European Union
EXTERNAL ACTION

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

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

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 pandemic. 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 Corona virus (COVID-19) during the current pandemic. For this purpose, additional information, including health related data, needs to be collected and retained, to allow for identification of contaminated 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 CORONA Task Forces. In particular, prior to and subsequent to the confinement measures, data related to health condition and travel history are to be collected by the various services at EEAS Headquarters and by EU Delegation Administrative Sections, either ahead of the meeting by mail or at the entry. In case meetings were necessary to be held during the confinement period, the aforementioned data had been collected for the same purpose. Where the standard procedures of the EEAS apply and no additional data is processed, the documentation recording the data processing activities and the linked Privacy Statements are relevant and pertain. In order to achieve the objectives of curbing the pandemic several data processing activities are necessary:

- **Managing COVID-19 related requests with new dedicated functional mailboxes** (FMBs) to support EEAS/EU Delegation staff:
  - **CORONA-MED-SERVICE@eeas.europa.eu**
  - **CORONA-ADMIN@eeas.europa.eu**
  - **HELP-IN-CONFINEMENT@eeas.europa.eu**
  - **CORONA-BUDGET-REQUESTS@eeas.europa.eu**
  - **TASK-FORCE-VACCINE-STRATEGY@eeas.europa.eu**
  - **COVID-19-VACCINATION@eeas.europa.eu**
  - **EEAS-DATA-TRANSFER-EU-COVID-CERTIFICATE-CONSENT@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, including any contact with contaminated persons. 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 Inter-institutional 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 in hard copy or electronically for the explicit purpose of protection of health.
  Data are processed and stored by the KITRY system, a recognised occupational health and safety software solution hosted by CEGEDIM, also used for COVID related information. PCR tests can be prescribed by EEAS Medical Service medical doctors, foreseen also by means of the electronic system used by the EEAS Medical Service. The KITRY standard Medical Module allows to register health data and to plan consultations with EEAS staff members in Headquarters and in EU Delegations and Commission staff posted in EU Delegations in any way affected by the COVID pandemic, either being infected, tested positive or are at risk. The KITRY Questionnaire Module permits the Medical Service to send questionnaires related to the COVID pandemic, including the specific survey on Covid-19 vaccinations. The privacy statement on the activity of the Medical Service is on the EEAS website.
- **Access control for staff at Headquarters / EU Delegations**
  Entry since measures of de-confinement (SG Message 19/05/2020) and Return to Work (SG 01/09/2021 and RM 13/09/2021): staff in agreement with line managers may return gradually to the office. Occupancy rate is controlled in light of varying threshold of presence in the office. For access control purposes no additional data of staff (badge data) are collected. During the emergency period, from the 27/03/2020 to the 26/05/2020, entry to Headquarters and Delegations was limited to certain categories of staff depending on the business continuity requirements of the service, this way a list of critical staff was established. Office location (floor, section, office number) was requested from staff members entering to the building and recorded solely for office cleaning purposes. The list of staff entering the building and their office numbers is shared with OIB to be transmitted to the cleaning provider. List of entry attempts from non-critical staff was not registered and no other control system has been in place.
- **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 as well as during the gradual Return-to-Work period, external visitors are requested to provide information on their health status and indicate risk factors by filling in a brief questionnaire before or at arrival to Headquarters (via the eVISITOR system) or to Delegations as well as 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 was formerly also included whether visitors have travelled to areas of risk, in particular in Delegations. 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. Replies to the questions are collected and processed via the eVISITOR tool in Headquarters (HQ), by the EU Delegation section organising a meeting or by the Administrative section of the Delegation. This practice has been in place since 07/03/2020. In HQ visitor entry was not relevant due to confinement 16/03/2020 - 19/05/2020; as of 25/05/2020 with gradual de-confinement, continued in accordance with 13/09/2021 Return-to-Work measures data collection is implemented by the eVISITOR system. As of 15/10/2021 external visitors are requested to exhibit either a proof of vaccination, a certificate of recovery or a negative Nucleic Acid Amplification Test (NAAT) of less than 72h or a Rapid Antigen Test (RAT) of less than 48h to be checked at entry with no further data storage. The Privacy Statement is available @ EEAS Privacy Statements.
- **Coordination of repatriation, voluntary return, consular support of expatriate staff for the purpose of returning to EU**
  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 personal data processing for the purpose of evacuations is separately documented.
- **Processing personal data for the purpose of office disinfection**
