

# EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

## PROCESSING PERSONAL DATA RELATED TO SECURITY INVESTIGATIONS 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. You have the right under EU law to be informed when your personal data is processed [e.g. 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.

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

#### Purpose of the processing

Processing of your personal data in the context of Security Investigations is necessary for investigative purposes. It ensures the regular functioning of the EEAS and the protection of EU interest, such as staff, visitors, premises, assets and information. The purpose of the data processing in the framework of EEAS security investigations, therefore, is to collect data and adequate elements that can contribute to the manifestation of the truth, to the assessment and to the possible identification of the alleged perpetrator of the offense in case of security incidents, breaches, compromises of classified information, crimes and/or other prejudicial events. Data processed includes the minutes of the hearing with the complainants, witnesses, alleged perpetrators, and the collection of evidence.

The ultimate goal of the Security Investigations is to draft a report with facts and elements gathered during an investigation.

#### Procedure of the reporting

The report is first transmitted to the Head of Division of Security Policy and HQ Security who decides if further actions are needed. If so, the report is transmitted to the Director of Security and Real Estate (RM.SECRE) and the Director General for Resource Management (RM), being the EEAS Security Authority, who will decide on further actions, if required.

#### Description of the processing

The assessment of security threats, incidents, breaches or compromises of classified information, crimes and/ or other prejudicial events of facts brought to the attention of the Security Division involved for each case:

1. The compilation of paper and/or digital files gathering the components and aspects of the complaint, statement or testimony of the alleged victim, perpetrator and of witness or of any individual involved in the case as well as conclusive elements, deductions.
2. The creation of a database of cases (open and closed), including useful information from each folder allowing both to find each file easily and to extract certain data, aiming at addressing preventive actions and at drawing anonymised statistics. The database also allows for cross-referencing between the various cases it includes.
3. The creation, maintenance, update and transmission of a list of individuals whose access is prohibited in the concerned EEAS buildings, based on a decision of the Security Directorate as an outcome of a previous investigation or a security verification by the Belgian authorities.
4. In the preliminary investigation, consultation of access entitlements and actual access and outgoing traffic – including images and recordings – security clearances, copies and storage of images recorded by cameras equipping buildings, including queries addressed to DIGIT and platforms belonging to the EEAS. Moreover, when there is no access granted to the content of files or emails, access is only provided to user lists, to metadata of databases or to handling patterns. Administrative Decision (2016)22 is the legal basis and an *ad hoc* mandate conferred by the EEAS Security Authority is not necessary.
5. Consultation of all EEAS communication and information systems (CIS) and equipment, including but not limited to ICT equipment, telephone and telecommunications traffic data, log files and user accounts, used in the EEAS requires an *ad hoc* mandate, signed by the EEAS Security Authority and informing the DPO.
6. Reporting on the findings of cases handled

### 3. DATA PROCESSED: What data do we process?

Data (category or type of data), including personal data, processed are the following:

1. Identification data and/or contact details available in EEAS databases.  
Personal data including surnames, names, place and date of birth, photo, address, telephone and mobile numbers of the relevant individuals, family composition, education, exclusively relevant for the investigation.
2. Circumstantial data  
The nature of the case, content of messages and documents, its circumstances (who, when, where, what happened, how and why), the evidence collected.
3. Sanction measures  
Sanctions or other administrative measures decided upon by the EEAS, in particular those forbidding access to EEAS premises.

### 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 (EEAS). The EEAS Division entrusted with managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

**Division "HQ Security and EEAS Security Policy" (EEAS.RM.SECRE.2)**

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

The recipients of your data may be:

- Authorised individuals within the EEAS and other EU Institutions and EU Member States appointed by the Director General for Resource Management who is also the EEAS Security Authority, in particular those participating in or supervising the investigations.
- OLAF/IDOC/HR.DS
- Judicial authorities or police (Investigatory Judge)
- Contracted firms concerned
- Data mentioned above might be transferred to third countries and international organisations in the context of an official investigation and by written request of the third countries and international organisations to the Security Authority

Access to these recipients is provided only as needed for their specific tasks.

The given information will not be communicated to third parties, except where necessary for the purposes outlined above. Data transferred to third countries or international organisations as indicated above will be limited on the basis of the need-to-know principle and transfer is implemented pursuant to Article 46-51 of the Regulation (EU) 2018/1725.

