

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Processing of personal data in the context of external guest access to Microsoft 365

Record reference: DPO-05-03

Table of contents

1. Introduction	2
2. Controller/ Joint controllers/Processors.....	2
3. Why and how do we process your personal data?	2
4. Categories of data subjects	3
5. Which personal data do we collect and further process and on which legal grounds?.....	3
6. Who has access to your personal data and to whom is it disclosed?	4
7. How long do we retain your personal data?	5
8. How do we protect and safeguard your personal data?	5
9. Transfer to a third country or international organisation.....	6
10. What are your rights and how to exercise them?	6
11. Where to find more detailed information?	7

1. Introduction

The protection of your privacy is of high importance to Global Health EDCTP3 JU is committed to respecting and protecting your personal data and ensuring your privacy rights.

All data of a personal nature processed within the framework of the access to Microsoft 365 granted to guests, namely data that can identify you directly or indirectly, will be handled fairly, lawfully and with due care.

This processing operation is subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals regarding the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data. The information in this communication is given pursuant to Articles 14, 15 and 16 of Regulation (EU) 2018/1725.

This Privacy statement provides detailed information on all types of data that can be processed in the context of the access to Microsoft 365 granted to guests users.

2. Controller/ Joint controllers/Processors

The relevant processing operation is under the responsibility of the Executive Director of the Global Health EDCTP3 JU, acting as the Data Controller. Your personal data are processed based on applicable data protection legislation by Global Health EDCTP3 JU, located at 56-60 Avenue de la Toison d'Or, 1060 Saint-Gilles. The Global Health EDCTP3 JU can be contacted by post (postal address TO-56, B-1049, Brussels, Belgium) or by email to Info@global-health-edctp3.europa.eu

Global Health EDCTP3 JU has appointed a Data Protection Officer (DPO). The task of the DPO is to ensure, in an independent manner, that Global Health EDCTP3 JU complies with the data protection law and protects individuals' rights and freedoms by effectively protecting their personal data. The DPO of Global Health EDCTP3 JU can be contacted by post postal address TO-56, B-1049, Brussels, Belgium) or by email at data-protection@global-health-edctp3.europa.eu

In addition, Global Health EDCTP3 JU relies upon the services of Microsoft Ireland as Cloud Service Provider (CSP) and Inetum as Licensing Solutions Provider (LSP), acting as processors. The use of MS365 is based on licensing agreement between Global Health EDCTP3 JU and Microsoft.

Microsoft Ireland Operations Ltd. processes anonymised data for internal business operations in the context of providing M365. These business operations consist of (exhaustive list):

1. billing and account management;
2. internal reporting and business modelling;
3. financial reporting and compliance with legal obligations.

3. Why and how do we process your personal data?

Your personal data is collected and processed for several specific purposes.

Firstly, it is used to grant and manage your access to Microsoft 365 services. This involves ensuring that authorized users can effectively use the platform's tools and resources. Additionally, it encompasses the administration of user permissions and access levels, which are crucial for maintaining a secure and efficient user environment.

Secondly, your data is utilized to provide end-user support for issues related to Microsoft 365. This support includes addressing technical problems, resolving user inquiries, and facilitating a seamless experience with the platform. Effective support ensures that any disruptions in service are promptly managed, thereby minimizing the impact on your work and productivity.

Moreover, your data plays a critical role in the prevention, detection, and resolution of security events. This proactive approach helps to safeguard your information and protect the integrity of the Microsoft 365 ecosystem. Additionally, your data is used to respond to requests from individuals exercising their rights under data protection laws. Importantly, the collection of this data is performed directly from you during your use of Microsoft 365 and is not employed for automated decision-making or profiling, ensuring that your data is handled with a focus on privacy and user control.

Global Health EDCTP3 JU reserves the right to consult user activity based on Service-Generated Data to maintain the security and integrity of the JU's M365 environment.

4. Categories of data subjects

The processing of personal data concerns the external collaborators being granted access to the Microsoft 365 platform as guests.

