

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

NAME OF PROCESSING ACTIVITY<sup>1</sup>: **Management of EMSA Active Directory**

<b>1) Controller(s)<sup>2</sup> of data processing operation (Article 31.1(a))</b>
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit <b>responsible</b><sup>3</sup> for the processing activity: Unit 3.3 Horizontal Digital Services -</p> <p>Contact person: Joost VAN BELLEGHEM</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: <a href="mailto:dpo@emsa.europa.eu">dpo@emsa.europa.eu</a></p>
<b>2) Who is actually conducting the processing? (Article 31.1(a))<sup>4</sup></b>
<p>The data is processed by EMSA itself <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is Unit 3.3 Horizontal Digital Services</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>
<b>3) Purpose of the processing (Article 31.1(b))</b>

<sup>1</sup> **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.

<sup>2</sup> In case of more than one controller (e.g. joint operations), all controllers need to be listed here

<sup>3</sup> This is the unit that decides that the processing takes place and why.

<sup>4</sup> Is EMSA itself conducting the processing? Or has a provider been contracted?

<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 purpose of the processing activity is to manage users and their access rights in the context of IT systems with the Active Directory, which is the core identity database used by Microsoft Systems.</p> <p>Data from the Active Directory might be made available to other contracted services who employ directory-enabled applications.</p> <p>The System Administrators in the Unit 3.3 manage users in Active Directory. Administrators can add, edit, and deactivate users. They can also set user groups, roles, and access rights. This ensures that each user has the appropriate permissions based on their role within the organisation.</p>	
<p>4) Lawfulness of the processing (Article 5(a)–(d)): Processing necessary for: <i>Mention the legal basis which justifies the processing</i></p>	
<p>(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)</p> <p>Article 2 ‘Core tasks of the Agency’, par.4 b) EMSA founding regulation.</p>	<input checked="" type="checkbox"/>
<p>(b) compliance with a legal obligation to which EMSA is subject</p>	<input type="checkbox"/>
<p>(c) necessary for the performance of a contract with the data subject or for the preparation of such a contract</p>	<input type="checkbox"/>
<p>(d) Data subject has given consent (<i>ex ante</i>, explicit, informed)</p> <p>Describe how consent will be collected and where the relevant proof of consent will be stored</p>	<input type="checkbox"/>
<p>5) Description of the categories of data subjects (Article 31.1(c)) <i>Whose personal data are being processed?</i></p>	
<p>EMSA staff Officials, Temporary Agents and Contract Agents</p>	<input checked="" type="checkbox"/>
<p>Non-EMSA staff Seconded National Experts, Trainees, Interims, NEPTs, contractors staff</p>	<input checked="" type="checkbox"/>
<p>Visitors to EMSA building</p>	<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) <b>General personal data:</b>	
The personal data contains:	
Personal details	<input checked="" type="checkbox"/>
Name and Surname.	
Education & Training details	<input type="checkbox"/>
Employment details	<input checked="" type="checkbox"/>
Username, E-mail address, desk phone number, professional cell phone number, office address, office location, Job-title, Unit, Department, managers identity.	
Financial details	<input type="checkbox"/>
Family, lifestyle and social circumstances	<input type="checkbox"/>
Goods or services provided	<input type="checkbox"/>
Other (please give details):	
Profile picture, if voluntary uploaded by the user as it is not a mandatory field.	
(b) <b>Sensitive personal data</b> (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"/>
<b>7) Recipient(s) of the data (Article 31.1 (d))</b> <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"/>
System Administrators of the Active Directorate in the Unit 3.3 Horizontal Digital Services	
Designated Contractors' staff members	<input type="checkbox"/>
Other (please specify): All users having EMSA e-mail address.	
<b>8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))</b> <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 checked="" type="checkbox"/>

No

☐

**If yes, specify to which country:**

United States, for cloud-based applications (e.g. Microsoft 365 and Microsoft Azure), which are part of the MICROSOFT ILA (DI/07880), from which EPDS issued a decision with corrective measures on the use of M365. As per the letter attached REF. ARES (2024)8367282 – 25/11/2024, DIGIT is negotiating a new ILA with Microsoft in view of the EDPS Decision C2021-0518 of 08/03/2024 focusing on the topics of international transfers of personal data, clarity of processing purposes and the processed data types.

**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

☒

Servers of the Microsoft 365 cloud, servers of the Microsoft Azure cloud.

Other (please specify):

Secured servers in the EMSA datacentre

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.*

EMSA's retention policy for disabled Active Directory user is 90 days after user leaves the EMSA agency.