

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

NAME OF PROCESSING ACTIVITY¹:

SMS Notification - Collection, use and management of private mobile telephone numbers of EMSA officials, temporary agents, contract agents, Seconded National Experts, NEPTs, interims, trainees 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: Andrea Iber, 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</p>
<p>The data is processed by a third party (contractor) <input checked="" type="checkbox"/> or the processing operation is conducted together with an external third party</p> <p>Meo Serviços de comunicações e multimídia, SA</p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</p> <p>DPOAlticePortugal@altice.pt</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 for Business Continuity Plan purposes. This includes preparing for and responding to crises and operational disruptions that may affect the normal functioning of EMSA, as well sending security and safety alerts.

For this reason, EMSA processes the staff's name, surname and private mobile phone number to primarily use them in the context of EMSA's Business Continuity Plan, but also in other security and safety related emergency situations.

The Business Continuity Plan serves EMSA to prepare and respond to business disruptions. The process involves all EMSA Departments and Units, as timely and efficient communication is critical. In the event of a major disruption, EMSA must contact staff quickly, which may occur at any time, possibly outside regular office hours. Staff responsible for business continuity response and critical or essential functions must be immediately informed. Staff, more generally, must also be informed of such events, which is in line with the Agency's duty of care.

EMSA has contracted a communication tool (SMS gateway) designed to send SMS alerts to EMSA staff instantly. Users' data (name/ surname and mobile phone) will be stored in the EMSA intranet server, which is the tool used by staff members to enter and update their mobile contact details voluntarily. If they change their mobile number, the staff member shall update their number.

The webmaster will collect the data and then transfer it to ICT Service Desk, who will upload the personal data into the SMS gateway, a web-based application, a product provided by the contractor.

The intranet account containing the mobile number of staff members who have left the service are deleted from the systems on a regular basis, based on information provided by Unit 4.1.

EMSA shall make clear to staff that the purpose of these measures is not to intrude into their private lives. In normal circumstances, the information will not be used and access to it will be limited based on the 'need to know' principle. Access to such data will only be granted to a limited number of identified staff.

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 ☐
- (c) necessary for the performance of a contract with the data subject or for the preparation of such a contract ☐
- (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	x
EMSA officials, temporary agents, contract agents	
Non-EMSA staff	x
Seconded National Experts, NEPTs, interims, trainees	
Relatives of the data subject	N/A
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)	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	<input type="checkbox"/>
Other (please give details):	
(b) Sensitive personal data (Article 10)	
The personal data reveals:	
Racial or ethnic origin	<input type="checkbox"/>
Political opinions	<input type="checkbox"/>
Religious or philosophical beliefs	<input type="checkbox"/>
Trade union membership	<input type="checkbox"/>
Genetic, biometric or data concerning health	<input type="checkbox"/>
Information regarding an individual's sex life or sexual orientation	<input type="checkbox"/>
7) Recipient(s) of the data (Article 31.1 (d))	
<i>Recipients are all parties who have access to the personal data</i>	
Data subjects themselves	x
Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	x
<p>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, Head of Department 3 and 4, the Head of Unit 3.3 Horizontal Digital Services, staff of EMSA ICT ServiceDesk acting as administrator of the system, EMSA Security Officer supported by EMSA Security and Safety team, Head of Executive Office supported by the Communication team.</p> <p>Messages to all staff shall be send following procedures established in EMSA Security Rules</p>	

Designated Contractors' staff members	<input checked="" type="checkbox"/>
Other (please specify):	
8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e)) <i>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.</i>	
<p>Data are transferred to third country recipients:</p> <p>Yes <input type="checkbox"/></p> <p>No x</p> <p>If yes, specify to which country:</p> <p>If yes, specify under which safeguards:</p> <p>Adequacy Decision of the European Commission <input type="checkbox"/></p> <p>Standard Contractual Clauses <input type="checkbox"/></p> <p>Binding Corporate Rules <input type="checkbox"/></p> <p>Memorandum of Understanding between public authorities <input type="checkbox"/></p>	
9) Technical and organisational security measures (Article 31.1(g)) <i>Please specify where the data are stored during and after the processing</i>	
<p>How is the data stored?</p> <p>EMSA network shared drive <input type="checkbox"/></p> <p>Outlook Folder(s) <input type="checkbox"/></p>	

Hardcopy file

☐

Cloud (give details, e.g. public cloud)

☐

Servers of external provider

☒

Other (please specify):

x

Data (name/surname/mobile phone) is store in the EMSA intranet server (<http://emsanet>) as part of each user login profile. The intranet uses Joomla (EMSA's web content management system).

This data is later imported into Users Data (name/surname/mobile phone) will be stored on the MEO/Altice Cloud server.

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 personal data is kept for as long as the staff member works in EMSA and will be erased from the tools as soon as possible after the staff member departs from EMSA and, at the latest, within six months.