EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO THE EXTRAORDINARY MEASURES IN VIEW OF THE COVID-19 EMERGENCY BY THE EEAS

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS), including the Delegations of the European Union, more than ever in this extraordinary situation linked to the COVID-19 emergency. We would like to reassure you of our commitment to respecting your rights regarding personal data collected and processed relating to the coronavirus pandemic. You have the right under EU law to be informed when your personal data is processed [collected, used, stored] as well as about the purpose and details of that processing. When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular Article 8 on data protection. Your personal data are processed in accordance with Regulation (EU) 2018/1725 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, aligned with Regulation (EU) 2016/679, the General Data Protection Regulation. In this privacy statement you find information about how the EEAS and EU Delegations process your personal data and what rights you have as a data subject. Your data will not be handled for all of the processing activities listed in this privacy statement. Under Point 2 you will find various purposes related to the COVID-19 emergency context. Please note that most of these data processing activities do apply under standard circumstances as well, nonetheless some additional personal data may be processed for specific and explicit purposes outlined below.

2. PURPOSE OF DATA PROCESSING: Why do we process your data?

The overall objective of the processing activities under this record is to ensure fulfilling the necessary public health measures and to protect EEAS/EU Delegations' staff and third parties, including external visitors by containing and preventing the spread of the Coronavirus (COVID-19) in the current emergency. For this purpose additional information, including health related data, needs to be collected and retained, to allow for identification of infected individuals, persons suspected to be contaminated and persons at risk. Health related data, is primarily collected and coordinated by the Medical Service in cooperation with the COVID-19 Taskforce. In particular, prior to the confinement measures, data related to health condition and travel history have been collected by the various services at EEAS Headquarters and by EU Delegation Administrative Sections before meetings were to be held; either ahead of the meeting by mail or at the entry. In case meetings are necessary to be held during the confinement period, the aforementioned data are collected for the same purpose. Where the standard procedures of the EEAS apply and no additional data is collected or processed, the documentation recording the data processing activities and their linked Privacy Statements are fully relevant and pertain.

In order to achieve the objectives of curbing the epidemics several data processing activities are necessary:

- **Managing emergency related requests with new dedicated functional mailboxes** (FMBs)
  Three FMBs are set up to provide support to both EEAS/EU Delegation staff:
  - **CORONA-MED-SERVICE@eeas.europa.eu**
  - **CORONA-ADMIN@eeas.europa.eu**
  - **help-in-confinement@eeas.europa.eu**
- **Processing of additional information, including health related data for the purpose of protection of public health and notification of staff and other individuals**
  Data need to be collected and retained, as contaminated individuals and persons at risk have to be identified. Staff consults the EEAS Medical Service if COVID-19 contamination is established or suspected. These staff members are requested to stay in self-isolation and asked to provide the identity of other individuals whom they have been in contact with. Persons, identified as known contacts, including dependents and EU institutions' staff, are tracked down, based on criteria agreed within the Interinstitutional Medical Board and are notified that they may have come into contact with a COVID-19 positive colleague. The disclosure of the name of a person contaminated or suspected to be contaminated is avoided (EEAS DPO guidance – March 2020). The EEAS Medical Service, when performing contact tracing will disclose the minimum amount of information in order to achieve the objective of the contact tracing. In accordance with the data minimisation principle staff members who have been identified as close contacts of an infected individual only receive the aforementioned 'de-personalised' information, as identified contacts do not need to know the identity of the person contaminated or suspected to be contaminated in order to protect themselves and follow instructions in that particular situation. Individuals, in particular other than staff members who have been in contact with a COVID-19 positive colleague, or have symptoms of the coronavirus, but not yet been tested or waiting for results, need to be tracked down and notified. Adequate and limited data only relevant for the purpose may be transferred to EU Medical services and healthcare institutions (hospitals) or to national authorities, as appropriate. Contacts outside the EU institutions will be notified in general by authorities about the risk and what measures to be taken, without naming the person who has given the information.
  Staff members, who through a third party or others means, become aware of the identity of a colleague infected with COVID-19 are required to respect the privacy and confidentiality of the affected staff member.
- **Storage of specific data related to COVID-19**
  Specific data, required for emergency measures and for follow-up on cases of contamination and on suspected infection, need to be stored in properly secured folders for the explicit purpose of protection of health.

