



EUROPEAN COMMISSION

## **PROTECTION OF YOUR PERSONAL DATA**

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

**Processing operation: Covid-19 pandemic crisis – follow-up of staff health and safety**

**Data Controller: HR.D**

**Record reference: DPR-EC-04906**

### **Table of Contents**

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

## **1. Introduction**

The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy. The Commission 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) No 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 processing operation “COVID-19 pandemic crisis - follow-up of staff health and safety” undertaken by HR.D is presented below.

## **2. Why and how do we process your personal data?**

The purpose of the processing of personal and medical data is to establish a list of the number of staff members affected by COVID-19 virus (positive/suspected), as well as close contacts of those Covid-19 positive, in order to be able to do the necessary follow up and implement the measures to protect staff during the COVID-19 pandemic crisis. The collected information will enable the Commission to implement procedures and policies to reduce the risk of infection in its premises, to protect the health of its staff and to provide adequate follow up.

This purpose is achieved via different modes of processing:

- Notification on being Covid-19 positive via Covid-19 Self-Declaration Form, in line with the Medical Protocol  
<https://myintracomm.ec.europa.eu/coronavirus/Documents/medical-protocol-for-staff.pdf>
- Voluntary testing performed in the Medical Service
- M-Tracker application

The collection of data is done through Covid-19 Self-Declaration secured page <https://webgate.ec.testa.eu/eHealth/> . Declaration is done on voluntary basis except in case staff member has been physically present in the office over the last 48 hours before testing positive. In such case staff is obliged to notify the Medical Service.

There is no specific download or installation required on mobile devices as these applications are web based and visible on any computer connected to TESTA interinstitutional network.

The identification and authentication of staff is done using the EU Login (see DPR-EC-03187.1 - Identity & Access Management Service (IAMS)).

The web based application eHealth is not storing personal information on mobile, computer or tablets, the transmission of data to the server uses an encrypted protocol HTTPS.

The personal data is collected through the means above and submitted and stored in SERMED system (IT platform using an encrypted oracle databases storage).

The application is not collecting unrelated or not needed information, which may include communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

In a very limited number of cases, data on Covid test results is also collected via voluntary testing performed by the Medical Service, both antigen testing and PCR (polymerase chain reaction) tests. Medical Service in a limited testing capacity offers a testing on voluntary basis to persons who are performing critical tasks, interruption of which could jeopardise the normal functioning of the Commission, and for cases where having a negative test is necessary for essential missions. In case of the PCR test, Medical Service only acts as a testing centre i.e. it takes the sample but the analysis is done by the external laboratory under contract. Test results are sent back to the Medical Service and Medical Service informs data subject. In case of rapid antigen test, the whole process is done at the Medical Service (taking a sample, analysis and generation of test results.) The data collected through the means above are stored and treated in the same manner as other data collected based on this record.

In order to facilitate tracing of the close contacts in the Commission premises, organisers of the events and meetings must register all the participants in M-Tracker. The registration in M-Tracker is compulsory in order to identify and trace participants in case of a COVID-19 infection. Organisers can upload the details of everyone involved in the meeting using M-Tracker. If possible, they should list participants' names in the order that people are sitting next to each other. Personal data registered in the M-Tracker are last name, first name and email address of the meeting participants. The meeting organiser can add the company name and cell phone number as non-mandatory information. There are no special categories of data registered in the M-Tracker. Access to M-Tracker is only given to Medical Service for tracking. For a given name, information about other participants to the same meeting can be retrieved for tracing in case of Covid-19 infection.

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

We process your personal data, because, in accordance with Article 5(1) (a) of Regulation 2018/1725, this "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" and Article 1 (e) of the Staff Regulations of officials according to which "Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties".

We process medical data of personal data indicated in Section 4, because the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (Article 10 (2) (i) of the Regulation 2018/1725).

### **4. Which personal data do we collect and further process?**

In order to carry out this processing operation HR.D collects the following categories of personal data:

- first name
- last name
- service
- place of employment
- medical status (COVID-19 symptoms; info on COVID-19 symptoms of household member – no names)
- result of the test (when the need for testing has been confirmed)

- time of onset of COVID-19 symptoms (if any)
- list of close contacts with the staff member concerned over a period to be determined on a case-by-case basis after appearance of the first symptoms (in case the staff member was at the office during the recent relevant period)
- number of the office and building floor of the staff member concerned (in case the staff member was at the office during the recent relevant period)
- time of recovery necessary for resuming work of the Covid-19 infected or suspected staff member
- vaccination status and/or previous Covid-19 infection (this additional information is necessary because the follow-up measures are different based on the vaccination and recovery status).
- healthcare information regarding the evolution of the disease (for instance, hospitalisation, treatments, etc.
- personal data registered in the M-Tracker are last name, first name and email address of the meeting participants. The meeting organiser can add the company name and cell phone number as non-mandatory information. There are no special categories of data registered in the M-Tracker.

