

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

NAME OF PROCESSING ACTIVITY¹:

Operation of the EU Seafarers' Certification Platform for the purpose of issuing e-certificates to Seafarers - Phase I

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: 1.2 Visits & inspections, Human Element</p> <p>Contact person: Head of Unit 1.2 Visits & inspections, Human Element</p> <p>Data Protection Officer (DPO): 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: 1.2 Visits & inspections, Human Element</p>
<p>The data is processed by a third party (contractor): 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>Data subjects may contact the data protection officer by filling out the webform at https://aka.ms/privacyresponse. The DPO can also be reached by post at:</p> <p>Microsoft EU Data Protection Officer</p> <p>One Microsoft Place</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?

South County Business Park

Leopardstown

Dublin 18

D18 P521

Ireland

Telephone: +353 (1) 706-3117

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 EU Seafarers' Certification Platform (Platform, thereunder) aims at facilitating the issue of electronic certificates to seafarers from the EU Member States, Norway and Iceland. By doing so, the Platform supports the Member States in the implementation of Articles 4(11) and 4(13) of Directive (EU) 2022/993 on the minimum level of training of seafarers.

According to the Directive, each Member State shall undertake:

(a) to maintain a register or registers of all certificates of competency and certificates of proficiency and endorsements for masters and officers and, where applicable, ratings, which are issued, have expired or have been revalidated, suspended, cancelled or reported as lost or destroyed, as well as of dispensations issued;

(b) to make available information on the status of certificates of competency, endorsements and dispensations to other Member States or other Parties to the STCW Convention and companies which request verification of the authenticity and validity of certificates of competency and/or certificates issued to masters and officers in accordance with Regulations V/1-1 and V/1-2 of Annex I produced to them by seafarers seeking recognition, under Regulation I/10 of the STCW Convention, or employment on board ship.

Tasks that are facilitated by the Platform, not only through the hosting of the Member States' data in an independent manner per country, but also by allowing for the verification of the validity of the seafarer's certificates to be conducted through a common search functionality. The processing entails several Phases.

Phase I of the development of the Platform includes an eSign and eSeal functionality by which duly authorised officials of the Member States' Maritime Administrations are entitled to electronically sign and seal STCW certificates issued to seafarers in a secure, accredited, and transparent way.

To achieve it, the Platform will use one of the European Commission's digital building blocks: the eSignature block, which consists of a set of standards, tools and services that help create and verify electronic signatures that have the equivalent legal effect of hand-written signatures (QES).

For the provision of such services, Member States will have to transfer, and the Platform will need to receive and process the (personal) data contained within the STCW certificates issued to seafarers before the electronic signature and signing process can proceed using DIGIT's EU Sign services.

After such processing, both the personal data and the signed certificates will be stored in the Platform for the purposes of the verification of the authenticity and validity of the issued certificates by interested parties.

In addition, for verification of certificates not issued within the Platform, an interface connection is also established allowing for a search to be performed against the data stored in the Member States' systems.

The Platform will not reuse the personal data for another purpose that is different to the one stated above. The processing is not intended to be used for any automated decision making, including profiling.

Considering the above, the Platform development obeys to specific security measures and technical solutions identified to guarantee that the personal data are securely exchanged and processed.

Particularities of the processing:

Unless specifically authorised by each individual Member State for testing or problem-solving reasons, EMSA staff will not have access to the personal data stored within the Platform by each Maritime Administration.

Any processing carried out by an external party such as Microsoft when providing Azure Cloud services will obey to the contractual provisions that govern the supply of Cloud services to EMSA.

Processing by EMSA (systems):

Besides hosting data regarding the STCW certificates issued to seafarers in individual areas per EU Member State, the Platform will also display Maritime Administration users' details such as Name, Surname, Username and Role (in a non-editable manner) as a way for Member States to assign their users an Issuing Authority, a Branch or a special authorisation (the ability to eSign and eSeal certificates). These details of each Member State user will be retrieved from EMSA IdM, the central application where all user data is stored and where users are managed at EMSA.

Processing by the Cloud Service Provider:

The terms by which the Cloud Provider (Microsoft) abides regarding Data Protection are detailed in the Microsoft Products and Services Data Protection Addendum, regularly updated and available at: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>.

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) ☒

(Regulation (EC) N° 1406/2002 as amended, Article 2 par. 3. b) and EMSA Single Programming Document 2023-2025, Section III, 4.4)

- (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): Seafarers subject to certification or endorsement under Directive (EU) 2022/993

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	<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 (Seafarers)	<input checked="" type="checkbox"/>

Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	<input type="checkbox"/>
Designated Contractors' staff members	<input type="checkbox"/>
<p>Other (please specify):</p> <p>Competent authorities in the EU, Norway and Iceland responsible for the issuing of the certificates to Seafarers while carrying out their obligations under Directive (EU) 2022/993 on the minimum level of training of seafarers;</p> <p>Other Maritime Administration officers in line with their obligation to comply with the verification of the authenticity and validity of the certificates issued to the seafarers that they are asked to recognise;</p> <p>Enforcement authorities acting in their line of duty (such as port state control officers or maritime police).</p>	
<p>8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))</p> <p><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></p>	
<p>Data are transferred to third country recipients:</p> <p>Yes <input type="checkbox"/></p> <p>No <input checked="" type="checkbox"/></p> <p>If yes, specify to which country:</p> <p>If yes, specify under which safeguards:</p> <p>Adequacy Decision of the European Commission <input type="checkbox"/></p> <p>Standard Contractual Clauses <input type="checkbox"/></p> <p>Binding Corporate Rules <input type="checkbox"/></p> <p>Memorandum of Understanding between public authorities <input type="checkbox"/></p>	

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) ☒

Azure EU hosted (i.e. Germany West Central Region)

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.

20 Years