- **Access control for staff at Headquarters / EU Delegations**
  During the emergency period, entry to Headquarters and Delegations is limited to certain categories of staff depending on the business continuity requirements of the service, this way a list of critical staff is established. Access control is automatically implemented with the badge readers; no additional system is in place. Entry to premises during confinement: as of 16 April 2020 at certain premises, including the Cortenbergh building at Headquarters, control was introduced to allow only staff members on the 'critical staff' list. Office location (floor, section, office number) is requested from staff members permitted to the building and recorded solely for regular cleaning purposes. List of entry attempts from non-critical staff was not registered. Entry since de-confinement measures are in place (Message of the Secretary General 19 May 2020): staff in agreement with line managers may return gradually to the office. For access control purposes no additional data of staff (badge data) are collected.
- **Data processing of (potential) visitors / Access control for visitors**
  In the context of the COVID-19 pandemic prevention measures additional personal data are processed apart from the standard identification and ID document details of visitors for access control. Ahead of attending any meeting at EEAS/EU Delegation premises, in particular prior to the confinement measures and during the de-confinement process, external visitors are requested to provide information on their health status, travel history and indicate risk factors by filling in a brief questionnaire before arrival to Headquarters (via the eVISITOR system) or to Delegations or by confirming information on health status and travel history at the entry to certain Delegations. This questionnaire contains questions on whether visitors have symptoms of fever, tiredness, dry cough, loss of smell or taste and whether visitors have been in contact with anyone who tested positive with Covid-19 in the last 14 days. An additional question has been also included whether visitors have travelled to areas of risk. If the answer to any of the questions is 'yes', visitors are requested to reconsider the form of the visit and make arrangements for an alternative solution, including a video-conference. The information (replies to the questions) has been collected and processed by the EEAS services (at present via the eVisitor tool), the EU Delegation section organising a meeting or by the Administrative section of the Delegation. This practice has been in place since 7 March 2020. Visitor entry at Headquarters was not relevant since confinement as of 16 March till 19 May 2020. As of 19 May 2020 with gradual de-confinement data collection is implemented by the eVISITOR system at EEAS Headquarters.
- **Coordination of repatriation, voluntary return as well as consular support of expatriate staff for the purpose of returning to the EU related to the COVID-19 emergency**
  To assist the effective coordination of consular crisis response specific data required for the emergency measures and for preparation of departure from certain host countries of EU Delegations need to be collected and managed. The Administrative sections, staff in charge of consular affairs of relevant Union Delegations, coordinate repatriation and support EU Member States with the return of EU Citizens who contacted their consulates expressing request to be repatriated. Data processing takes place by receiving information and creating consolidated list of passengers from Delegations and Member State embassies as well as consulates. These return travels are carried out via commercial or consular flights. Up-to-date information and additional data may be processed, in particular in EU Delegations, about the presence or location of staff if necessary, including for eventual repatriation or follow-up purposes. Repatriation organised by EU Member States and supported by EU Delegations may necessitate data collection, including – when absolutely necessary – special categories of data and might involve coordination activity as well as transmission of data to or reception of data from Member State embassies/consulates in the same host countries as EU Delegations. To be noted that processing of personal data for the purpose of evacuations in general is separately documented ("*Evacuations and Contingency Plans by EU Delegations*").
- **Processing personal data for the purpose of office disinfection**
  In accordance with the safety measures in place for the corona virus emergency, the offices of staff members contaminated or suspected to be contaminated with COVID-19 must be disinfected. In order to carry out the necessary duties the Division Infrastructure and Safety, responsible for disinfection of offices, needs to receive names of suspected/probable/confirmed cases from the Medical Service. There is no retention or onward transmission of personal data, only the office numbers are subsequently processed. The de-personalised data (office number) are shared with the European Commission Office of Infrastructure and Buildings and with the cleaning company for the purpose of organising the disinfection.
- **Extraordinary opening of postal mail**
  In order to dispatch paper mail electronically, inward professional postal mail is opened and scanned. The scanned copy is sent to the addressee by e-mail so that colleagues can access and process it while teleworking. Envelopes addressed to certain staff members (e.g. to staff of the Medical Service) or marked "personal", "confidential" are not opened. If a letter is opened by error, a warning is written on the envelope. In order to perform their duties, critical staff may open the mail delivered to the different departments, for further processing for professional purposes. None of these activities is for the purpose of processing personal data, which is avoided in so far as possible.
- **Processing of data via open sources for compiling up-to-date information and in the fight against disinformation**
  Specific coronavirus news monitoring (COVID-19 Headlines) is established and issued by the EEAS Situation Room. Only open source information is used. In addition, due to the fact that disinformation in the health space is thriving, including on COVID-19, it is important that EU institutions and bodies, including the EEAS and the European Commission, are leading to provide information relying only on authoritative sources to get updated information on the COVID-19 outbreak. The EEAS issues analysis on the information environment and disinformation situation related to Covid-19. The document produced is a snapshot of the actual current situation and is meant to provide additional background elements for policy making and communications activities and it does not contain any personal data. In line with the mandate of the EEAS and the Strategic Communications Task Forces, the EEAS in close cooperation with the European Commission aim at combatting disinformation also cooperating with online platforms, which are encouraged to promote authoritative sources, demote content that is fact-checked as false or misleading, and take down illegal content or content that could cause physical harm. The disinformation report is shared with colleagues in EU institutions, the Member States (e.g. via the Rapid Alert System) and selected international partners. It brings together a variety of sources inside and outside the institutions, using open source material. Personal data is non-deliberate, not intended to be specifically collected and not further processed in any way.

