

EDPS record of processing activity

Record of EDPS activities processing personal data, based on Article 31 of 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Description
		Security authorisation procedures
1.	Last update of this record	15.03.2022
2.	Reference number	59
3.	Name and contact details of controller	<p>European Data Protection Supervisor (EDPS) Postal address: Rue Wiertz 60, B-1047 Brussels Office address: Rue Montoyer 30, B-1000 Brussels Telephone: +32 2 283 19 00 Email: edps@edps.europa.eu</p> <p>Responsible department or role: EDPS Local Security Officer (LSO): edps-lso@edps.europa.eu Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/node/759</p> <p>The National Security Authorities (NSA) of the Member State of provenience of the staff member undergoing a vetting procedure act as separate controller for the processing of personal data provided for by national legislation in the context of the security authorization procedure. Contact details depending on the relevant NSA: please see Annex 1 below (as also provided in the data protection notice) for a list thereof.</p>



Nr.	Item	Description
4.	Name and contact details of DPO	DPO@edps.europa.eu
5.	Name and contact details of joint controller (where applicable)	Not applicable.
6.	Name and contact details of processor (where applicable)	EC SECURITY CLEARANCE Directorate-General Human Resources and Security Security Directorate Information Security Unit DS.3 +32 2 29 91551 EC-SECURITY-CLEARANCE@ec.europa.eu
7.	Short description and purpose of the processing	<p>Overall purpose of the data processing is to determine whether a person is eligible for an authorisation to access classified information and to facilitate the vetting procedure for staff members who are required to have a security clearance. The primary responsibility for the data processing lies within the HRBA Unit. In particular, the EDPS LSO is competent for supervising security authorisations, through the help of the EC Security Clearance sector of the Security Directorate in DG HR and Security of the European Commission that liaise with the NSAs of Member States. The security authorisations are signed by the Supervisor or by the Director upon delegation.</p> <p>The EC Security Clearance office collects and retains personal information about staff members in a specific security clearance form issued by the staff members' home country NSA. The staff members fill in the relevant forms, which are consequently forwarded to the competent NSA through the EC. The results of the vetting procedures are communicated by the Member States NSAs to HR DS directly. No copies of the filled-in forms are retained by the EDPS; indeed, the LSO maintains only a record a list of of the communications received by the EC concerning the duration of the clearances released by the NSAs and the original of the Security Authorisations released by the director within the unit. In case of positive opinion from the relevant NSA, the Supervisor or the Director, after receiving the information from the Clearance sector, may grant the security authorisation. In the case a negative opinion is issued, the person concerned may be heard by the Supervisor and the Clearance Sector. If the Supervisor considers it necessary, he</p>



Nr.	Item	Description
		<p>may ask the competent NSA for further clarifications. However, if the negative opinion is confirmed, the Supervisor cannot grant an authorisation. All the aforementioned documents are kept in a file (hard copies) but also in the EC electronic database. Each national security questionnaire is different and depends on the laws and regulations of the Member State in question. The Commission only checks whether the information provided is complete, before transmitting it to the competent NSA responsible for carrying out the security investigation.</p> <p>Within the EDPS, the HRBA Unit is informed and kept updated by the LSO on the security roles of the personnel (so-called ‘sensitive posts’) on the basis of an assessment conducted by each Head of unit/sector. The HRBA unit is also informed in the case of a negative outcome of the vetting procedure, as failure to achieve security clearance by a staff member may result in the necessity of switching the ‘sensitive post’, which is indeed linked to the handling of classified information.</p>
8.	Description of categories of persons whose data the EDPS processes and list of data categories	<p>All staff members of the EDPS and SNEs for which it has been decided to have a Security authorisation to handle classified information. Data subjects involved in the processing are staff members of the EDPS and possibly members of their close family.</p> <p>The categories of personal data collected vary slightly from Member State to Member State based on different laws and regulations, but usually include the following:</p> <ul style="list-style-type: none"> - name, name history, date and place of birth, nationality, national identification or social security numbers - previous and present marital status - education - previous and present employment - criminal record details - security-related activities (including details of prior security clearance, and details of any activities which could negatively affect security clearance)



