

Data Protection Statement/Privacy Statement on the processing of personal data in the context of European database for reporting and analysis information concerning marine casualties and incidents

The protection of privacy is of high importance to the European Maritime Safety Agency ('EMSA'). EMSA is responsible for the personal data it processes. Therefore, we are committed to respecting and protecting the personal data of every individual and to ensuring efficient exercising of data subject's rights. All the data of personal nature, namely data that can identify an individual directly or indirectly, will be handled fairly and lawfully with the necessary due care.

This processing operation is subject to Regulation 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. The information in this Privacy Statement is given pursuant to Articles 15 and 16 of the Regulation 2018/1725.

1. Nature and the purpose(s) of the processing operation

The purpose(s) of the processing of personal data is/are:

[EMCIP is the European database for reporting and analysis information concerning marine casualties and incidents. 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 public user wishing to report a marine casualty/incident opens a web interface made available via the EMCIP portal and/or the EMSA website;
- 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);
- EMCIP sends an automatic email to the indicated email address containing a security code (token) and the instructions to report in the system;
- 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;
- 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;
- 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.

EMSA will not reuse the personal data for another purpose that is different to the one stated above.

2. Categories/types of personal data processed

Personal details include name, surname, email, phone number.

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

Metadata contained in the uploaded files (e.g. video, pictures or documents).

3. Processing the personal data

The processing of the personal data needed to create and manage users is done via the EMSA Identity Management platform in line with the EMSA ICT policies.

The processing of the personal data of the public users reporting an occurrence via EMCIP is carried out under the responsibility of the Head of Unit 2.1, acting as delegated EMSA data controller.

4. Access to and disclosure of personal data

The personal data is disclosed to the following recipients:

The information concerning the personal data of the EMCIP users will only be shared with people necessary for the implementation of such measures *on a need to know* basis. The data are not used for any other purposes nor disclosed to any other recipient.

The information in question will not be communicated to third parties, except where necessary for the purpose(s) outlined above.

Personal data are not intended to be transferred to third countries.

5. Protecting and safeguarding personal information

EMSA implements appropriate technical and organisational measures in order to safeguard and protect data subjects' personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.

All personal data related to EMCIP reporters are stored in secure IT applications according to the security standards of the Agency as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of *access are granted* individually only to the above recipients.

Personal data could be shared with the interested entitled authorities for the purposes described at the previous point 1.

The database is password protected under single sign-on system and automatically connected to the user ID. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.

6. Access, rectification, erasure or restriction of processing of personal data

Data subjects have the right to access, rectify, erase, and receive their personal data, as well as to restrict and object to the processing of the data, in the cases foreseen by Articles 17 to 24 of the Regulation 2018/1725

If data subjects would like to exercise any of these rights, they should send a written request explicitly specifying their query to the delegated data controller, Head of Unit 2.1.

The right of rectification can only apply to inaccurate or incomplete factual data processed within the... [procedure.

The above requests will be answered without undue delay, and in any event within one month of receipt of the request. However, according to article 14 (3) of the Regulation 2018/1725 that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. EMSA shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

7. Legal basis for Data processing

Processing is based on Article(s) 5, a) of the Regulation 2018/1725 and EMSA founding Regulation 1406/2002 as amended.

The personal data are collected and processed in accordance with ED decision 2020/018 amending the Implementing Rules concerning Protection of Personal Data by the European maritime Safety Agency.

The legal basis justifying the data processing are:

- Article 17 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 Regulation (EC) Nr.1406/2002 as amended (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

8. Storing Personal data

EMSA does not keep personal data longer than necessary for the purpose(s) for which that personal data is collected.

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 public EMCIP users will be stored in the EMCIP server for 60 days, then will be automatically deleted.

In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.

9. Data protection points of contact

Should data subjects have any queries/questions concerning the processing of your personal data, they should address them to the data controller, Head of Unit 2.1 under the following mailbox: [EMCIP-helpdesk@emsa.europa.eu]¹.

Any data subject may also consult EMSA Data Protection Officer at: DPO@emsa.europa.eu.

Recourse:

¹ Please use a functional mailbox, not a personal one, as far as possible – this saves time when updating records and contributes to business continuity.

Complaints, in cases where the conflict is not resolved by the Data Controller and/or the Data Protection Officer, can be addressed at any time to the European Data Protection Supervisor: edps@edps.europa.eu.