

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

NAME OF PROCESSING ACTIVITY¹: System Administration of the Identity Management V2 (IdM-V2) by EMSA

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 3</p> <p>Contact person: António Anciães, Unit 3.1</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:</p> <ul style="list-style-type: none"> All EMSA Units that owns a Maritime Application running under Identity Management are processors within their respective record of processing activity system. The Unit 3.1 is responsible for the System administration of the Identity Management V2 (IdM-V2) system.
<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.

[IdM](#), which stands for “Identity Management”, is the platform developed and owned by EMSA where administrators may configure user accounts for all services of the EMSA Maritime Applications Portal, e.g. European Index Server (SafeSeaNet), EU LRIT CDC, THETIS, CleanSeaNet, Integrated Maritime Services (IMS).

The system provides functionalities to manage user accounts lifecycle (creation, modification and retirement of accounts), which are divided in two types:

- Human: the user account relates to a physical person (e.g. end-user),
- System: the user account relates to a system (e.g. National SSN System). For system user accounts, the personal information will indicate the contact point in charge of the management of the system. System user accounts do not have access to any Web User Interface. System accounts can only be seen and controlled by EMSA.

Accounts lifecycle management is handled by 3 types of administrators:

- Application Administrators (EMSA): can manage accounts inside a specific application and for all Member States and Institutions
- National Administrators (Member States): can manage accounts inside a specific application, only within his own Member State/Institution
- Organization Administrators: can manage accounts inside a specific application, for his own Member State/Institution and only inside his own organization.

For human users accounts, the following data is stored:

- accountID (AKA userID)
- Name (First, Middle, Last)
- E-mail address
- Address
- Contacts (Phone)
- Member State
- Organisation
- Service (usually matches a Maritime Application)
- Application Profiles and Roles

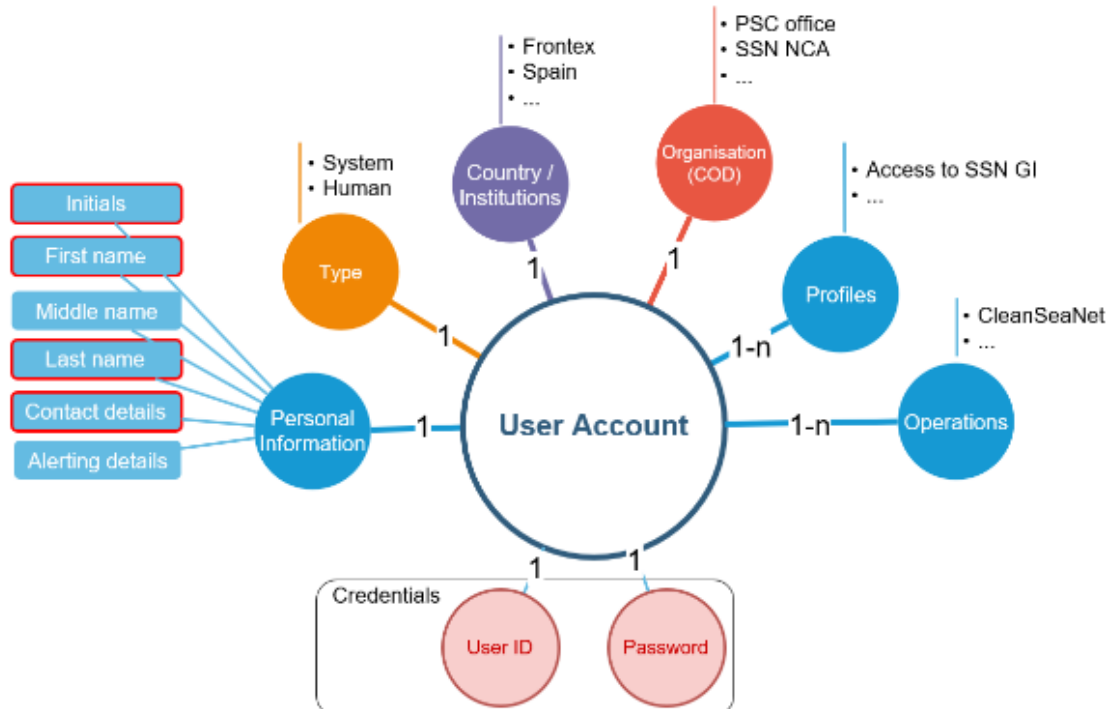


Figure 1: Attributes of a user account

The Unit 3.1 is responsible for the general system administration and maintenance of the IdM-V2 system. 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**

All EMSA Units that owns a Maritime Application running under Identity Management are processors within their respective record of processing activity system. For further information, please consult their respective privacy statement.

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 Service Catalogue: Maritime Digital Services.](#)

- (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 (*ex ante*, explicit, informed) ☐

5) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

- EMSA staff ☒
- Officials, Temporary Agents and Contract Agents
- Non-EMSA staff (contractors staff, external experts, trainees) ☒
- Contract Agents, Trainees, Interims, SNEs and NEPTS
 - External users of EMSA Maritime applications hosted in the EMSA Maritime Portal
- 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, Middle, Last)

-	
Education & Training details	<input type="checkbox"/>
Employment details	<input checked="" type="checkbox"/>
- E-mail address,	
- Address	
- Contacts (Phone)	
- 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))

Recipients are all parties who have access to the personal data

Data subjects themselves ☒

Managers of data subjects ☐

Designated EMSA staff members ☒

Identity Management V2 (IdM-V2) Administrators

Designated Contractors' staff members ☐

Other (please specify):

Also, if appropriate, access will be given to EU staff with the statutory right to access the data required by their function, i.e. the European Ombudsman, the Civil Service Tribunal, the Internal Audit Service, the European Court of Auditors, OLAF and the European Data Protection Supervisor.

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	<input type="checkbox"/>
Memorandum of Understanding between public authorities	<input type="checkbox"/>
9) Technical and organisational security measures (Article 31.1(g)) <i>Please specify where the data are stored during and after the processing</i>	
<p>How is the data stored?</p> <p>EMSA network shared drive <input type="checkbox"/></p> <p>Outlook Folder(s) <input type="checkbox"/></p> <p>Hardcopy file <input type="checkbox"/></p> <p>Cloud (give details, e.g. public cloud) <input type="checkbox"/></p> <p>Servers of external provider <input type="checkbox"/></p> <p>Other (please specify): EMSA internal servers located at EMSA's data centre in Lisbon and replicated at EMSA's BCF facility at Madrid.</p>	
10) Retention time (Article 4(e)) <i>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.</i>	
<p>The user account is disabled by the administrators and personal data is marked as not available in the system interface.</p> <p>The personal data is being retained by EMSA depending on the official retention of the maritime application.</p>	

--