  In accordance with the safety measures in place for the COVID pandemic, the offices of staff members tested positive must be closed off and disinfected. In order to carry out the necessary duties the Division Real Estate, Safety and Greening, responsible for the coordination of disinfection of offices, receives only the office number of positive cases from the Medical Service. The office number with eventual location data of common areas, i.e. kitchenette, are shared with the HQ Security for closing the area concerned and the European Commission Office of Infrastructure Brussels (OIB) for the purpose of organising the disinfection and transmitting the necessary information to the cleaning company. OIB is to provide a 'retour d'intervention' to the Facility Manager and a notice to HQ Security to open up the area, once the disinfection has taken place. The name tags next to the offices to be disinfected are being covered, leaving only the information of office numbers visible.
- **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.
- **Processing data for facilitating compliance with confinement rules and return to work (de-confinement) of staff**
  In order to assist staff and their family members living in the same household in vulnerable situations, those who tested positive or are subject to restrictions by national authorities, exceptions to the teleworking rules, the rules concerning rest leave and to the procedure of returning to office after the pandemics (de-confinement process) can be authorised and in these cases, information is captured in the register of exceptions and non-compliance events and the following costs are reimbursed to staff where justified:
  ▫ Reimbursement of PCR testing ▫ Reimbursement and transfer of rest leave ▫ Reimbursement of quarantine costs
  Medical data is processed via Kitry, an occupational health and safety software system. The privacy statement on the activity of the EEAS Medical Service via the Kitry system is available on the EEAS website under Data Protection and Privacy Statements.
- **Processing personal data for the COVID-19 vaccination campaign, its coordination and the related survey**
  To implement prevention measures, the EEAS proceeds with the COVID-19 vaccination campaign. To set priorities, a vaccination related survey was launched in January 2021. The survey collected data, including data of being infected or having tested positive with COVID-19, certain vulnerability factors defining priority for the COVID-19 vaccination, contra-indications and precautions as well as location data. Based on the collected data the priority groups for vaccination were determined and indicated to the Medical Service of the EEAS and of the European Commission; including the risk factors related to the vaccination, as the EC Medical Service have administered vaccines. Limited data may be transmitted to the Budget Division for reimbursement purposes. Vaccines, including booster doses, are to be administered by the EEAS Medical Service. The Paronella (DOCLR) application, also used by the Belgian authorities responsible for COVID-19 vaccination, allows for the EEAS Medical Service to manage appointments for vaccines. Health related data is collected by a specific consent form. If applicable, data about vaccination related information, including priority groups with risk factors may be also indicated to local healthcare authorities and institutions, in case local authorities' designated healthcare services might be involved in the recording within a national vaccination-specific database and/or in the process of administering the vaccines. The privacy statement on the activity of the EEAS Medical Service via Kitry, an occupational health and safety software system is available on the EEAS website under Data Protection and Privacy Statements. The dedicated functional mailbox is set up for arrangements of vaccination along with collection of information (temporary NISS number) for facilitating access to vaccination certificates.
- **Processing personal data to provide COVID Vaccination Certificates and the follow-up of the progress of vaccinations**
  In order for staff and their family members having or eligible for a Belgian Special Identity Card to send the necessary information to the Belgian authorities to receive the digital key allowing to access public sites, including the Ma Santé portal for obtaining the EU Digital COVID Certificate, the European Commission (EC) adjusted Sysper to offer this option. Access to the module for EEAS staff and their family members shall be provided to enable the data transmission from the EEAS to the EC. EC DG HR is responsible for the transmission of personal data to the Belgian authority (DG Digital Transformation of the Federal Public Service Strategy and Support 'BOSA'). Consent is collected via: EEAS-DATA-TRANSFER-EU-COVID-CERTIFICATE-CONSENT@eeas.europa.eu.
  For Delegation staff and their family members that have never resided in Belgium, data and passport copy are collected via an ad hoc questionnaire to create a temporary NISS number, encode vaccines into the BE vaccination registration system (VACCINNET) and allow access to 'MaSante' by creating a Helena code via Care Connect (Corilus).
  Data collected about vaccination are also used to follow the progress of vaccination.
- **COVID-19 Vaccine Strategy Task Force**
  In order to maximise the added-value of the EU global response to the COVID-19 pandemic and to support partner countries in accessing the vaccines, the task force coordinates and steers the issues related to COVID-19 global response within the EEAS, including the vaccine-sharing mechanism as well as the vaccination strategy. Vaccine Strategy Task Force activities comprise:
  - providing information and advice to the HRVP and the Cabinet
  - coordination and exchange of information with the Commission, with the Council and Member States
  - multilateral coordination with key actors, in particular in the area of vaccination strategy for EU Delegations colleagues
  - clearance of main outputs, among others in the field of public diplomacy, communication and countering disinformation

