Ref. Ares(2026)6533542 - 29/06/2026

European Maritime Safety Agency

TEMPLATE FOR RECORDING OF PROCESSING ACTIVITY

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

Filling instructions

(When you finish, delete these instructions and save the file.)

hr.info@emsa.europa.eu
Tel +351 21 1209 200 / Fax +351 21 1209 XXX
EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal / emsa.europa.eu

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

NAME OF PROCESSING ACTIVITY[1]: Use of GPT@EC at EMSA

1) Controller(s)[2] of data processing operation (Article 31.1(a))
Controller: European Maritime Safety Agency (EMSA) Organisational unit **responsible**[3] for the processing activity: Head of Department 3 under the following mailbox: hr.info@emsa.europa.eu Contact person: Head of Department Digital Service Data Protection Officer (DPO): dpo@emsa.europa.eu
2) Who is actually conducting the processing? (Article 31.1(a))[4]
The data is processed by EMSA itself ☒ The organisational unit conducting the processing activity is: Digital Service Department
The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party ☐ Contact point at external third party (e.g. Privacy/Data Protection Officer):

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 information is handled in relation to processing operations on the use of the GPT@EC service, the primary aim of which is to provide a platform version of a generative AI tool that embeds a fully operational general purpose conversational platform with proper access controlled through EU Login and a secure

[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?

infrastructure to keep information processed and controlled by the Commission. GPT@EC service is provided by DIGIT B.1 and is presented below.

GPT@EC service is offered to EMSA as production-grade service, with support services and a service-level agreement (SLA) in place for availability of the service; the SLA is, however, based on a fair use principle, and where applicable respect of the assigned quota.

GPT@EC is strictly for professional use and supports the processing of sensitive non-classified (SNC) information, fully complying with relevant corporate policies. GPT@EC supports three sensitivity levels that correspond to the information confidentiality levels of the Commission: Publicly available (PA); Commission use (CU); and Sensitive non-classified information (SNC). The processing of classified information (EUCI) or any special categories of personal data as defined by the GDPR Regulation 2018/1725 is strictly prohibited.

On one hand, the processing of personal data is to provide DIGIT with information about EMSA users for authenticating and authorising secure users access to the EU Login system and Identity & Access Management Service (IAMS).

On the other hand, the processing activities are linked to the handling of the prompt (input) and the generation of the output by the LLM, this is performed automatically, without the need of further human intervention. This processing activity does not fall under the scope of an automated individual decision-making.

EMSA users are responsible for the data they provide (e.g. prompts or attachments) and for using any output generated by GPT@EC in line with the EC AI Guidelines for Staff and EMSA Guidance for Staff on the use of online available Artificial Intelligence Tools **Ares(2025)6773981** Prompts must be drafted in accordance with any output provided by GPT@EC shall be appropriately revised before using it in any document.

EMSA users are responsible for ensuring that they do not use GPT@EC for prohibited practices or high-risk scenarios as described in the Regulation (EU) 2024/1689 (AI Act). Prohibited practices include using AI to manipulate human behaviour or using subliminal techniques, examples of high-risk scenarios include biometric identification or recruitment processes. High-risk uses require strict safeguards and possible corporate governance approval. Violation of these provisions may result in the suspension or termination of the access to the GPT@EC service.

EMSA users are responsible for protecting their personal data, refraining from processing **any special categories of data (sensitive personal data)**, as defined by Regulation (EU) 2018/1725, such as health-related data. For handling other personal data, ensure that processing is accurate, proportionate, and necessary.

EMSA users are responsible for minimising the use of personal data, using proper tools for anonymised data in their inputs and critically evaluating outputs before reusing to prevent the inadvertent disclosure of personal data, which could occur through model inference.

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):

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):	

(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	☒
Managers of data subjects	☐
Designated EMSA staff members	☐
Designated Contractors' staff members	☐
Other (please specify): Informatics (DIGIT)]	

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	☐
Memorandum of Understanding between public authorities	☐

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): Concerning to the data provided by EMSA to DIGIT for the execution of the SLA, the data is stored in ARES. Regarding to the data stored as result of the use of the service, please see this specific processing operation included in the DPO's public register DPR-EC-25348.2 GPT@EC.

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.

Concerning to the data provided by EMSA to DIGIT for the execution of the SLA, the data is stored in ARES as part of the SLA file. According to the EMSA retention list, these types of files related to legal commitments are kept for 10 years after the end of the contract and afterwards, eliminated.

Regarding to the data stored as result of the use of the service, please see this specific processing operation included in the DPO's public register DPR-EC-25348.2 GPT@EC

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

Electronically signed on 25/06/2026 16:48 (UTC+02)