

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

NAME OF PROCESSING ACTIVITY¹:

Upgrades and alterations of existing CCTV system 25/03/2020

1) Controller(s) ² of data processing operation (Article 31.1(a))	
Controller: European Maritime Safety Agency (EMSA)	
Organisational unit responsible ³ 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)) ⁴	
The data is processed by EMSA itself	<input checked="" type="checkbox"/>
The organisational unit conducting the processing activity is: Unit 4.2	
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>

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?

The purpose of the video surveillance system is the reduction and prevention of security incidents. The system helps to ensure the buildings security, the safety of staff and visitors, as well as property and information located or stored on the premises, by means of controlling access to the Agency buildings in compliance with Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and the applicable Portuguese legislation as well as the European Data Protection Supervisor (EDPS) Guidelines.

In accordance with the security assessment of EMSA premises carried out in November 2017 by DG HR DS and EMSA Security Plan, the Agency commenced implementing the recommended security measures listed in the report. One of the measures envisaged some upgrades and alterations of existing CCTV system (i.e. installation of additional internal cameras to cover the strategic points of the EMSA building by the monitoring system according to "Data Protection Impact Assessment for the upgrade and alteration of the EMSA CCTV system" - emsa.a.2.0.dir(2018)5553682).

Installation of the new cameras as well as their maintenance may interrupt the proper work of existing CCTV system. As part of the technical operations during the installation and testing, it is required that during the installation works and during preliminary configuration of new cameras (February and March 2020), as well as consecutive maintenance or repairs all elements of the system may need to be switched on 24/7 temporarily. From a technical point of view, this allows to detect immediately any interruptions or malfunctioning of the whole CCTV system.

However, during such installation works it may happen that images of random people (mainly EMSA staff and visitors) may be 'caught' by the cameras i.e. live monitoring of the random people whose identity can be recognised. This possibility was already identified as a risk "Data Protection Impact Assessment for the upgrade and alteration of the EMSA CCTV system" - emsa.a.2.0.dir(2018)5553682) and the risk mitigating measures were employed. In order to emphasise a warning to EMSA staff and visitors who are the most likely data subjects affected, the responsible Section of the Data Processing Unit (4.2.3) regularly sends e-mail updates to All staff and POs responsible for hosting external events or visitors are advised to notify the invitees of this possibility.

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) | 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): images 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))

Recipients are all parties who have access to the personal data

- | | |
|---------------------------------------|-------------------------------------|
| 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))

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 | <input type="checkbox"/> |
|-----|--------------------------|

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):

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 and applicable Portuguese legislation – 30 days.

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