5. Which personal data do we collect and further process and on which legal grounds?

In this processing operation, Global Health EDCTP3 JU processes data directly collected from you when you access and use Microsoft 365 products. In particular, four groups of personal data can be distinguished:

1. **Identification Data** contains personal data necessary for the proper identification of the user and the corresponding user account, including exhaustively: (i) email address and, in certain cases, account status; and (ii) user personal data (last name, first name). This information is copied to all M365 data centres around the globe used to provide the service that allows global access and access control to JU's environment in M365. Note that identification data is visible to everyone having access to M365.
2. **Service-Generated Data** contains information related to the guest's usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in M365. Event data will allow to monitor all activity in the cloud environment of each user. Examples: IP address, logs (creation of document, renaming of document, copying of document, modification of document, etc.), etc.
3. **Diagnostic data**, which is a category of data collected by Microsoft from software installed on local devices used in connection with the services. Examples of diagnostic data include installed product and version and the installation status; document, feature, and add-in error conditions that may compromise security, including product update readiness; unexpected application exits and the state of the application when that happens. A detailed list of diagnostic data is provided on Microsoft website at this page: <https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/required-diagnostic-data>
4. **Content Data** includes any content uploaded to M365 by users, such as documents, and multimedia (e.g. video recordings). Such data is stored in M365 but not otherwise processed by the service. Examples: emails, databases, uploaded batches of data, images (still/moving), sound

recordings, documents, chat conversations, channel messages, spreadsheets, presentations, etc.

Global Health EDCTP3 JU carries out specific and important tasks in accordance with various regulations, decisions, initiatives, strategies and/or action plans, in particular with regards to Horizon Europe. The personal data is processed by Global Health EDCTP3 JU for the purpose of granting external guests access to and use of Microsoft 365 collaboration tools where this is necessary to facilitate communication, information sharing, and cooperation with individuals or organisations that interact with Global Health EDCTP3 JU within the scope of its responsibilities undertaken in the public interest, in accordance with Article 5, §1, (a) of the Regulation 2018/1725.

Providing external guests with access to Microsoft 365 enables Global Health EDCTP3 JU to collaborate effectively with relevant stakeholders, including through the exchange of documents, participation in meetings, and access to shared workspaces. Such processing is necessary to provide the technical means required to support Global Health EDCTP3 JU's activities and to enable it to carry out its tasks and exercise its official functions in the public interest.

In addition to the processing activities described in this privacy statement, personal data processed within M365 through the content created, uploaded, shared or exchanged by individual users or groups of users. This refers for example to documents or messages exchanged between members of a specific group or team. The decision regarding what data should be processed using M365 in the context of a particular operational activity remains the responsibility of the respective operational controller or user. Existing policies or instructions concerning this data may exist and need to be taken into account. Relevant documents might for instance be instructions on how to process HR-related data, medical data etc. Global Health EDCTP3 JU does not take any responsibility for the inappropriate use of M365. Please refer to the relevant record and privacy statement of the particular processing activity for further information.

Global Health EDCTP3 JU and Microsoft do not process special categories of personal data in the context of M365. Nevertheless, users may use M365 as a means for processing special categories of personal data in the context of specific policies.

6. Who has access to your personal data and to whom is it disclosed?

Access to your personal data processed for the operation of M365 is provided to the Global Health EDCTP3 JU staff responsible for carrying out this processing operation and to authorised staff of external contractors on a 'need to know' basis.

Such authorised staff abide by statutory, and when required, additional confidentiality agreements. External contractors' staff act under the supervision of the abovementioned Global Health EDCTP3 JU staff. Such staff may belong to:

1. external bodies: European Court of Auditors, European Court of Justice, the Global Health EDCTP3 JU Internal Auditor (Internal Audit Service of the European Commission), may also access to relevant personal data for audit control or appeal purposes; and
2. external contractors of Global Health EDCTP3 JU (such as Microsoft Ireland and Inetum).

For services related to M365, Microsoft, as Cloud Service Provider (CSP), acts as data processor. Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland. Inetum, as managed services provider, also acts as a data processor. Contact details: Inetum, A. Vaucampslaan 42, 1654 Beersel, Belgium.

Global Health EDCTP3 JU will ensure that staff and contractors having access to personal data are bound by statutory and/or contractual confidentiality obligations.

Exceptionally, personal data might be disclosed to a third party if, and to the extent that, we are required to do so by Union of Member State law.

