

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

Processing operation: Management of Personal Files

Data Controller: Innovative Health Initiative Joint Undertaking

Record reference: DPO–HR-04

Table of Contents

1. Introduction
2. Who are the data subjects?
3. Why and how do we process your personal data?
4. On what legal ground(s) do we process your personal data?
5. Which personal data do we collect and further process?
6. How long do we keep your personal data?
7. How do we protect and safeguard your personal data?
8. Who has access to your personal data and to whom is it disclosed?
9. What are your rights and how can you exercise them?
10. Contact information
11. Where to find more detailed information?

1 Introduction

The Innovative Health Initiative Joint Undertaking (hereafter 'IHI JU') is committed to protecting your personal data and to respect your privacy. IHI JU collects and further processes personal data pursuant to [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 (repealing Regulation (EC) 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to the processing operation "*Management of Personal Files*" undertaken by IHI JU is presented below.

2 Who are the data subjects?

In order to carry out this processing operation the IHI JU HR Team collects the personal data of IHI Staff Members (active, non-active and retired) covered by the Staff Regulation and the Conditions of Employment of Other Servants of the European Union, namely:

- Temporary agents;
- Contractual agents;
- Officials of the European Commission;
- Officials of other EU institutions, agencies and bodies;
- Officials on probation
- Former staff members on termination of service (pension, end contract, etc).

The IHI JU HR Team also processes data concerning family members of IHI JU Staff members: parents, grandparents, children, spouses (and assimilates, recognized legal partner, civil partnership) and potentially any other depending from the IHI JU Staff member.

3 Why and how do we collect your personal data?

Purpose of the processing operation:

IHI JU processes the personal data of IHI JU Staff members in the module NDP-personal files to make them accessible to the staff members as well as to file managers to settle the rights of the staff members.

Since October 2023, the IHI JU Staff members in active employment can freely consult their personal file in a secure manner via the SYSPER application due to the computerization of the personal file via NDP application (Numérisation des Dossiers Personnels).

For retired staff or staff who have ceased in their functions, the consultation of the personal file can be done contacting the IHI JU HR Team or via Sysper Post Activity if a digital version is available.

NDP-personal files allows the IHI JU team to create files, allows for the digitalization and uploading of documents, the printing of a whole file or part of it, the moving of a document within a file following an indexing error or to another file (following a data breach for example), the deletion of documents, the creation and granting of access rights to file managers. However, it does not allow any profiling or statistical analysis in relation to personal data.

IHI JU, in view of applying the requirements of the Staff Regulations, manages the individual personal files of staff covered by the [Staff Regulations](#)¹, notably Article 26 of the Staff Regulations.

4 On what legal ground(s) do we process your personal data

IHI JU processes the IHI JU Staff members' personal data, under the following legal basis:

- Regulation (EU) 2018/1725:
 - Article 5(1)(a) “*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*”;
 - Article 5(1)(b) “*processing is necessary for compliance with a legal obligation to which the controller is subject*”;
 - Article 10(2)(b) we process **special categories of personal data** indicated in Section 4, because “*the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject*.”
- Staff Regulations:
 - Article 26 (applicable by analogy to temporary and contract staff under Articles 11 and 81 of the Conditions of Employment of Other Servants of the European Union):

‘The personal file of an official shall contain:

(a) all documents concerning his administrative situation and any reports concerning his ability, efficiency and conduct;

(b) any comments by the official on such documents.

Documents shall be registered, numbered and filed in serial order; the documents referred to in subparagraph (a) may not be used or cited by the institution against an official unless they were communicated to him before they were filed.

The communication of any document to an official shall be evidenced by his signing it or, failing that, shall be effected by registered letter to the last address communicated by the official.

An official's personal file shall contain no reference to his political, trade union, philosophical or religious activities and views, or to his racial or ethnic origin or sexual orientation.

The preceding paragraph shall not however prohibit the insertion in the file of administrative acts and documents known to the official which are necessary for the application of these Staff Regulations.

There shall be only one personal file for each official. An official shall have the right, even after leaving the service, to acquaint himself with all the documents in his file and to take copies of them.

The personal file shall be confidential and may be consulted only in the offices of the administration or on a secure electronic medium. It shall, however, be forwarded to the Court of Justice of the European Union if an action concerning the official is brought.'

- Commission SEC(2019) 900 /3 on the Commission Common Retention List

5 Which personal data do we collect and further process?

IHI JU processes the following categories of personal data:

All documents representing all the decisions taken by the EU institution with regard a IHI JU Staff member or a former IHI JU Staff member, their relatives and the fundamental external documents transmitted by the staff member at the time of recruitment and during their career. The types of data collected and processed are listed in three subfolders which are grouped as follows:

- (1) administrative file (application file, acts during the career),
- (2) assessment file,
- (3) private file (personal and family documents).

