EUROPEAN COMMISSION

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Personal data processing in the framework of HR.DS.2 Counter-Intelligence / Counter-Terrorism / Extremism /Threats Affecting the European Commission

Data Controller: HR.DS.2 Investigations & Analysis

Record reference: DPR-EC-00677

Table of Contents

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 "Counter-Intelligence / Counter-Terrorism-Extremism Threats Affecting the European Commission", undertaken by the Security Directorate's Operations Unit (HR.DS.2) is presented below.

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

Purpose of the processing operation: The Security Directorate's Operations Unit (HR.DS.2) collects and uses your personal information in order to:

- Identify, monitor, assess, investigate and thwart threats faced by the institution (its personnel, its premises and/or its information) with regard to hostile intelligence operations, terrorism/extremism, unauthorised disclosure of sensitive or classified Commission information or other threats against the institution's staff, information and assets.

- identify and counter threats emanating from disinformation measures or "fixated individuals" with a fixation on Commission's College members and staff. Fixated individuals are persons obsessed with other persons to the effect that they regularly stalk them physically or by other means (electronic or other communication methods).

- Conduct security verifications and screenings regarding the background of individuals working in (for example, through a traineeship, a secondment or an employment contract) or providing a service to (for example, through an external service provider) the institution, having access to Commission infrastructures (buildings, IT networks, communications, etc.), staff and/or information.

- Conduct verifications, screenings and/or investigations in other cases of existing or suspected activities against the security and integrity of Commission infrastructures, staff, information and assets, or against its reputation.

In this context the following processing steps are taken:

- When receiving information from partner law enforcement, security or intelligence services, from Commission services or colleagues, or from other EU institutions;

- When verifying information with Commission data repositories and IT applications;

- When performing OSINT (Open Source Intelligence) searches on the internet, social media and other publicly available information;

- When conducting security verifications and screenings regarding the background of individuals working in (for example, through a traineeship, a secondment or an employment contract) or providing a service to (for example, through an external service provider) the Commission;

- When performing investigative actions within a mandated inquiry, for example during interviews with staff.

Certain processes include an initial automated collection phase, which is later followed by an individual threat assessment by a mandated staff member.

Processing is done on a secure internal network, where data is adequately stored and protected in a case management system that providing access only to mandated staff.

Your personal data will *not* be used for an automated decision-making including profiling.

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

We process your personal data, because:

(a) 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;

(b) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

The basis for the processing referred to in points (a) and (b) above has been laid down in Article 22 (2) of Commission Decision (EU/Euratom) 2015/443.

We may process any of the following special categories of personal data:

(a) Data revealing racial or ethnic origin
(b) Data revealing political opinions
(c) Data revealing religious or philosophical beliefs
(d) Data concerning health
(e) Data concerning a natural person's sex life or sexual orientation

This is done because the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; an indicative example would be that such special categories' personal data could be received by HR.DS.2 from an EU partner service, in the framework of a security inquiry.

Special categories of data may need to be processed if they are related to threat or identification of circumstances of the threat, such as specific extremist religious affiliations or extremist political views that form the background of the potential threat towards the Commission. Similarly, health data may have to be processed where they are related to potential victims of threats at the Commissions or where they are circumstantial to the person posing such a threat.

In some instances the processing relates to personal data which are manifestly made public by the data subject; an indicative example would be a threat assessment process evaluating the special categories' personal data, that the data subject of interest has wilfully shared on social media.

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

In order to carry out this processing operation, HR.DS.2 may collect the following categories of personal data:

- Identification and contact data, such as first and last name, date and place of birth, nationality, telephone number, e-mail and office and home addresses;
- Physical characteristics (tattoos, birth marks, etc.), national identity number, identity card or passport number and/or copy of official identity documents, photographs;
- Family data, such as marital status, family background;
- OSINT (=open source intelligence) identification data (profiles, accounts, etc.);
- Professional data such as employer, function to be performed in the institution, curricula vitae, evaluation reports;
- Behavioural data relating to potential involvement in espionage, sabotage, terrorist or other violent activities;
- Communication data such as metadata, traffic data and content of communication, such as e-mail or telephone calls to the Commission, Members of the Commission or other staff concerned;
- Statements and claims of data subjects;
- Vehicle number plates;
- Criminal records, police records, weapons' licenses and serial numbers of weapons, explosives' licenses.

5. How long do we keep your personal data?

HR.DS.2 only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for as long as the threat exists towards the institution. When the threat ceases to exist, however, the data is kept for 15 years as of then.

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 either 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. The physical access to these areas is done using a badge, so only a limited number of staff has access. The data are processed on password-protected computers/laptops used only by staff with the need to know. Electronic storage is done on a network not linked to the Commission network, accredited to process EU classified information. Access to this network is controlled through a combination of measures and procedures aimed at achieving a security in depth.

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. In addition, staff working at the Security Directorate need to have a valid Security Clearance, delivered by the National Security Authority of their EU Member State of origin.

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

Access of staff to your personal data is managed based on internal system procedures. These procedures define how mandated investigators are given access to specific personal data residing on the system, from the moment of their taking up of duties in the Unit until the end of their work in this unit.

In addition, your personal data may be disclosed to other Commission services (such as competent HR.DS services or the Appointing Authority), EU institutions, bodies or agencies or national law enforcement authorities, security or intelligence services and/or governmental security bodies of EU Member States, on condition that these entities have a legitimate interest to have access to that data.

Moreover, and upon the same condition of legitimate interest, HR.DS.2 may identify the need to transfer your personal data to the recipients in a third country or to an international organisation in accordance with Regulation (EU) 2018/1725. These recipients may be authorities of third countries, as well as international organisations such as Interpol, NATO or the United Nations. The controller will transfer your personal data based on one of the following criteria:

- adequacy decision of the Commission for a specific country / commercial sector (Article 47 of Regulation (EU) 2018/1725), as e.g. in the case of the United Kingdom.

- in the absence of such an adequacy decision, HR.DS.2 will ensure that appropriate safeguards are in place before sharing that personal data (Article 48 of Regulation (EU) 2018/1725);

- in absence of both an adequacy decision and appropriate safeguards, transfer of your personal data is only possible following a derogation, under the conditions mentioned in Article 50 of Regulation (EU) 2018/1725, namely where the transfer is necessary for important reasons of public interest (Article 50 (g) of Regulation (EU) 2018/1725 such as the security of persons, assets and information in the Commission.

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) on grounds relating to your particular situation.

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.

Please note that the abovementioned rights may be restricted to safeguard the internal security of Union institutions and bodies, including their electronic communication networks and the protection of the data subject or the rights and freedoms of others pursuant to Commission

Decision 2019/236[1] in accordance with Article 25 (1) (d) and (h) of Regulation (EU) 2018/1725. 5.

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-MAIL-DS2@ec.europa.eu .

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

You may contact the Data Protection Officer (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) 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-00677.

[1] Commission Decision (EU) 2019/236 of 7 February 2019 laying down internal rules concerning the provision of information to data subjects and the restriction of certain of their rights in the context of the processing of personal data by the European Commission for the purposes of internal security of the Union institutions, OJ L 37, 8.2.2019, p.144.