

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Whistleblowing procedure in IHI JU (handling confidential whistleblowing reports)

Data Controller: Innovative Health Initiative Joint Undertaking

Record reference: DPO – IC - 03

CONTENTS

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

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 "Whistleblowing procedure in IHI JU (handling confidential whistleblowing reports)" undertaken by IHI JU is presented below.

2 Why and how do we collect your personal data?

Purpose of the processing operation: IHI JU collects and uses your personal information in the frame of the processing operation for whistleblowing based on Articles 22a (internal whistleblowing) of the Staff Regulations.

Having procedures for raising concerns about fraud, corruption or other serious wrongdoing is relevant for all responsible organisations and for the people who work there. While good internal control systems can reduce the probability of something going seriously wrong, this risk can never be reduced to zero. Where this risk materialises, the first people to realise or suspect the problem will often be those who work in or with the organisation. Yet unless the culture is one where employees believe that it is safe and accepted that such concerns are raised, the risk is that people will stay silent. This denies the organisation an important opportunity to detect and investigate the concern, to take any appropriate action and to protect its assets, integrity and reputation.

The most effective way to encourage staff to report concerns is to provide assurance of protection. Clearly defined channels for internal reporting as well as safe and accepted routes through which staff may raise concerns outside the organisation as an option of last resort should be in place. Viewed in this way, having whistleblowing procedures and whistleblower protection in place is simply a question of good management and a means of putting into practice the principle of accountability. They contribute to improving the diligence, integrity and responsibility of an organisation. It is against this background that rules on whistleblowing were adopted and included in the Staff Regulations (Articles 22a and 22b)¹ in 2004. They complement the general principle of loyalty to the European Union, the obligation to assist and tender advice to superiors (Article 21) as well as the rules on how to deal with orders which are considered to be irregular or likely to give rise to serious difficulties (Article 21a).

Whistleblowers also have the possibility to blow the whistle in an anonymous manner but the protection which is offered reduces the need and justification for anonymity and deprives the investigative services of the possibility of asking the source for clarification or more information. Anonymous reporting is thus not encouraged.

While these rules have already triggered a number of significant investigations by the European Anti-Fraud Office (OLAF), some staff may be reticent to make full use of the whistleblowing procedure, because of a fear of negative repercussions on their reputation or career. As part of the IHI JU's duty to have regard for the interests of staff members ('devoir de sollicitude'), it is necessary to ensure that members of staff who report serious wrongdoings or concerns in good faith are afforded the utmost confidentiality and greatest degree of protection against any retaliation as a result of their whistleblowing.

As whistleblowing arrangements are widely recognised as an important tool to detect fraud, corruption and serious irregularities, it is important that staff fully understand the types of situations where the obligation to 'blow the whistle' applies, and to whom they should address their concerns. Providing guidance on this issue is part of the IHI JU's overall ethics policy, which aims inter alia at clarifying the rules regarding professional ethics in IHI JU.

Thus, the purpose of the processing operation in IHI JU is to:

- Provide safe channels to staff to report fraud, corruption or other serious wrongdoings in IHI JU;
- Offer guidance and support to potential whistleblowers;
- Provide feedback to the whistleblower;
- Ensure the proper follow-up on the reported alleged facts;
- Ensure protection of the whistleblower and the person against whom the allegation is made and any other natural person mentioned in the report/involved in the case.

The whistleblowing procedure/channels are not used for reporting:

- Information already in the public domain (for example: newspaper articles, publicly available audits);
- Unsubstantiated rumours and hearsay;
- Matters of a trivial nature;
- Disagreements over legitimate policy;
- Information not linked to the performance of one's duties;
- Personnel issues where staff have a personal interest in the outcome;
- Harassment claims and personal disagreements or conflicts with colleagues or hierarchy;
- Abusive disclosures (repeated disclosures of alleged facts aimed merely at paralysing a service);
- Malicious, frivolous or potentially defamatory disclosures (i.e. false or unverifiable accusations with the aim of harming another person's integrity or reputation).

Your personal data will not be used for an automated decision-making including profiling.

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

We process your personal data because the processing operations carried out in this context are necessary and lawful under the following legal basis:

[Regulation \(EU\) 2018/1725](#) more specifically:

- Article 5(1)(a) “*processing is necessary for the performance of a task carried out in 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;*”

The necessity is foreseen by the following legal and administrative acts:

- Articles 317 and 325 of the Treaty on the Functioning of the European Union (TFEU) regarding the protection of the financial interests of the Union and the fight against fraud affecting these interests;
- The Staff Regulations of Officials of the European Union (‘Staff Regulations’) and the Conditions of Employment of Other Servants of the European Union (CEOS), laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68, in particular Articles 22 of the Staff Regulations and Articles 11 and 81 of the Conditions of Employment of Other Servants of the European Communities;
- Regulation (EU, Euratom) 2018/1046 on the financial rules applicable to the general budget of the Union, repealing Regulation (EU, Euratom) No 966/2012 (2012 Financial Regulation);
- IHI JU Financial Rules (IMI2 FR) adopted by GB decision n° 2020-16 on 27 May 2020, applicable as of 1 June 2020.¹
- Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999;
- Communication from Vice-President Šefčovič to the Commission on Guidelines on Whistleblowing (SEC (2012) 679 final);
- GB Decision on IMI2 JU Guidelines on Whistleblowing of 27.05.2020 – (IMI2-GB-DEC-2020-17).²
- IHI JU Anti-fraud strategy adopted by ED decision on 16.12.2022 (Ares(2022)8755031).

¹ The decisions of IMI2 continue to apply as per GB decision IHI-GB-DEC-2021-03 of 16.12.2021 (Ares(2021)7794962)

² The decisions of IMI2 continue to apply as per GB decision IHI-GB-DEC-2021-03 of 16.12.2021 (Ares(2021)7794962)

4 Which personal data do we collect and further process?

In order to carry out this processing operation IHI JU collects the following categories of personal data:

For the whistleblower: first name and last name, function and place of employment / administrative address, email.

For the person allegedly committing wrongdoing: first name and last name, function and place of employment, email, any other data necessary for the demonstration of the wrongdoing.

For the witness: first name and last name, function and place of employment, any other data necessary for the justification of his/her quality as a witness.

For the third party: first name and last name, function and place of employment, any other data contained in the report.

The provision of personal data is mandatory to meet statutory requirement and to proceed with investigations in the context of a whistleblowing alert.

5 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 5 years as from the date of the decision about the follow-up to give to the whistleblowing report.

6 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 either on the servers of IHI JU or the European Commission. 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 in place. 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.

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

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

- the IHI JU Executive Director;
- the IHI JU Head of Finance and Administration;
- the IHI JU Internal Control Officer;
- the IHI JU Audit manager.

In addition, as a follow-up to the handling of the whistleblowing report, the information reported by the whistleblower can be transferred to OLAF. The necessity for transferring the personal data to OLAF is assessed on a case-by-case basis.

If staff considers it to be safer to bypass the normal chain of hierarchical command, or one of the abovementioned staff members, they must be able to do so. Then, the staff member may address his or her report to the Secretary General, or equivalent, or directly to OLAF. OLAF may also be notified through the Fraud Notification System³. The access to personal data will then be restricted.

8 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.

³ https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en

9 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 IHI JU.

10 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 – IC – 03.




Contact

Tel +32 (0)2 221 81 81
infodesk@ihi.europa.eu

Postal address:
IHI JU - TO56
1049 Brussels – Belgium

Visiting address:
Ave de la Toison d'Or 56-60
1060 Brussels – Belgium

ihi.europa.eu
 @IHIEurope