

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

NAME OF PROCESSING ACTIVITY¹:

Incident reporting for non-EMCIP users.

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 2.1</p> <p>Contact Person: Enrico Gironella (EMCIP-helpdesk@emsa.europa.eu)</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: [Unit 2.1]</p> <hr/> <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>

3) Purpose of the processing (Article 31.1(b))

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?

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.

According to the Article 17.3 of Directive 2009/18/EC (hereinafter AID), the Accident Investigative Bodies (AIB) of the Member States shall notify the Commission on marine casualties and incidents in accordance with the format in Annex II, AID. They shall also provide the Commission with data resulting from safety investigations in accordance with the database schema. The EMCIP platform has been developed to store and analyse marine casualties and incident data in accordance with the Article 17.1 and to support improving the quality of investigation reports as per Article 14.3.

The high-level components of the EMCIP platform include: (i) a reporting tool, where the user community can report data on marine casualties and incidents, (ii) a query engine and export tool, used to retrieve data, (iii) an interface with Jaspersoft business intelligence tools, supporting the data analysis, (iv) an administration console for the security settings, workflow configuration, taxonomy editor and other tasks relevant for the database administration, (v) a public portal where a subset of data on marine accident and incidents is shared with the public in line with the data sharing policy agreed by the Permanent Cooperation Framework (PCF), established as per Article 10.

The management of users and organisations is done via the EMSA Identity Management (IdM) platform whereas the users' authentication in EMCIP is carried out by the EMSA portal, in line with the ICT policy of the Agency.

The EMCIP user community needs to provide EMSA with personal data in order to get the credentials to access the tool and to facilitate the cooperation between MS in the conduction of joint safety investigations (e.g. the reporting of a given occurrence can be shared between investigators belonging to different organisations to increase efficiency and effectiveness in reporting).

Within the agreed technical implementation for 2020, a new functionality will be developed to allow persons not provided with EMCIP credentials (i.e. public users) to send to the interested AIB reports concerning marine casualties or incidents, thus facilitating the notifications to the AIBs as per Article 6 and the subsequent reporting into EMCIP as per Article 17.

The entailed workflow is described in the following steps:

- a. A public user wishing to report a marine casualty/incident opens a web interface made available via the EMCIP portal and/or the EMSA website;
- b. He/she enters the following personal data for the registration process: name, surname, email address, phone number, reporting entity (e.g. crew member, company, ship agent etc);
- c. EMCIP sends an automatic email to the indicated email address containing a security code (token) and the instructions to report in the system;
- d. The public user selects the competent AIB, then he/she fills-in the report as deemed as

appropriate. In addition to factual information, the public user has the possibility to upload other files relevant to the marine casualty / incident, like videos or photos;

- e. EMCIP notifies the interested AIB that a new report, created by a public user, is available and should be treated for the follow-up actions. Depending on its assessment, the newly created report can be submitted into EMCIP or discarded;
- f. The competent AIB may decide to contact the public user via the personal data indicated at the previous letter b. for further details on the event (e.g. he/she might be a key witness of an occurrence leading to a safety investigation).

The personal data processing is needed to allow:

- MS to fulfil the reporting obligations stemming from Article 17, AID;
- EMCIP community to analyse data on marine casualties and incidents;
- EMSA and the Commission to assess the quality of safety reports as per Article 14, AID;
- EMSA to analyse safety reports to identify added value in terms of lessons to be drawn at EU level and in drafting a yearly overview of marine casualties and incidents;
- To facilitate the cooperation between AIBs;
- To implement the reporting tool for public users (planned in Q4 2020) facilitating the reporting of marine casualties and incidents into EMCIP as agreed by the PCF. For this specific feature, the personal data processing is needed to allow:
 - the EMCIP system to send the automatic email to the public user to start the reporting process, and;
 - the competent AIB that receives the notification to contact the public user in case further clarification on the occurrence are needed.

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) ☒

- Article 2 'Core tasks of the Agency', par.4 b) Regulation (EC) Nr.1406/2002 as amended (EMSA Founding regulation);
- Article17 of AID and letter from the Commission ref. ARES (2011)1088721 dated 13/10/2011, which appointed EMSA with the management of the EMCIP database;
- Supporting the activities to improve the quality of investigation reports as per Article 14, AID;
- Under the Article 2.c of EMSA founding regulation, EMSA is charged with the analysis of accident investigation reports to identify added value in terms of

lessons to be drawn at EU level. The Agency also uses EMCIP to compile a yearly overview of marine casualties and incidents.

- Single Programming Document 2017-2019, providing that the Agency should develop an improved version of EMCIP to be hosted at EMSA.

(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

The non-EMCIP user will be explicitly informed of the personal data processing via a disclaimer and access to the relevant EMSA policy

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): Data subjects concerned are the authorised users of the EMCIP platform, including (i) users belonging to the national entitled Authorities, (ii) EMSA accident investigation staff, public users that finalise the authentication procedure to submit a notification to the competent AIB.

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):

Personal details include name, surname, email, phone number

Professional details including address, telephone, fax, business email, organisation to which the user belongs to

(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 checked="" type="checkbox"/> |
| Managers of data subjects | <input type="checkbox"/> |
| Designated EMSA staff members | <input checked="" type="checkbox"/> |
| Designated Contractors' staff members | <input type="checkbox"/> |
| Other (please specify): | |
| <ul style="list-style-type: none">• The entitled Authorities from the MS that have access to EMCIP under Article 17, AID | |

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

☐

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):

Personal data of EMCIP users provided with credentials (usernames and password) are stored within the EMSA ICT infrastructure.

Personal data of public users wishing to report marine casualties / incidents will be temporarily stored in the EMCIP server and automatically deleted after 60 days. Data sent to the AIBs is subject to national rules on data protection.

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.

According to the AID, data stored in EMCIP concerning marine casualties and incidents are persistent over the years and made promptly available to users.

Personal data concerning users belonging to national entitled Authorities or EMSA staff are kept as long as these entities consider the user active in this field.

Personal data for non-EMCIP users will be stored in the EMCIP server for 60 days, then will be automatically deleted.

This period is justified by the possibility, for the competent AIB, to decide whether launching a safety investigation within the timeframe established by Directive 2009/18/EC, art.5.5 (i.e., not later than 2 months after the marine casualty occurs).

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