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 the following categories of individuals:
  - EEAS and EU Delegations' staff and their family members living in the same household
  - Staff of other institutions; Member States' representatives, including contact persons of Vaccine Strategy Task Force
  - 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
- Office number of concerned staff
- 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, and their family members living in the same household
  - Risk factors for prospective visitors
  - Travel history of staff and prospective visitors presenting symptoms or other contamination risk to staff and external individuals
  - Fact/symptoms of being contaminated, having tested positive with COVID-19, being in contact with an infected individual
  - Vulnerability factors determining priority of COVID-19 vaccination and defining rights for travel reimbursements, or justifying exception to teleworking rules, the rules concerning rest leave or the de-confinement process
  - Data related to PCR testing
  - Data related to exceptions to rest leave and teleworking rules (including entries in the register of exceptions and non-compliance events)
  - Quarantine or similar obligations prescribed by national administrations in the host country or during travel
  - Cost of quarantine or PCR testing
  - Contra-indication/pre-caution related to COVID-19 vaccination, including current or planned pregnancy
  - Location data, incl. travel and telework locations where necessary for the exceptions from rules or reimbursement of costs
  - Family composition and need for special assistance of concerned individuals in particular for the purpose of repatriation
- Data related to administering vaccines: name , staff number, e-mail, date of birth, Belgian NISS/BIS, vaccination dates and time, lot number, brand name, vaccinator, contraindications, caution factors and other relevant health data
- 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
- Personal data, including temporary NISS number and copies of identification documents for issuing the vaccination certificate.
- Personal data collected by the EEAS or the European Commission and transmitted to the Belgian authority 'BOSA' for issuing the vaccination certificate - For Officials and other servants: Personal ID, Full name, Date of birth, National registration number (NISS/BIS), passport number/copy, e-mail address; - For Family members (if any): Full name, Date of birth, Relation with staff member, National registration number (NISS/BIS), passport number/copy, e-mail address.
- Data about vaccination collected for monitoring the progress of the Vaccination campaign, except for sensitive medical data.
- Specific information about the progress of vaccine-sharing and vaccination and its results for the purposes of coordination, advice and communication concerning the vaccine strategy within the field of activity of the Vaccine Strategy Task Force.

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), Directorate-General for Resource Management (EEAS.RM), EEAS CORONA - COVID-19 Task Forces

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

The recipients of your data may be

- Medical Service (EEAS.RM.HR.3 – Section on medical repatriation and medical support)
- Dedicated senior and middle management
- Assigned staff of the EEAS CORONA and COVID-19 Task Forces (incl. CORONA-MED and CORONA-ADMIN)
- Assigned staff and contact persons of the Vaccine Strategy Task force in the EEAS, other EU institutions and Member States
- Assigned staff of the Secretariat-General (EEAS.SG)
- Assigned staff of the Directorate-General for Budget and Administration (EEAS.RM)
- Assigned staff of the Managing Directorate for Global Agenda and Multilateral Relations (EEAS.GLOBAL)
- 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.RM.HR)
- Assigned staff of the Directorate for Security and Real Estate (EEAS.RM.SECRE)
- Assigned staff of the Directorate for Budget and Support (EEAS.RM.BS)
- Assigned staff of other EU institutions, in particular the European Commission, including its Medical Service, DG HR and OIB
- In the context of the COVID-19 survey related to vaccination technical staff under the obligation of confidentiality and on instructions only, in accordance with data protection rules, for the purpose of processing results to support the Medical Service

- Organisers of meetings in EEAS services being tasked to request additional data on health status and travel history, if relevant
- Contractors providing services, including disinfection and security; DOCLR.be for vaccination appointment booking
- Vaccinnet database, Vaccination centres, Health insurance fund to which you are affiliated, if relevant
- Healthcare institutions (e.g.: hospitals) as well as local health authorities and services, including those administering vaccines
- Authorities of the host country (for Headquarters in Belgium, the Ministry of Foreign Affairs (Federal Public Service Foreign Affairs of the Kingdom of Belgium – Foreign Trade and Development Cooperation)
- Belgian authority – the DG Digital Transformation of the Federal Public Service Strategy and Support (La DG Transformation digitale du Service Public Fédéral Stratégie et Appui – 'BOSA'): https://fedweb.belgium.be/fr/d%C3%A9claration-de-confidentialit%C3%A9

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 the relevant functional mailbox:

CORONA-MED-SERVICE@eeas.europa.eu
CORONA-ADMIN@eeas.europa.eu
HELP-IN-CONFINEMENT@eeas.europa.eu
CORONA-BUDGET-REQUESTS@eeas.europa.eu
TASK-FORCE-VACCINE-STRATEGY@eeas.europa.eu
COVID-19-VACCINATION@eeas.europa.eu
EEAS-DATA-TRANSFER-EU-COVID-CERTIFICATE-CONSENT@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, supplemented by the consent of the data subjects.