7. How long do we retain your personal data?

The retention period for personal data varies according to its category and is determined in the following way:

- *Identification data*: retained for the duration of the active user account.
- *Content data*: where content data is processed as part of a specific business process or activity, the retention period applicable to that process or activity shall apply. In any event, unless deleted earlier in accordance with the applicable retention requirements, content data will be deleted no later than 180 days following the expiration or termination of the subscription.
- *Diagnostic data*: Microsoft will delete the data after the purposes for which the data was collected have been fulfilled or earlier upon Global Health EDCTP3 JU's request, unless authorized under Global Health EDCTP3 JU's documented instructions to retain such data.
- *Service-generated data*: Retained for 6 months from the date of generation.

Upon the conclusion of these retention periods, the data is permanently deleted.

8. How do we protect and safeguard your personal data?

Global Health EDCTP3 JU implements the following technical and organisational measures to safeguard your personal data:

- Staff dealing with this processing operation is designated on a need-to-know basis;
- Data kept according to the best security practices of Union entities;
- Access control and technical measures such as physical locks and/or secure connections and firewalls;
- Obligation of confidentiality of the staff;
- Computer systems hardened.

In particular, Global Health JU has put in place appropriate technical and organisational measures to prevent or act against any unauthorised and unlawful processing or disclosure, as well as accidental loss, modification or destruction of personal data.

These technical and organisational measures are based on the state of the art, the risks of processing, and the need to protect the personal data. Furthermore, these technical and organisational measures will regularly be adjusted to the technical developments and organisational changes.

Global Health EDCTP3 JU's contractors and processors, including Microsoft Ireland and Inetum, are bound by specific contractual clauses for processing operations with regards to personal data on behalf of the JU and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation (Regulation 2016/679) in the EU Member States.

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. Where personal data and information related to M365 is stored on the servers of

the JU, the operation of such servers abides by the JU's security decisions and provisions established for this kind of servers and services.

9. Transfer to a third country or international organisation

Microsoft may temporally grant access to technical staff and sub-processors located outside EU/EEA where this is necessary to provide their services. Transfers of personal data by Microsoft Ireland may therefore include transfers to third countries, including those that are not covered by an adequacy decision under Article 45 of Regulation 2016/679. In such cases, Microsoft relies on the Standard Contractual Clauses under Article 46(2)(c) of Regulation (EU) 2016/679 as a transfer mechanism to ensure appropriate safeguards are in place for the protection of personal data.

10. What are your rights and how to exercise them?

As 'data subject' you have, under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, specific rights. In particular:

- You have the right to request access to all personal data processed by us pertaining to you.
- You have the right to rectification, i.e., to ask that any personal data pertaining to you that are inaccurate, be corrected.
- You have the right to withdraw your consent for processing of your personal data.
- You have the right to erasure, i.e., to request that personal data pertaining to you be deleted if these data are no longer required in the light of the purposes outlined above in Heading 3.
- You have the right to restriction instead of deletion, i.e., to request that we limit the processing of your personal data.
- you have the right not to be subject to a decision based solely on automated processing of data, including profiling, if such decision has legal effect on him or her, except for certain situations, such as entering a contract (as required by articles 14-16 & 24 of Regulation (EU) 2018/1725).
- You have the right to data portability, i.e., to receive from us in a structured, commonly used and machine-readable format all personal data you have provided to us if the processing is based on your consent or a contract with you and the processing is carried out by automated means.

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 Global Health EDCTP3 JU Data Protection Officer by post (postal address TO-56, B-1049, Brussels, Belgium) or by email at data-protection@global-health-edctp3.europa.eu

The European Data Protection Supervisor (EDPS)

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 Global Health EDCTP3 JU, as a data subject, you have a right to recourse to the European Data Protection Supervisor (EDPS) at any time by e-mail to edps@edps.europa.eu or a letter to the EDPS postal address marked for the attention of the EDPS DPO:

European Data Protection Supervisor
Rue Wiertz 60
B-1047 Brussels
BELGIUM

For more information on the EDPS, please consult their website: <https://www.edps.europa.eu>.

11. Where to find more detailed information?

The Global Health EDCTP3 JU Data Protection Officer (DPO) publishes the Register of all processing operations on personal data by the Global Health EDCTP3 JU on the website. The Register can be found [here](#).

This specific processing operation has been included in the Global Health EDCTP3 JU Public Register with the following Record reference: DPO-05-03.