The personal file of the IHI JU Staff member includes the following documents which contain some personal data falling under the scope of application of Article 10.2.b of the Regulation dealing with processing of special categories of personal data:

- Medical fitness (which might indirectly reveal data concerning the health of the staff member),
- Marriage or legal cohabitant certificate (which may indirectly reveal data concerning natural person's sexual orientation),
- Birth certificate and children certificate (which may indirectly reveal data concerning racial or ethnic origin),
- Request and decision taken upon Art.15 SR (which may indirectly reveal data concerning political opinion or orientation),

- Request and decision taken upon Art. 12b – 12b/40 - 16 SR on activities related to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
- Decision on invalidity (which by nature reveal indirectly data concerning health of the staff member),
- Copy of passport or ID containing some biometrical data or information regarding religious beliefs of the staff member (which may indirectly reveal racial or ethnic origin and, biometric data),
- Probationary Period reports and Career Development Reports.

6 How long do we keep your data?

IHI JU only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for at least 100 years after the recruitment of the person concerned and 8 years after the termination of the rights of the beneficiaries concerned (Section IHI.3.7.6 of the IHI Retention List).

For disciplinary decisions IHI JU keeps your personal data for 20 years followed by elimination (Section IHI IHI.3.7.12 of the IHI Retention List).

However, in accordance with the Staff Regulations², disciplinary decisions may be withdrawn upon request of the data subject after 3 years in the case of a written warning or reprimand or after 6 years in the case of other sanctions from the personal file. The person concerned may address their request to the Appointing Authority, which will take a decision thereon. As soon as the IHI HR Team is informed of the positive withdrawal decision, the warning, reprimand, or disciplinary sanction is deleted from the scanned personal file and the document used for digitisation is removed from the archives and destroyed.

7 How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of IHI JU. All paper documents are stored in folders in a secured room accessible only to authorised persons (e.g. IHI JU HR Team). All processing operations (including process of personal data collected on paper) are carried out pursuant to the [IHI JU Decision Nr 19/2021 on Record Management of 6 of September 2021](#) that adopts by analogy the [Commission Decision \(EU\) 2020/4482 of 6 of July 2020](#) on the security of communication and information systems in the European Commission.

In order to protect your personal data, IHI JU has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

² Article 27 of Annex IX to the Staff Regulations.

8 Who has access to your data and to whom is it disclosed?

Access to your personal data is provided to IHI JU Staff members responsible for carrying out this processing operation and to authorised IHI JU Staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The access to the personal file is strictly limited according to the legitimate needs of the main user entities, namely:

- A statutory IHI JU Staff member who consults his/her personal file in accordance with Article 26 of the Staff Regulations;
- IHI JU Head of Finance and Administration;
- IHI JU Human Resources Team;
- Paymaster Office (PMO) in charge of determining, calculating and paying out individuals' entitlements;
- Other EU institution/agency in the event that the personal file has been transferred (DPR-EC01847).

Access rights are given at the level of each of the headings making up the individual file and depending on the role and the need to know of the various actors involved. This makes possible to grant specific access rights to certain parts of individual files more appropriately.

Roles and access rights are defined according to the legitimate needs of the user entities. These entities have permanent access (linked to the job ID) to all the files for which they are responsible, and for each of these files only to the sections accessible for their role. The access is only granted upon request from the superior of the file manager. Special roles are also foreseen to allow ad hoc and time-limited access to one or more files on the basis of a justified request from the superior of the file manager to the personal file sector. This covers requests from the Legal Service, OLAF, IDOC, EDPS, the Court of Justice and the Court of Auditors, authorised for inspection purposes or in the event of disputes, in compliance with Regulation (EU) 2018/1725.

Updates of personal files are carried out by:

- The IHI JU HR Team
- Some other services which produce documents (PMO) in IT modules (e.g. SYSPER) that can be automatically injected in NDP but, they cannot under any circumstances withdraw them.

Any consultation of the file is recorded in a diary. This diary is accessible by the staff member for their own files via their SYSPER portal. However, some consultations may be temporarily masked upon request in some investigations by OLAF, IDOC or HR Security — DS.

9 What are your rights and how can you exercise them?

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) on grounds relating to your particular situation.

You can exercise your rights by contacting the IHI JU Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

10 Contact information

The Data Protection Officer of IHI JU

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the IHI JU Data Protection Officer (DPO) at data-protection@ihi.europa.eu with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor, https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en or edps@edps.europa.eu if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the IHI JU.

11 Where to find more detailed information?

The IHI JU DPO publishes the register of all processing operations on personal data by IHI JU, which have been documented and notified to the DPO. You may access the register via the following link: <https://www.ihi.europa.eu/legal-notice-and-privacy>

This specific processing operation has been included in the IHI JU DPO's public register with the following Record reference: DPO-HR-04.