

**NOTIFICATION TO THE DATA PROTECTION OFFICER
(ARTICLE 31 REGULATION 2018/1725)**

NAME OF PROCESSING ACTIVITY¹: **Obtention Personal Security Clearance (PSC) for EMSA staff**

1) Controller(s) ² of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit responsible³ for the processing activity: Department 4</p> <p>Contact person: Dominika Lempicka-Fichter, - Head of Department 4</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Magerlein: dpo@emsa.europa.eu</p>
2) Who is actually conducting the processing? (Article 31.1(a)) ⁴
<p>The data is processed by EMSA itself <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is: 4.1</p> <hr/> <p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party: European Commission DG HR Security <input checked="" type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer): data-protection-officer@ec.europa.eu</p>

¹ **Personal** data is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.

Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

² In case of more than one controller (e.g. joint operations), all controllers need to be listed here

³ This is the unit that decides that the processing takes place and why.

⁴ Is EMSA itself conducting the processing? Or has a provider been contracted?

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing.

Personnel Security Clearance (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date.

EMSA currently handles EU classified information (EUCI) at the level RESTREINT UE/EU RESTRICTED in the team of Maritime Security.

Security clearances are not required at the level RESTREINT UE/EU RESTRICTED, however some Member States impose higher levels of protection even for documents at RESTREINT UE/EU RESTRICTED level, therefore EMSA staff who carries out maritime security inspections need to present their clearances in order to perform their duties.

The Executive Director of EMSA shall identify the positions within the Agency for which the holders need to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above to perform their duties and therefore need to be security authorised.

Steps of the procedure:

1. Staff member/HoU ask Security officer (with assistance of the Unit 4.1) to launch the request of PSC
2. Unit 4.1 sends to staff member a form to complete
3. Unit 4.1 sends to EC this form via ARES to request a PSC
4. EC sends Unit 4.1 the PSC
5. Unit 4.1 sends to ED authorisation to sign/validate
6. Unit 4.1 sends a notification to the staff member of the PSC authorisation with a validity date
7. PSC is filed in e-personal file of the staff member concerned

4) Lawfulness of the processing (Article 5(a)–(d)): Processing necessary for:

Mention the legal basis which justifies the processing

- (a) a task carried out in the public interest or in the exercise of official authority vested in EMSA (including management and functioning of the institution) ☒

[EMSA Security Rules for protecting EU classified information \(EUCI\) Security Rules Version: 2.3 Date: 01/05/2020 Ref. Ares\(2020\)2484715 - 11/05/2020](#)

[Decision No. 2020/024 of The Executive Director Relating to the Implementation of EMSA Security Rules for Protecting EU Classified Information \(EUCI\) – Security Clearances \(Ref. Ares\(2020\)2483988 - 11/05/2020\)](#)

- (b) compliance with a legal obligation to which EMSA is subject ☐

- (c) necessary for the performance of a contract with the data subject or for the preparation of such a contract ☐

(d) Data subject has given consent (<i>ex ante</i> , explicit, informed)	<input type="checkbox"/>
5) Description of the categories of data subjects (Article 31.1(c)) <i>Whose personal data are being processed?</i>	
EMSA staff	<input checked="" type="checkbox"/>
Non-EMSA staff (contractors staff, external experts, trainees)	<input type="checkbox"/>
Visitors to EMSA building	<input type="checkbox"/>
Relatives of the data subject	<input type="checkbox"/>
Other (please specify):	
6) Categories of personal data processed (Article 31.1(c)) <i>Please tick all that apply and give details where appropriate</i>	
(a) General personal data: The personal data contains:	
Personal details (Name, Birthdate, Nationality and personnel number and grade)	<input checked="" type="checkbox"/>
Education & Training details	<input type="checkbox"/>
Employment details (Description of the staff member tasks)	<input checked="" type="checkbox"/>
Financial details	<input type="checkbox"/>
Family, lifestyle and social circumstances	<input type="checkbox"/>
Goods or services provided	<input type="checkbox"/>
Other (please give details):	

(b) **Sensitive personal data** (Article 10)

The personal data reveals:

- | | |
|--|--------------------------|
| Racial or ethnic origin | <input type="checkbox"/> |
| Political opinions | <input type="checkbox"/> |
| Religious or philosophical beliefs | <input type="checkbox"/> |
| Trade union membership | <input type="checkbox"/> |
| Genetic, biometric or data concerning health | <input type="checkbox"/> |
| Information regarding an individual's sex life or sexual orientation | <input type="checkbox"/> |

7) Recipient(s) of the data (Article 31.1 (d))

Recipients are all parties who have access to the personal data

- | | |
|--|-------------------------------------|
| Data subjects themselves | <input checked="" type="checkbox"/> |
| Managers of data subjects | <input checked="" type="checkbox"/> |
| Designated EMSA staff members | <input checked="" type="checkbox"/> |
| Administrative Assistant Unit 4.1, SO, ED and Head of Executive office | |
| Designated Contractors' staff members | <input type="checkbox"/> |
| Other (please specify): | |
| Commission staff dealing with the procedure in DG HR Security | |

8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))

If the personal data are transferred outside the European Economic Area, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Data are transferred to third country recipients:

Yes ☐

No ☒

If yes, specify to which country:

If yes, specify under which safeguards:

Adequacy Decision of the European Commission ☐

Standard Contractual Clauses ☐

Binding Corporate Rules ☐

Memorandum of Understanding between public authorities ☐

9) Technical and organisational security measures (Article 31.1(g))

Please specify where the data are stored during and after the processing

How is the data stored?

EMSA network shared drive ☒

Outlook Folder(s) ☒

Hardcopy file ☐

Cloud (give details, e.g. public cloud)

☐

Servers of external provider

☐

Other (please specify): *ARES, E-personal file and SO Database*

10) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Keep in mind that there are pre-determined retention periods for most types of files. Those are explained in the Records Management Policy and Procedure of the Agency. You can check EMSA Records Management Policy and Procedure at the Intranet of the Agency.

Personal Security Clearance are kept in the personal file of the staff member and have to be kept as long as the personal file is retained.

Personal files are destroyed 10 years following the termination of employment or the last pension payment.