

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

NAME OF PROCESSING ACTIVITY: **Alteration and upgrade of EMSA CCTV system**

Please provide here a meaningful name of the processing operation involving personal data (e.g. staff recruitment, business continuity contact list)

1) Controller(s) ¹ of data processing operation (Article 31.1(a))
Controller: European Maritime Safety Agency (EMSA) Organisational unit responsible ² for the processing activity: Unit 4.2 Contact person: Dominika Lempicka-Fichter Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu
2) Who is actually conducting the processing? (Article 31.1(a)) ³
The data is processed by EMSA itself <input checked="" type="checkbox"/> The organisational unit conducting the processing activity is: Unit 4.2 <hr/> The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party [indicate third party] <input type="checkbox"/> Contact point at external third party (e.g. Privacy/Data Protection Officer):

3) Purpose of the processing (Article 31.1(b)) <i>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.</i>
The purpose(s) of the processing of personal data is/are: The Agency uses its video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to the Agency building and helps ensure the security of the building, the safety of the staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support Agency's broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps

¹ In case of more than one controller (e.g. joint operations), all controllers need to be listed here

² This is the unit that decides that the processing takes place and why.

³ Is EMSA itself conducting the processing? Or has a provider been contracted?

prevent, detect and investigate theft of equipment or assets owned by the Agency, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault)	
4) Lawfulness of the processing (Article 5(a)–(d)): Processing necessary for: <i>Mention the legal basis which justifies the processing</i>	
(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)	X
EMSA Founding Regulation)	
(b) compliance with a legal obligation to which EMSA is subject	<input type="checkbox"/>
(c) necessary for the performance of a contract with the data subject or for the preparation of such a contract	<input type="checkbox"/>
(d) Data subject has given consent (<i>ex ante</i> , explicit, informed)	<input type="checkbox"/>
Describe how consent will be collected and where the relevant proof of consent will be stored	
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 checked="" type="checkbox"/>
Visitors to EMSA building	<input checked="" type="checkbox"/>
Relatives of the data subject	<input checked="" 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, address etc)	<input type="checkbox"/>
Education & Training details	<input type="checkbox"/>
Employment details	<input 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): image of the persons	
(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))	
<i>Recipients are all parties who have access to the personal data</i>	
Data subjects themselves	<input type="checkbox"/>
Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	<input checked="" type="checkbox"/>
Designated Contractors' staff members	<input checked="" type="checkbox"/>
Other (please specify):	
8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))	
<i>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.</i>	
Data are transferred to third country recipients:	
Yes	<input type="checkbox"/>
No	<input checked="" type="checkbox"/>
If yes, specify to which country:	

If yes, specify under which safeguards:

- | | |
|--|--------------------------|
| Adequacy Decision of the European Commission | <input type="checkbox"/> |
| Standard Contractual Clauses | <input type="checkbox"/> |
| Binding Corporate Rules | <input type="checkbox"/> |
| Memorandum of Understanding between public authorities | <input type="checkbox"/> |

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 | <input checked="" type="checkbox"/> |
| Outlook Folder(s) | <input type="checkbox"/> |
| Hardcopy file | <input type="checkbox"/> |
| Cloud (give details, e.g. public cloud) | <input type="checkbox"/> |
| Servers of external provider | <input type="checkbox"/> |

Other (please specify):

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.

In accordance with the EMSA CCTV Rules – 30 days

**Thank you for completing the form.
Now please send it to the DPO using the ARES workflow**