Nr.	Item	Description
		<ul style="list-style-type: none"> - financial situation, interests and history - past and present address and travel - health data - conduct which could provide grounds for pressure or improper influence - present or past use of, and attitude towards addictive substances (such as drugs and alcohol). <p>The information is provided by the data subjects by filling up <i>ad hoc</i> forms.</p> <p>A completed security clearance form may also contain information on the staff member's close family members (parents, in-laws, present and former spouses or partners and children). The categories of people covered also vary depending on which Member State is issuing the form for security clearance. The information provided in this regard contains the following:</p> <ul style="list-style-type: none"> - name, name history, date and place of birth, nationality, occupation - financial situation, interests and history - details of any activities which could negatively affect security clearance - financial situation, interests and history - past and present address and travel. <p>These data are processed by the NSA of the Member State of provenience of the staff member. Some of them might be processed by EC Security Clearance Team within EC DG HR and security. The fact of family members having to provide data for the completeness of the vetting procedure depends entirely on Member State's legislation.</p> <p>A copy of the paper file kept in the HS.DS unit, Clearance Sector, as well as a computerized nominative archiving which includes: NAME, SURNAME, DATE OF BIRTH, NATIONALITY and the applicant's institution (as personal data). Other (non-personal) data archived automatically are:</p>



Nr.	Item	Description
		<p>Date of receipt of the request formulated by the LSO of the DG concerned.</p> <p>Date of dispatch of the form (different depending on the nationality of the applicant) to the interested party for information.</p> <p>Date of receipt of the form filled out by the person concerned</p> <p>Date of sending the form to the NSA as well as the date of receipt of the security clearance from the NSA.</p> <p>Date of the mandatory security briefing prior to the security clearance granted by the Director of the DS.</p>
9.	Time limit for keeping the data	<p>As a general principle, personal data will be kept as long as the staff member is covered by a valid security authorisation and are thus destroyed, as applicable, either (i) six months after the date the security clearance is no longer deemed necessary; (ii) six months after the expiration of the validity date indicated by the NSA; or (iii) six months after the staff member has left the institution. The electronic file is blocked (in fact inactivated so that the LSO no longer has access to this file) when the HR.DS has been notified that the person no longer needs a security clearance. The EDPS LSO will maintain only a list of the clearance released and the original of the Security Authorisations in his record in accordance to the above indicated retention periods.</p>
10.	Recipients of the data	<ul style="list-style-type: none"> - Personnel of the EC Clearance (HR.DS) office of the European Commission. - Relevant staff of the NSA of the Member States.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No such transfers are envisaged.
12.	General description of security measures, where possible.	In order to safeguard personal data against any possible misuse or unauthorised access, electronic information are accessible with a restricted access on a strict need-to-know basis for the recipients only, the EDPS LSO and the security personnel of the EC Security Clearance



Nr.	Item	Description
		<p>team. (HR.DS). The computerized database contains only the nominative personal identification data, (Name, Surname, date of birth, nationality, DG concerned). Other personal data entered by the person requesting the Security Authorization remains in the paper file only and is not computer-processed. The personal file (paper file filled-in by the interested party) security clearance application is available to each official or other agent who wishes to make a request for access to his own file. It is archived in the secure area of the Security Directorate. The judicial authorities in the Member States carry out the investigations in a completely leakproof manner in relation to the Commission. For paper copies of the lists they should be protected by keeping them locked away when not in use and stored in a locker, thrower or cupboard.</p>
13.	<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</p>	<p>Data protection notice is available internally on the EDPS Intranet. Also, to better inform family members of possible implication this data protection notice is published on the EDPS Website and is provided to the family member of the staff member upon request.</p> <p>The EDPS LSO will regularly (at least once per year) update the list of cleared staff within the EDPS, depending on the possible departure of security cleared staff, and will take care of informing the EC Clearance Office of that, which in turn will update the electronic database.</p>