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

You have the right of access to your personal data and the right to correct your inaccurate, or incomplete personal data taking into account the purpose of the processing.

The right of rectification can only apply to factual data processed. You have the possibility to have data that you have communicated corrected, whether the communication takes place, later or during additional statements which will be noted to the file. This ensures the update based on further developments. This possibility is always communicated in an interview.

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 without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. 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 (EU) 2018/1725 may apply. Certain data can be subject to the aforementioned restrictions as well as may be covered by the exceptions referred to in Articles of 19-24 of the Reg. (EU) 2018/1725. When, in particular, access to these data may compromise the investigation or the rights and freedoms of others, access to these data may be refused, limited or delayed in time. You can appeal to the European Data Protection Supervisor to have the legal aspects of the data processing controlled as well as to verify the data relating to you and, if necessary, give instruction to correct or remove them for a legitimate reason.

If you wish 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:

**[eeas-security-investigations@eeas.europa.eu](mailto:eeas-security-investigations@eeas.europa.eu)**

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

### Lawfulness

The processing of your personal data is necessary for the performance of a task carried out by the EEAS in the public interest, in particular for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof.

In order to comply with the legal obligation imposed on the EEAS, the processing of your personal data is necessary to provide access to an investigation following an official request from the competent Prosecutor's office [Article 5(1)(b) of Regulation (EU) 2018/1725]

Restrictions may apply as indicated under point 6: Article 25(1)(b),(c) and (d) of Regulation 2018/1725 provides that the Union institutions and bodies may restrict the application of Articles 14 to 22, 35, and 36, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, when such restriction constitutes a necessary measure to safeguard:

(b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(c) other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(d) the internal security of Union institutions and bodies, including of their electronic communications networks in the cases referred to in points (b) to (d). You can find further information on restrictions in the [Internal Rules of the EEAS](#).

### Legal references

- Administrative Decision on the scope and procedures of investigations to be carried by the HQ Security and EEAS Security Policy Division [ADMIN (2016)22]
- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service, and in particular art. 1, 7, 9 and 10 (OJ C 2018 126/01)
- Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service, art. 10, (2010/427/EU)
- Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)
- European Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission
- European Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
- Decision of the Director-General for Budget and Administration of the European External Action Service of 10/05/2021 on the acceptable use of Unclassified Communication and Information System services of the EEAS (ADMIN(2021) 5)
- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 1 October 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the European External Action Service [2019/C 370/06](#)

### Further references

2017/46, Commission Decision on the security of communication and information systems in the EC, Article 15 due to 2010/427/EU, Article 10

2017/1584 Commission recommendation on coordinated response to large-scale cybersecurity incidents and crises  
2016/1148 Directive (EU) concerning measures for a high common level of security of network and information systems across the Union.

## 8. TIME LIMIT FOR DATA STORED & SECURITY MEASURES: For what period and how we process your data?

### Data storage

The data referred to under point 3.1 and 3.2 may be retained by the EEAS for a period of thirty years from the closure of the file. The storage period is set at thirty years for the following reasons:

- (1) This retention period takes into consideration the legal provisions related to penal files. Agents handling the files can be requested to testify to the competent bodies. The conservation period for serious crimes in Belgium is twenty years and the Security Investigation Sector should be able to answer inquiries from the Belgian Authorities or other authorities concerning acts committed several years before.
- (2) Certain intelligence, espionage or terrorism files can be spread over very long periods (sometimes several decades).
- (3) The average career of a civil servant is spread over at least thirty years and the different stages of this career as well as the incidents that occurred during the career are essential elements to describe the profile of a person involved in complex investigations.

The data referred to under point 3.3 will be retained as long as it is strictly necessary for the application of the withdrawal of access, but not longer than five years after the measure has been applied.

Security of data:

Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU)2018/1725. The collected personal data are stored on servers that abide by pertinent security rules. Data is processed by assigned staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/Password. Physical copies of personal data are stored in a properly secured manner. Where needed, communications are encrypted. Encrypted email is used for transmission of documents containing Personal Data related to Security Investigations. Computer systems are protected by physical protection measures.

**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](mailto: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](mailto:edps@edps.europa.eu).