPA (BOS, MB, WG, Seminars, Events, other)   If selected, please specify: …………………………………………………………………………………………… ☐ Providers of good or services ☐ Complainants, correspondents and enquirers ☐ Relatives and associates of data subjects ☐ Other (please specify): ………………………………………………………………………………………………
Categories of personal data
(a) **General personal data:** The personal data contains: ☒ Personal details: full name, date of birth, gender, personnel number, addresses, phone number ☐ Education & Training details ☒ Employment details: contract type, position/job title, Department/Unit/Team ☐ Financial details ☒ Family, lifestyle and social circumstances ☐ Other (please give details): In the case of the management of leave, the following personal data might be processed, depending on the type of leave requested: -   Individual request for all type of leaves -   Civil status and statutory status of the staff member and SNE -   Name of the relatives (spouse, child, ascendant) of the Staff members and SNEs mentioned in the supporting document when necessary (e.g in case of request of absence linked to family,

parental leave or special leave due to serious illness of a relative and spouse in the case of marriage.

- Certificate of marriage, birth, adoption of a child, death of relatives
- Certificate of sickness of the staff member and SNE
- Certificate of sickness of the staff members' relative
- Election attendance certificate
- Invitation to summon before a court
- Certificate of attendance to an exam/competition
- Declaration of outside activities

In the case of the management of flexitime, the following personal data might be processed:

- Woking pattern and time arrangement
- Working hours (beginning/end of the working day and lunch break
- Flexi credit (in case of TW, leave, mission)
- Flexitime recuperation and balance

In the case of the management of teleworking, the following personal data might be processed:

- Type of teleworking request
- Start/end dates
- Reasons of teleworking (concentrate on a project, personal mobility issue/health, transport problem/strike, specific family circumstances, teleworking away from the place of employment, other reasons)

(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

Categories of Recipients & Data Transfers

Recipient(s) of the data
☒ Managers of data subjects: Executive Director, Line Manager.
☐ Designated EIOPA staff members
If selected, please specify:
-    HR and Finance Units.

- Legal Unit, on a need-to-know basis.
- Team Leader (if applicable)
- Staff member may have access to the planning of absence of their colleagues in the same Unit/Department. This information in strictly limited to the full name and date of absence of the staff, without further information on the reasons.

☐ Relatives or others associated with data subjects.

☐ Current, past or prospective employers

☐ Healthcare practitioners.

☐ Education/training establishments

☐ Financial organisations

☐ External contractor

☒ Other (please specify):

- PMO staff managing the remuneration of staff in case of part-time work, parental/ family leave/ unpaid leave or any other working condition. The note to PMO includes the name of the person concerned, personal number, period of leave and the name of the relatives concerned (child, spouse, parents, etc.);
- external lawyers, internal audit services, EU Court of auditors, OLAF, EU Ombudsman, EU courts, EDPS.

Data transfer(s)

☐ To third countries

If selected, please specify: …………………………………………………………………………………………

Whether suitable safeguards have been adopted:

☐ Adequacy Decision of the European Commission[2]

☐ Standard Contractual Clauses (SCC)

☐ Binding Corporate Rules (BCR)

☐ Administrative Arrangements between public Authorities (AA)

☐ 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:

………

---

[2] Third countries for which the European Commission has issued adequacy decisions are the following: Adequacy decisions (europa.eu)

Automated Decision Making

Automated Decision-making, including profiling
A decision is taken in the context of this processing operation solely on the basis of automated means or profiling: ☒ No ☐ Yes In case of an automated decision-making or profiling, please explain: …………………………………………………………………………………………………

Retention Period & Security Measures

Retention period
How long will the data be retained? 1. In the case of the management of working hours, flexitime and teleworking, the data will be retained according the retention period set in SYSPER (4 years after the employment at decision has ceased) . 2. Document providing evidence related to sick, annual and special leaves are retained in SYSPER with the exception of compensatory leave, in procedure data which will be kept for up to 3 years. In case of invalidity procedures, data is retained for the time necessary for further processing as foreseen in Article 59(4) of the SR. The data can be kept longer in case of dispute or appeal or when the leave has effect on the calculation of the pension rights. 3. Data related to maternity, parental and family leave and to part time work are kept in SYSPER at least until the end of active service. 4. In case of death of a family member, the data is retained in SYSPER at least until the end of the active service.
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
Technical & organisational security measures taken
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 'Description and Purpose of the Processing'.