European Maritime Safety Agency

Record of Processing Activity

Digital Access Reinforcement Program (DARP)– Mobile Application Management (MAM)

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

Digital Access Reinforcement Program (DARP) – Mobile Application Management (MAM)

NAME OF PROCESSING ACTIVITY: Mobile Application Management (MAM) for access to EMSA digital services

1) Controller of data processing operation (Article 31.1(a))
Controller: European Maritime Safety Agency (EMSA) Organisational unit **responsible** for the processing activity: **Horizontal Digital Services** Contact person: Antoine DAMAGEUX / ICT Service Desk (ICT.ServiceDesk@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))
The data is processed by EMSA itself ☒ The organisational unit conducting the processing activity is: Horizontal Digital Services
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):

ict.servicedesk@emsa.europa.eu
Tel +351 21 1209 321
EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal / emsa.europa.eu

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 purpose of the processing is to protect EMSA organisational data when accessed from mobile applications on personal devices.

Mobile Application Management (MAM) is used to enforce application-level security controls, ensure secure authentication, prevent unauthorised data disclosure, and allow selective removal of organisational data where required.

The processing supports EMSA's information security objectives while ensuring that personal devices remain unmanaged and private.

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): User account identifier (e.g. EMSA username), application metadata, operating system version, mobile device name (name of the smartphone)	

(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): Access is limited to authorised ICT staff for administrative and security purposes.

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): Data is stored and processed within Microsoft Intune, Microsoft Entra ID, and Microsoft 365 cloud services, under EMSA institutional agreements and security controls.

Security measures include authentication controls, encryption, application-level data isolation, access logging, and selective data removal.

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.

Personal data is retained only for the duration necessary to provide secure access to EMSA services and in accordance with EMSA Records Management Policy.

Application-related metadata is automatically deleted when the user account is deactivated or when access is no longer required.

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

Electronically signed on 30/04/2026 11:59 (UTC+02)