

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

NAME OF PROCESSING ACTIVITY: Questionnaire about information sharing on maritime cybersecurity incidents

1) Controller(s)¹ of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit responsible for the processing activity: 2.1</p> <p>Contact person: Luca Gargano, Chronis Kapalidis</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu</p>
2) Who is actually conducting the processing? (Article 31.1(a))²
<p>The data is processed by EMSA itself x</p> <p>The organisational unit conducting the processing activity is: Unit 2.1 Safety & Security</p>
<p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party NO <input type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</p>

3) Purpose of the processing (Article 31.1(b))
<p><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></p>
<p>The survey will be launched using the E-Survey Platform and is intended to, on the one hand, gather information from the EU and EFTA Member States about the current state-of-play regarding information sharing and incident reporting in their respective countries and, on the other hand, collect their views on the development of a mechanism at EU/EFTA level, potentially building on EMSA expertise on sharing maritime</p>

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

² Is EMSA itself conducting the processing? Or has a provider been contracted?

information. This will help EMSA understand the capabilities and the needs of the Member States in order to proceed accordingly in the future.

The Survey is fully anonymous and not linked to any email address, or entity.

Furthermore, it is not open to the public. It will be sent via email to the Maritime Security Regulatory Committee emails list, which EMSA regularly uses for communication with MS. The communication normally goes through a 'corporate' mailboxes, however, processing of some 'residual' personal data is possible.

The questionnaire won't be published on EMSA website but will be put on-line on EUSurvey, the European Commission's official online survey management tool, which already foresees thorough measures about the processing and the protection of personal data: [EUSurvey - Privacy Statement \(europa.eu\)](https://eusurvey.europa.eu/privacy-statement)

The collected anonymous data will be analysed by the relevant EMSA staff to prepare the working sessions of the cyber conference to be hold on 3 October 2024.

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) ☒
Article 2 'Core tasks of the Agency', par.1 e) EMSA founding regulation
- (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 ☐

Important Note

Consent may not be the most appropriate legal basis, in particular in the employment context. However, if you wish to use consent as legal basis, ensure that it complies with the following: it must be freely given, specific, informed and unambiguous consent. Contact the DPO if you need further clarifications.

- (d) Data subject has given consent (*ex ante*, explicit, informed) ☐
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 type="checkbox"/>
Non-EMSA staff (Member States staff)	<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, email address etc)	<input checked="" type="checkbox"/>
Education & Training details	<input type="checkbox"/>
Employment details	<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"/>
<div style="border: 1px solid black; padding: 10px; text-align: center;"> <p>Important Note</p> <p>If you have ticked any of the sensitive data boxes, please contact the DPO before processing the data further.</p> </div>	
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 checked="" type="checkbox"/>
Designated EMSA staff members	<input checked="" type="checkbox"/>
Designated Contractors' staff members	<input 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

☐

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

☐

Important Note

If no safeguards are applicable, please contact the DPO before processing the data further.

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.

The data will be stored in an Outlook folder and in a separated file, handled by the Security cell staff, in order to process the data for further analysis. The retention of the data will be decided by the HoU and Coordinator of the section 2.1 in accordance with the specific needs of the Unit and in compliance with the EMSA Records Management Policy and Procedures.

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