

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

NAME OF PROCESSING ACTIVITY¹: System Administration of the Ship Web User Interface of the Union Maritime Information and Exchange System (SafeSeaNet)

1) Controller(s) ² of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA), Head of Department 3 - Digital Services and Simplification, acting as delegated EMSA data controller Organisational unit responsible³ for the processing activity: Unit 3.1</p> <p>Contact person: Head of Unit 3.1, MaritimeSupportServices@emsa.europa.eu</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)) ⁴
<p>The data is processed by EMSA itself <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is: Unit 3.1</p>
<p>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"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</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.

The Union Maritime Information and Exchange System (SafeSeaNet - SSN) is an electronic platform designed to facilitate the exchange of vessel and voyage-related information among designated participants within the European Union. The primary objective of SSN is to support EU and Member State activities by enabling the receipt, storage, retrieval, and exchange of critical maritime data to ensure maritime safety, port and maritime security, marine environmental protection, and the overall efficiency of maritime traffic and transport operations.

The SafeSeaNet web user interface for ships is specifically used for the submission and consultation of Ship Reporting System (SRS) reports, including responses from Coastal Station (CST) authorities. Access to the system and its features is based on predefined roles and access rights, which are assigned by SSN administrators at the national or EU levels, and by the central SSN administrator.

The system provides functionalities to manage user accounts lifecycle (creation, modification and retirement of accounts).

Accounts lifecycle management is handled by the following types of administrators:

- Application Administrators (EMSA): can manage accounts for all Member States and Institutions
- National Administrators (Member States): can manage accounts only within his own Member State/Institution

For user accounts, the following data is stored:

- accountID (AKA userID)
- Name (First, Last)
- E-mail address
- Member State
- Organisation
- Application Profiles and Roles
- Vessel details (IMO, MMSI, Ship Name, Call sign)

The Unit 3.1 is responsible for the general system administration and maintenance of the Union Maritime Information and Exchange System (SafeSeaNet - SSN).

Activities are limited to:

- Maintenance and Operation of the technical components of the system (servers, database, application and surrounding technical components)
- Data storage
- Access to the data is only in the scope of the operational tasks

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)



(Examples of legal basis: e.g. Article 2 'Core tasks of the Agency', par.4 b 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))

Whose personal data are being processed?

- EMSA staff ☒
- Non-EMSA staff (External users - MS authorities and ship representatives) ☒
- Visitors to EMSA building ☐
- Relatives of the data subject ☐
- Other (please specify):

6) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) **General personal data:**

The personal data contains:

- Personal details (name, address etc) ☒
- accountID (AKA userID)
 - Name (First, Last)
- Education & Training details ☐
- Employment details ☒
- E-mail address,
 - Member State
 - Organisation

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))	
<i>Recipients are all parties who have access to the personal data</i>	
Data subjects themselves	<input checked="" type="checkbox"/>
Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	<input checked="" type="checkbox"/>
SSN Administrators	
Designated Contractors' staff members	<input type="checkbox"/>
Other (please specify):	
EU MS public authorities responsible for Ship Reporting Systems (SRS)	
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"/>

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):

EMSA internal servers located at EMSA's data centre in Lisbon and replicated at EMSA's BCF facility at Madrid.

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 user account is disabled by the administrators and personal data is marked as not available in the system interface.

The personal data is being retained by EMSA for no longer than is necessary for the purposes for which the personal data are processed.

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