- **Processing data for facilitating movement/travel of staff members and the members of their household as per the Vienna Convention on Diplomatic Relations (VCDR) of 18 April 1961:** Based on the official measures imposed by the Belgian Government, travel restrictions to/from the Belgian territory are imposed in order to contain the spreading of the Covid-19 virus. These measures are not applicable to staff members with an essential function. Hence, under the legal obligation set out by the Note Verbale of the Belgian Government P0.0/PRO.3143/17.07.2020/COVID-19/11 dated 17 July 2020, the EEAS is bound to share information on staff members travelling to/from the Belgian territory, as well as the members of their households, in order to ensure their travelling to be duly authorised by the competent Belgian authorities.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed for that purpose are the following:

- Identification and contact data of all concerned individuals
  - EEAS and EU Delegations' staff
  - Staff of other institutions and Member States' representatives
  - EU citizens requesting consular support in relation to repatriation
  - External visitors
  - Staff travelling to/from Belgium under the framework of the Rotation 2020 exercise, included in 'Taking Up Duty' lists
- Health related data in relation to the corona virus pandemic situation:
  - Appearance of symptoms of concerned individuals
  - Medical conditions, including underlying health conditions, if any, for staff, in particular in EU Delegations
  - Fact of being infected, tested positive with COVID-19 or at risk for staff
  - Risk factors for prospective visitors
  - Travel history of staff and prospective visitors
  - Office number of staff
  - Family composition and need for special assistance of concerned individuals in particular for the purpose of repatriation
- Specific up-to-date information and additional data may be processed, in particular in EU Delegations about the presence or location of staff if necessary for a specified, explicit and legitimate purpose, including any follow-up actions

4. DATA CONTROLLER: Who is entrusted with processing your data?

The data controller determining the purpose and the means of the processing activity is the European External Action Service.

European External Action Service (EEAS)
Rond Point Schuman 9A, 1046 Brussels, Belgium
Secretariat-General (EEAS.SG) and Directorate-General for Budget and Administration (EEAS.BA)
EEAS COVID-19 Taskforce

5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?

The recipients of your data may be

- Medical Service (EEAS.BA.HR.3 – Section on medical repatriation and medical support)
- Dedicated senior and middle management
- Assigned staff of the Secretariat-General (EEAS.SG)
- Assigned staff of the Directorate-General for Budget and Administration (EEAS.BA)
- Assigned staff of the Deputy Secretariat-General for CSDP and Crisis Response (EEAS.DSG-CSDP-CR)
- Assigned staff of the Directorate for Inter-institutional relations, policy coordination and public diplomacy (EEAS.AFFGEN)
- Assigned staff of the Directorate for Human Resources (EEAS.BA.HR)
- Assigned staff of the Directorate for Security and Infrastructure (EEAS.BA.SI)
- Assigned staff of the Directorate for Budget and Support (EEAS.BA.BS)
- Organisers of meetings in EEAS services being tasked to request additional data on health status and travel history
- Healthcare institutions (hospitals)
- Authorities of the host country (Belgium), i.e. Ministry of Foreign Affairs (Federal Public Service Foreign Affairs of the Kingdom of Belgium – Foreign Trade and Development Cooperation)

Access is on a need-to-know basis.

Primarily, personal data are not intended to be transferred to a third country or an international organisation. Under exceptional circumstances, information about contaminated staff members, third parties or individuals suspected to be contaminated may need to be processed by medical institutions of the host countries of EU Delegations. Local hospitals selected by EU Delegations may receive data about staff members for the eventual need to be tested and to be admitted to hospital, if required.