#### **5. How long do we keep your personal data?**

Your personal data are only kept for the time necessary to fulfil the purpose of collection or further processing, namely:

- Note that the staff member was infected with Covid-19 and date of the positive test result/of reporting is stored in the medical file of the staff member and kept in accordance with the retention period applicable to these files, 30/40 years (see record DPR-EC-01837 (legacy notification DPO-496)).
- The COVID-19 contact points in OIB and/or OIL keep your personal data for 5 years.
- List of participants registered in M-Tracker is kept for one month, after which data are anonymised.
- All data related to the follow up and tracing except for the note that staff member was infected with Covid-19 and when, will be deleted 14 days following the complete follow up and tracing. Automated timeframe for a complete follow up and tracing will be set for 2 months i.e. data will be deleted 14 days following 2-month period starting from the notification to the Medical Service. Under specific circumstances justified by medical situation, such as Covid-19 complications or hospitalization, a longer retention period will be applied but in any case, 14 days after the end of complete follow up/tracing data will be deleted.
- Data that was gathered via the SharePoint (old reporting tool used until 02 February 2022) will be extracted from that reporting tool. Part of that data will be saved in each individual medical file and the rest will be deleted, in line with above listed retention periods. Data that was gathered via the SharePoint is kept until relevant data is extracted and aligned with the new retention periods. This project will be finalized within next 6 months.

#### **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 on the servers of the European Commission. All processing operations are carried out pursuant to the [Commission Decision \(EU, Euratom\) 2017/46](#) of 10 January 2017 on the security of communication and information systems in the European Commission.

In order to protect your personal data, the Commission 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.

Access to information concerning the staff experiencing COVID-19 symptoms and/or tested COVID-19 positive was compiled and shared via a SharePoint site. After 02 February 2022 data from SharePoint will be extracted from that reporting tool. Part of that data will be saved in each individual medical file and the rest will be deleted, all in line with the retention periods.

SharePoint as a tool will be deleted and no longer accessible.

All data in electronic format (emails, documents, downloaded data, etc) are stored on encrypted drive accessible only to members.

The Covid-19 Self-Declaration Form is secured with EU Login and it is not a downloadable application.

The Covid-19 Self-Declaration Form is an interface towards the functional mailbox and it is not storing any information on mobile, computer or tablets or access to information already stored in the terminal. It is not using any individual tracking technology, location device (GPS) or proximity tracking (Bluetooth or other proximity detection protocol). The application is not collecting unrelated or not needed information, which may include communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.

The marking "Sensitive" is applied to all documents registered in ARES. All the recipients apply strict measures to ensure that personal data are not accessed by anybody else. This includes the use of locked closets, encrypted email and printing with badging. The controller applies the principles set out by the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

M-Tracker is an application composed of a front office for employees to register meetings, a back office for Medical Service online investigations and a MySQL database to store information.

## **7. Who has access to your personal data and to whom is it disclosed?**

Access to your personal data is provided to the Commission 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.

- Full access:
  - Director of Directorate HR.D (Health & Wellbeing - Working Conditions), controller of this processing and their assistants;
  - The Heads of Unit of the Medical Services in Brussels, Luxembourg and Ispra;
  - Doctors and other medical professionals of the Medical Services in Brussels, Luxembourg and Ispra;
  - Administrative staff member of the Medical Service designated to follow the list of COVID-19 cases and tasked with assisting medical professionals with administrative follow up;
  - COVID-19 IT contact point for DG.HR (until SharePoint is disabled and deleted);
  - Doctor of the EEAS who is in charge of Commission's staff in delegations;

- Contact point in OIB, OIL or other processor providing the cleaning/sanitation in order to provide necessary sanitation of offices and shared spaces.
- Specific access regarding individual case:
  - Directors General, Assistants to the Directors General of the DG/services of the staff member and Business Correspondents team have access only to the information of the specific case concerning their DG/service that they have reported themselves (until SharePoint is disabled and deleted);
  - Line managers of the person concerned inform the Director-General and the HR Business Correspondent of any situation requiring particular attention. They also inform the Medical Services and the list close contacts established together with the Medical Service. This in only if they were notified by the staff member themselves.
- Access to the data collected (access to aggregated data only without names):
  - EC Secretary General and assistants;
  - Members of Cabinet of the Commissioner in charge of Budget and Administration;
  - DG and DDG of DG HR and their assistants;
  - Participants in the Covid-19 coordination meeting at the level of the Commissioner in charge of Budget and Administration.

The name and other justified information may be reported to local health authorities, in line with national requirements.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

## **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).

You can exercise your rights by contacting the Data Controller, or in case of conflict the 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.

## **9. Contact information**

### **- The Data Controller**

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 Data Controller, HR.D, (for Brussels [HR-MAIL-D3@ec.europa.eu](mailto:HR-MAIL-D3@ec.europa.eu); Luxembourg [HR-LUX-SERV-MEDICAL@ec.europa.eu](mailto:HR-LUX-SERV-MEDICAL@ec.europa.eu) and/or Ispra [HR-ISP-MEDICAL-SERVICE@ec.europa.eu](mailto:HR-ISP-MEDICAL-SERVICE@ec.europa.eu)).

- **The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer ([DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:DATA-PROTECTION-OFFICER@ec.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 ([edps@edps.europa.eu](mailto: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 Data Controller.

**10. Where to find more detailed information?**

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: <http://ec.europa.eu/dpo-register>.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-04906.