NAME OF PROCESSING OPERATION: Ex post control on the compliance with EB decision 2022/03 “Application by analogy of the Commission Decision C(2022)1788 on working time and hybrid working”

Reference number: DPR-2023-200
Creation date of this record: 10/01/2024
Last update of this record: 16/01/2024
Version: 1.0

Part 1 (Publicly available)

1) Controller(s) of data processing operation (Article 31.1(a))

Controller: European Union Agency for Fundamental Rights (FRA)
Schwarzenbergplatz 11, A-1040 Vienna, Austria
Telephone: +43 1 580 30 – 0
Email: contact@fra.europa.eu
Organisational unit responsible for the processing activity: Corporate Services Unit
Contact details: expostcontrols@fra.europa.eu
Data Protection Officer (DPO): dpo@fra.europa.eu

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

The data is processed by the FRA itself ✗

The data is processed also by a third party (contractor) [mention the third party] □

---


2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.

3 Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

5 This is the unit that decides that the processing takes place and why.

6 Is the FRA itself conducting the processing? Or has a provider been contracted?
### 3) Purpose of the processing (Article 31.1(b))

*Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).*

The purpose of the processing is to perform an ex-post control of the application of the rules on working time and teleworking introduced by [Executive Board (EB) Decision 2022/03](#) “Application by analogy of the Commission Decision C(2022)1788 on working time and hybrid working”.

In accordance with Decision 2022/03, the Agency shall perform an evaluation of its implementation. In this context, the access to personal data is intended to verify the correct application of the existing rules.

The categories of personal data mentioned in section 5 below will be extracted directly from SYSPER in an aggregated way by the authorised HR administrators. Only the authorised HR administrators will have access to the personal data. After this first access, all personal data will be anonymised. Following the extraction of the anonymised data, an analysis of the aggregated data will be performed by the assigned FRA staff in the context of the ex post control/compliance exercise.

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

*Whose personal data are being processed?*

- **FRA staff**
  - ✔️
- **Non-FRA staff (please specify e.g. Roma community, judges, etc.)**
  - ❌
5) Categories of personal data processed (Article 31.1(c))

*Please tick all that apply and give details where appropriate*

<table>
<thead>
<tr>
<th>(a) <strong>General personal data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal details name and surname, presence in the office</td>
</tr>
<tr>
<td>Only in the first access to Sysper, then the extracted data will be aggregated and anonymised</td>
</tr>
<tr>
<td>Contact details (e.g. postal address, email address, mobile and fax number)</td>
</tr>
<tr>
<td>Education &amp; Training details</td>
</tr>
<tr>
<td>Employment details (e.g. work experience, languages, name and type of the employer/organisation, address of the employer/organisation)</td>
</tr>
<tr>
<td>Financial details (e.g. financial identification form, bank account information)</td>
</tr>
<tr>
<td>Family, lifestyle and social circumstances</td>
</tr>
<tr>
<td>Goods or services provided</td>
</tr>
<tr>
<td>Other (please give details):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) <strong>Special categories of personal data</strong> (Article 10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The personal data collected reveal:</td>
</tr>
<tr>
<td>Racial or ethnic origin</td>
</tr>
<tr>
<td>Political opinions</td>
</tr>
<tr>
<td>Religious or philosophical beliefs</td>
</tr>
<tr>
<td>Trade union membership</td>
</tr>
<tr>
<td>Genetic, biometric or data concerning health</td>
</tr>
<tr>
<td>Information regarding an individual’s sex life or sexual orientation</td>
</tr>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(c) <strong>Personal data relating to criminal convictions and offences</strong> (Article 11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal record (or similar, e.g. declaration of good conduct)</td>
</tr>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>
6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data within FRA? Who will have access to the data outside FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

<table>
<thead>
<tr>
<th>Designated FRA staff members</th>
<th>✗</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR Staff for the first access</td>
<td></td>
</tr>
<tr>
<td>Staff performing ex post controls on anonymised data only</td>
<td></td>
</tr>
<tr>
<td>HR staff, Head of CS, Director on the results of the analysis</td>
<td></td>
</tr>
</tbody>
</table>

**Recipients outside FRA:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

7) Transfers to third countries or international organisations (Article 31.1 (e))

*If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.*

**Transfer outside of the EU or EEA**

| Yes | |
| No | ✗ |

If yes, specify to which country:

**Transfer to international organisation(s)**

| Yes | |
| No | ✗ |

If yes specify to which organisation:

**Legal base for the data transfer**

- Transfer on the basis of the European Commission's adequacy decision (Article 47)
- Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

---

6 Processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.
a) □ A legally binding and enforceable instrument between public authorities or bodies.
   Standard data protection clauses, adopted by
b) □ the Commission, or
c) □ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2).
d) □ Binding corporate rules, □ Codes of conduct, □ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
□ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.
□ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

□ Transfer based on an international agreement (Article 49), specify:

**Derogations for specific situations (Article 50.1 (a) –(g))**

□ N /A  
□ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

□ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
□ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request
□ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
□ (d) The transfer is necessary for important reasons of public interest
□ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
□ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
□ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case


8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g., in selection procedures candidates who made it onto the reserve list vs. those who didn’t). Are the data limited according to the adage “as long as necessary, as short as possible”?

Personal data will remain in the system (SYSPER), only aggregated data will be extracted, anonymized and kept for 3 years for the duration of the control exercise, including time for potential review by auditing bodies.

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

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor.

**How is the data stored?**

- Document Management System (DMS)
- FRA network shared drive
- Outlook Folder(s)
- CRM
- Hardcopy file (for anonymised data)
- Cloud (MS 365)
- Servers of external provider
10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the Data Protection notice: e-mail to expostcontrols@fra.europa.eu

**Data subject rights**

- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to have recourse
- Right to withdraw consent at any time