The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

6. ACCESS, RECTIFICATION, ERASURE OF DATA: What rights do you have?

You have the right of access to your personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed. Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you. For more detailed legal references, you can find information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. If you would like to exercise your rights or have questions concerning the processing of your personal data, you may address them to the Data Controller via the functional mailbox:

CORONA-ADMIN@eeas.europa.eu and **CORONA-MED-SERVICE@eeas.europa.eu**

7. LEGAL BASIS: On what grounds do we collect your data?

- Data, including health-related information is processed pursuant to Article 10.2 (b),(c), (g), (h) and, in particular to (i) public interest in the area of public health, as well as to Art. 10.3, in addition to Art. 5.1 (a) necessity for the public interest in the exercise of duty of care and Art. 5.1 (e) vital interest of individuals
- 2010/427/EU Council Decision of 26/07/2010 establishing the organisation and functioning of the EEAS (OJ L 201)
- ADMIN(2017)10 Decision of the High Representative of the Union for Foreign Affairs and Security Policy on EEAS Security Rules
- Council Directive 2015/637 of 20 April 2015 and Article 23 TFEU on consular protection in a third country
- Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community(OJ 45, 14.6.1962, p. 1385)

8. TIME LIMIT - DATA STORING: For what period and how do we process your data?

Data, including health related information, collected in the context of the COVID–19 emergency situation is intended to be kept not longer than necessary for that specific purpose. Data should accordingly be retained only as long as the crisis situation related to the pandemic is upheld with a subsequent technical retention until deletion, destruction or anonymisation of data could be implemented. The following categories of data is intended to be kept for the specific periods outlined:

- Data concerning contamination or risk factors provided on a voluntary basis by prospective visitors prior to meetings, held before the confinement measures, are to be kept for 14 days (timeframe according and adjusted to updated information issued by ECDC or WHO for the incubation period) unless it is necessary to keep them longer for reasons of protection of public health, including when a contamination makes it necessary to ensure the possibility to warn individuals who are at risk of contamination.
- Data related to staff members whose contacts need to be notified are kept until follow-up safety or other measures are necessary.
- Information about office numbers (de-personalised data) held for ordinary cleaning purposes are kept only until necessary to organise and execute the cleaning as well as for administrative (invoicing purposes).
- Data, related to staff members and office locations in relation to confirmed or suspected COVID-19 cases, are kept in an identifiable format for a very brief period of time (less than a week, as possible) in order to organise disinfection or sealing of an office or other necessary premises.
- Specific up-to-date information on presence in the building and location is to be kept until epidemics is declared to be ceased.
- Emergency related medical information, including underlying health conditions, received via the dedicated FMBs as a response to the Note of the Director General for Budget and Administration to Heads of Delegations on COVID 19 crisis-clarification on administrative and financial issues (ref. Ares(2020)1764137 - 25/03/2020) will be retained as part of the continuous EEAS Health and Safety risk inventory and evaluation towards location and personnel for the purpose of follow-up assessment and advice of the EEAS Medical Service on repatriation, relocation or return to Europe.
- Medical data of positive COVID-19 EEAS staff members will be kept in their medical filing system.
- Data collected by the dedicated functional mailboxes is foreseen to be kept until the crisis situation is officially upheld (with a subsequent period up to 12 months from the date of the closure of the mailboxes).

Data collected at entry for standard access control purposes is to be kept in accordance with the ordinary access control retention periods for EU staff and visitors. The processing is documented and Privacy Statements are made available. In case of an incident, event or enquiry by authorities, data subjects or other concerned individuals personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. It may be necessary to keep data until all claims and any follow-up to them expire. The personal data shall, however, be kept not longer than 5 years after the judgment on the pending case is final. Data is intended to be kept in an anonymised form for statistical purposes, to the extent possible, taking into account secure technical measures.

Security of data

Data is kept secured. Appropriate organisational and technical measures are implemented according to Article 33 of Reg. (EU) 2018/1725. Collected personal data are stored on servers that abide by pertinent security rules. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. Access to EEAS servers and equipment is password-protected with appropriate authentication policy. Data is processed by assigned staff members. Access to specific files requires authorisation. General access to personal data is only possible to recipients with a UserID/Password. Physical copies of personal data, if created, are stored in a properly secured manner.

Specific access limitation with regard to special categories of data: General access to special categories of data (health related) data is granted only to the Medical Service. Other assigned staff members have access to certain data only on a need-to-know basis (in particular as part of managing the functional mailboxes for the Covid-19 emergency. Access to the functional mailboxes (CORONA-MED-SERVICE@eeas.europa.eu; CORONA-ADMIN@eeas.europa.eu; help-in-confinement@eeas.europa.eu) is restricted.
Envelopes addressed to certain staff members (e.g. to medical staff) or marked "personal", "confidential" are not opened. If a letter is opened by error, a warning is written on the envelope. In order to perform their duties, critical staff may open the mail delivered to the different departments, for further processing for professional purposes. For the purpose of disinfection, the number of persons with access to the information is limited. Only one person has access to the special category of data received from the Medical Service. Additional two line managers have access to the de-personalised information on the office location.

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

If you have enquiries you can also contact the EEAS Data Protection Officer at data-protection@eeas.europa.eu.

10. RECOURSE

You have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.