

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

NAME OF PROCESSING ACTIVITY¹:

Vessels positions and derived information data access (control based on the user identification from IdM - EMSA Identity Management application).

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: Unit 3.1 'Maritime Digital Services'</p> <p>Contact person: Marin Chintoan-Utah, Head of 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 type="checkbox"/></p> <p>The organisational unit conducting the processing activity is:</p> <hr style="border: 0; border-top: 1px solid black; margin: 10px 0;"/> <p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party: Together with third party - Microsoft <input checked="" type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</p> <p>Microsoft EU Data Protection Officer</p> <p>Dedicated mailbox to data subjects: https://www.microsoft.com/en-GB/concern/privacy</p> <p>Tel: +353 (0) 1 295-3826</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?

Attn: Data Protection

One Microsoft Place

Microsoft, South County Business Park, Leopardstown

Dublin 18, D18 P521, Ireland

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.

HP-IMS uses the user id from IdM (another EMSA application), which is a unique identifier in IdM that identifies a user that is created at that application. The IdM is the central application where all user data is stored and where users are managed at EMSA. To note that user id could identify a person.

The user id from IdM is used to identify what roles the user has (a user making a data request using HP-IMS webservises). These roles allow the HP-IMS application to control the data that the respective user can have access to.

Processing by EMSA

When a webservice call is made to HP-IMS the user id from IdM is included on the HTTP call. HP-IMS retrieves that user id and calls a webservice of IdM to get the roles for that user id. HP-IMS then stores the user id and the respective roles on its database in order to speed up subsequent data requests from the same user. The information in the HP-IMS database is refreshed from time to time by requesting again the roles to IdM for the user ids in HP-IMS database. If a user id does not exist anymore in the IdM that user id is also deleted from the HP-IMS database.

Processing by provider (Processor):

a) Providing Customer the Online Services:

Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;

Troubleshooting (preventing, detecting, and repairing problems); and

Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other

purpose, unless such use or processing is in accordance with Customer's documented instructions.

b) Processing for Microsoft's Legitimate Business Operations:

"Microsoft's legitimate business operations" consist of the following, each as incident to delivery of the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and modelling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure outlined below).

When processing for Microsoft's legitimate business operations, Microsoft will not use or otherwise process Customer Data (i.e. EMSA) or Personal Data for: (a) user profiling, or (b) advertising or similar commercial purposes or any other purposes incompatible with the purposes of the processing by EMSA. In addition, where Microsoft is processing this data for legitimate business operations, Microsoft will process it only for the purposes set out in this section.

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 (contractors staff, external experts, trainees) ☐

Visitors to EMSA building ☐

Relatives of the data subject ☐

Other (please specify): All users which are stored at EMSA Identity Management application.

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) ☐

Education & Training details ☐

Employment details ☐

Financial details ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):

Just the user id is processed as personal data. No other personal data is processed.

(b) Sensitive personal data (Article 10)

The personal data reveals:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☐

Information regarding an individual's sex life or sexual orientation ☐

Important Note

If you have ticked any of the sensitive data boxes, please contact the DPO before processing the data further.

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 | <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"/> |



Important Note

If no safeguards are applicable, please contact the DPO before

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)

☒

Data is stored in a database that is hosted in Microsoft Azure public cloud, and it is processed also in the same cloud provider. The data is secured using the security mechanisms of Azure, access control, key vaults, etc...

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 is only stored for the period that it exists in IdM application. Once it is deleted from IdM application it is also deleted from HP-IMS. Therefore, the retention time is controlled by IdM application.

Microsoft will delete or return all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled or earlier upon Customer's request, unless Microsoft is permitted or required by applicable law, or authorized under DPA, to retain such data.

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