EMSA
European Maritime Safety Agency

TEMPLATE FOR RECORDING OF PROCESSING ACTIVITY

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

NAME OF PROCESSING ACTIVITY[1]:

Use of HERMES, ARES (Advanced Records System) and NOMCOM (Nomenclature Commune)

1) Controller(s)[2] of data processing operation (Article 31.1(a))

Controller: European Maritime Safety Agency (EMSA), Executive Director

Organisational unit **responsible**[3] for the processing activity: A.1 Human Resources & Internal Support

Contact person: Carmen Ruiz León: carmen.ruiz-leon@emsa.europa.eu

Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: 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: Every Unit at EMSA

The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party Directorate-General for Informatics of the European Commission (DIGIT)   ☒

Memorandum of Understanding on HAN Services between the European Maritime Safety Agency and the Directorate-General for Informatics of the European Commission. Reference: DIGIT-00737-000

Contact point at external third party (e.g. Privacy/Data Protection Officer): DIGIT-ARES-SUPPORT@ec.europa.eu

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?

EMSA's Records Management Policy and Procedures[5] implements an effective policy for the management and archiving of documents and files based on a body of common rules and procedures. Managing the Agency's documents and files (and the personal data which may be contained in the documents themselves or in their metadata) is intended to meet a whole array of essential needs of the institution, namely improving the quality of its services, preserving its memory, allowing it to account for its activities to its auditing institutions, and allowing transparency towards its citizens.

EMSA's Records Management Policy and Procedures establishes the framework under which official documents and official files are managed in compliance with the Council Regulation (EU) 2015/496 of 17 March 2015 amending Regulation (EEC, Euratom) No 354/83 as regards the deposit of the historical archives of the institutions at the European University Institute in Florence.

Under the new Regulation, the European Agencies are obliged to put in place organisational and physical structures to implement the regulation; to establish its Historical Archives and to develop strategies for preserving born digital records. All official files are managed throughout their lifecycle.

The aim is further to register all documents drawn up or received by the Agency within the scope of its activities, which are likely to require action, follow-up or a reply from the Agency or which contain important information that is not short-lived. The purpose of the registration is to provide evidence that a record has been created or captured in a records system.

The aim is also to file all the registered documents to meet administrative and legal requirements according to the retention periods and disposition actions described on the EMSA Specific Retention List.[6]

The processing of personal data is used, to the extent necessary, at the following stages in the life cycle of documents:

- registration of the appropriate documents;
- filing these documents;
- assigning documents to functional mailboxes, virtual entities, officials or other members of EMSA staff for action, information or circulation, including deadline management;
- creation of workflows (e-Signatories for outgoing documents and assignment of incoming documents), including approval by EMSA staff;
- structured transmission of documents between internal users in the Commission and EMSA via ARES in comparison to non-structured transmission via e-mail (Outlook);
- managing the transfer of responsibilities between Agency's departments and units, including the transfer of files to the Agency's Central Archives first and later to the EMSA's historical archives;
- elimination of documents, files and/or their metadata in accordance with EMSA Specific Retention List;
- creating an audit trail of operations to guarantee the authenticity and security of the files stored in the

---

[5] EMSA Records Management Policy and Procedures: http://emsanet/index.php/dm/records.html

[6] EMSA Specific Retention List: http://emsanet/index.php/dm/procedures.html

repository (electronic file repository);

- access, based on the 'right to know' principle, for members of EMSA staff to the documents and files relating to their tasks;
- accountability towards the Commission, the Parliament, the Court of Auditors, OLAF, the Court of Justice, etc.);
- public access to documents and transparency towards citizens.

The following safeguards are in place to ensure the rights of the data subjects:

- The visibility of the documents when personal data are contained is restricted by markings in ARES. The access to documents with markings are being granted on the basis of the "need to know principle".

- The visibility of files when personal data are contained is restricted to the file's users and readers on the basis of the "need to know principle".

- The elimination after the corresponding administrative retention period of specific categories of files when personal data are contained according to the EMSA specific retention list.

- Personal File electronic data is mainly kept in the E-Personal File application. Documents and files related to staff members will be only identified by personnel number (not names) in ARES-NOMCOM.

- Access to EMSA's registered documents and files (including personal data) is protected by means of a login and access rights which are strictly limited in accordance with the 'need to know' principle and are based on the duties entrusted to access holders. Access rights are linked to a person's position and are thus constantly updated on the basis of the position the person occupies. The usernames (logins) and passwords are managed by the European Commission's common authentication service.

- Every access right holder in ARES-NOMCOM may delegate his or her rights to someone they trust in the interests of the smooth operation of the service. This delegation is transparent and reversible. The person who delegates his or her rights retains responsibility. The delegation is linked to the person's position, and as a result the person loses all his or her access rights when he or she leaves that position. 'Audit trail' methods apply to all access to and manipulation of data in ARES-NOMCOM and can be used if there is an investigation.

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) ☒

Regulations and standards which have a direct impact on the document management of the Agency:

- EMSA Founding Regulation and Regulation (EC)1406/2002 as amended

- Obligation to open Historical Archives Council Regulation (EU)2015/496 as amended

- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union

institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

- Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

- Financial Regulation of the European Maritime Safety Agency adopted by the Administrative Board on 18 December 2013

- Staff Regulations of Officials ('Staff Regulations') and the Conditions of Employment of Other Servants of the European Union ('CEOS') laid down by Council Regulation (EEC, Euratom, ECSC) No 259/687, as amended

- Decision nº2004/08 of the Executive Director on Code of Good Administrative Behaviour for Staff of the European Maritime Safety Agency (EMSA) in their relation with the Public

- Internal Control Standards ICS 11. Document Management

(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   ☐

<div style="border: 2px solid black; padding: 10px;">

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.

</div>

(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

By relevant privacy statement

5) Description of the categories of data subjects (Article 31.1(c))
Whose personal data are being processed?

---

7   OJ L 56, 4.3.1968, p. 1, as last amended by Regulation (EU, Euratom) No 1023/2013 of the European Parliament and of the Council of 22 October 2013, OJ L 287, 29.10.2013, p.15.

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):	☒

Given that ARES-NOMCOM is an internal tool to the Commission, Executive Agencies and Decentralised Agencies such as EMSA but not a public registry, the recipients of treatment of documents are exclusively those internal to the Commission, Executive Agencies or Decentralised Agencies that access data in accordance always with the "need to know" principle, to fulfil their tasks.

Commission staff, Executive Agencies staff, Decentralised Agencies staff such as EMSA staff will not have access to documents and files containing personal data that could undermine the privacy and the integrity of the individual. (See point 3)

However, it is possible for external stakeholders to request access to the documents, in which case the request is reviewed according to Regulation 49/2001 on Access to Documents (http://www.europarl.europa.eu/RegData/PDF/r1049_en.pdf) and related legislation, including Regulation

45/2001 on data protection (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF), before any access to documents is granted.

<table>
<tr><td>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.</td></tr>
</table>

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.

<table>
<tr><td>9)   Technical and organisational security measures (Article 31.1(g))

Please specify where the data are stored during and after the processing</td></tr>
</table>

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): Electronic data are stored in the Commission's Data Centre in Luxembourg and are therefore protected by a number of measures introduced by DG DIGIT to protect the integrity and confidentiality of the Commission's electronic assets. Physical access to the data centre is restricted to selected personnel only and secured by recent security protocols.	

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 available on EMSA Intranet.
The storage period of documents is defined by EMSA Specific Retention List and varies from topic to topic.

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