

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

NAME OF PROCESSING ACTIVITY¹:

Collection, use and management of private mobile telephone numbers of officials, temporary agents, contract staff, trainees, SNEs and NEPTs in the context of the Business Continuity Plan (hereafter BCP) security management and other emergency situations.

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 4.2 Legal, Finance and Facilities</p> <p>Contact person: Dominika Lempicka-Fichter, Head of Unit 4.2 Legal, Finance and Facilities</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 x</p> <p>The organisational unit conducting the processing activity is: Unit 4.2 Legal, Finance and Facilities and Unit 4.1 Human Resources and Internal Support</p> <hr/> <p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party <input type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</p>

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?

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.

Without prejudice to other legitimate purposes defined under the Staff Regulations, staff personal contact details shall be processed and used exclusively for BCP purposes, i.e. to prepare (exercises) and respond to crises and/or operational disruptions affecting the normal functioning of EMSA, as well as to send security and safety alerts. It shall be made clear to staff that the purposes of these measures is not to intrude in their private lives; that in normal circumstances, the information would not be used and that access to this information will be limited on the basis of the 'need to know' principle. This point should also be made clear to management. Access to such data will only be granted to a limited number of identified staff.

The on-line collection and updating of private mobile phone numbers of EMSA staff with a view to their use primarily in the context of EMSA's Business Continuity Plan, but also in other security and safety related and emergency situations.

Business Continuity Management (BCM) serves EMSA to prepare and respond to business disruptions. The process involves all EMSA Departments and Unit, as timely and efficient communication is critical. In the event of a major disruption, EMSA must contact staff quickly which occur at any time, possibly other normal office hours. Staff in charge of business continuity response and/or critical or essential functions must be immediately informed. Staff more generally must be informed of such events, in line with the Agency's duty of care.

An IT tool Calles AcySms will be used for this purpose and will enable a sms notification to be sent to each staff member on his/her mobile phone. The mobile numbers are entered and updated by the staff members themselves, in the event that they change their mobile number.

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)

x

(Examples of legal basis: e.g. Article 2 'Core tasks of the Agency', par.4 b) EMSA founding regulation)

Under 15.2(e) of the EMSA Founding Regulation, Regulation (EC) No 1406/2002, as amended, the Executive Director shall exercise (e) he/she shall exercise, in respect of the staff, the powers laid down in Article 6(2). As part of the duty of care incumbent upon the Executive Director as Appointing Authority, staff need to be informed of disruptions affecting the normal functioning of EMSA and which may have consequences for the health and wellbeing of the staff.

(b)	compliance with a legal obligation to which EMSA is subject	<input type="checkbox"/>
(c)	necessary for the performance of a contract with the data subject or for the preparation of such a contract	<input type="checkbox"/>
(d)	Data subject has given consent (<i>ex ante</i> , explicit, informed)	<input type="checkbox"/>
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))		
<i>Whose personal data are being processed?</i>		
	EMSA staff	x
	EMSA officials, temporary agents, contract agents, Seconded National Experts as well as personnel working <i>intra muros</i> such as interims, trainees, NEPTs, contractors	
	Non-EMSA staff	x
	N/A	
	Relatives of the data subject	<input type="checkbox"/>
	Other (please specify):	
6) Categories of personal data processed (Article 31.1(c))		
<i>Please tick all that apply and give details where appropriate</i>		
(a) General personal data:		
The personal data contains:		
	Personal details (name, address etc)	x
	Only name, surname and mobile phone number.	
	Education & Training details	<input type="checkbox"/>
	Employment details	<input type="checkbox"/>
	Financial details	<input type="checkbox"/>
	Family, lifestyle and social circumstances	<input type="checkbox"/>

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 ☐

7) Recipient(s) of the data (Article 31.1 (d))

Recipients are all parties who have access to the personal data

Data subjects themselves x

Managers of data subjects ☐

Designated EMSA staff members x

Access to this information will be limited on the basis of the 'need to know' principle. Access to the data stored

by the tool will only be granted to a limited number of identified staff, namely the Webmaster in the Executive

Office, the Head of Unit 3.2 Digital Infrastructure, the Senior Project Officer in Department 3 Digital Services and Simplification, the Security Team including Security Officer within Unit 4.2 Legal, Finance and Facilities, the Senior Human

Resources Officer in the Unit 4.1 Human Resources and Internal SupportThe Webmaster in the Executive Office, the Head of Unit 3.2 Digital Infrastructure, the Senior Project Officer in Department 3 Digital Services

and Simplification and the Security Team within Unit 4.2 Legal, Finance and Facilities Messages can send messages to all staff (and other identified groups) through the tool following procedures established in EMSA Security Rules

Designated Contractors' staff members ☐

Other (please specify):

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 x

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 ☐

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): x

The data is collected through an IT tool called AcysSms. AcySms is a component fully integrated in Joomla, the Web Content Management System used by EMSA. AcySms is installed in the EMSA intranet at <http://emsanet/e-sms/>.

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 [here](#).

The mobile phone number is kept for as long as the staff member works in EMSA and will be erased in the tool as soon as possible after the departure from EMSA and at the latest within six months