Legal bases:

- 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)
- For access to the Digital Key or COVID vaccination certificates data processing is based on Articles 11 and 15 of the Protocol (No 7) on the Privileges and Immunities of the European Union and Article 9 of Regulation (EU) 2018/1725 as well as the European Commission Decision of 5 March 2021 on the transmission of personal data of Commission staff, pensioners and their family members to national health authorities in the context of COVID-19 vaccination.
- ADMIN(2021)251 Decision of the Secretary General of the European External Action Service of 12/10/2021 on Health and Safety Measures for visitors to the EEAS premises in Brussels (Ref. Ares(2021)6208970 - 12/10/2021)

Further references:

- Note Verbale of the Belgian Government P0.0/PRO.3143/17.07.2020/COVID-19/11 dated 17 July 2020
- Note Verbale of the European External Action Service NV.EEAS.2021.035 dated 8 April 2021
- Note Verbale of the Belgian Government P1/PRO.PV/12.04.2021/EEAS_Vaccin dated 12 April 2021

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 pandemic 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 by prospective visitors prior to meetings, held before and subsequent to the confinement measures as well as during the gradual Return-to-Work period, are to be kept for 30 days, taking into account the general incubation and quarantine period of fourteen days, plus one day prior to the visit (testing and feedback of results) equalling fifteen days doubled for the purposes of staff safety, tracing and duty of care (timeframe adjusted to updated information issued by ECDC or WHO for the incubation period) unless it is necessary to keep data longer for reasons of protection of public health, including when a contamination requires to ensure the possibility to warn individuals who are at risk.
- Data of visitors related to proof of vaccination, certificates of recovery or results of a NAAT/RAT tests are not kept by the EEAS.

- 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 including office locations related to positive COVID-19 cases for the purpose of closing off the area and disinfection of the office or other locations concerned are kept for a brief period of time (up to one week) or until OIB 'retour d'intervention'.
- Up-to-date information on presence in buildings, in particular in EU Delegations, including data in aggregated form for threshold percentage as well as location data, if applicable, are to be kept until the pandemic is declared to be ceased.
- Pandemic related medical information, including underlying health conditions, received via the dedicated FMBs will be retained as part of the continuous inventory and case evaluation for follow-up as well as policy advice of the EEAS Medical Service, in addition to information on personnel and location 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) for the purpose of 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 about exceptions to rules and reimbursement of costs will be kept according to archiving rules of Human Resources data, taking into account the expiry of legal claims arising from these measures.
- Data collected for and processed in the framework of the COVID-19 vaccination survey and the access to the COVID vaccination certificates except for the medical files will be erased after the right of claims related to the vaccination campaign expires.
- Data collected related to vaccination are kept in the medical files. Appointment data by DOCLR system is retained for 5 days after the publication day of the Belgian Royal Decree declaring the end of the COVID-19 pandemic, as stated by DOCLR.be
- Copies of ID documents will be erased shortly after the NISS/BIS number has been created, if possible not later than in 6 months.
- In relation to the EU Digital COVID Certificate issued in Belgium, the EEAS and the European Commission (HR.D.1) retain your personal data for the time necessary to fulfil the purpose of the specific processing, namely until 8 years after the extinction of all the rights. All the retention periods are in agreement of section 12.3.7 of SEC (2019)900 "Common Commission-Level Retention List for European Commission Files", in general applied by the EEAS.

Data collected by the Corona and Covid-19 Task Forces, including the Vaccine Strategy Task Force will be kept according to the above retention periods depending on their nature. 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 pandemic. Access to the COVID-19 functional mailboxes 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. HR data are kept according to relevant confidentiality rules. Additional two line managers have access to the de-personalised information on the office location. Data collected for and processed in the framework of the COVID-19 vaccination survey and data collected and processed by the Vaccine Strategy Task Force, is kept only on password-protected local workstations, saved in password-protected files and transferred solely through secured means. Data stored by the KITRY system is secured by specific security measures. Safety, confidentiality, integrity and availability of the data is guaranteed by AFAQ Healthcare Data hosting certified provider.

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.