

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

NAME OF PROCESSING ACTIVITY:

Management of EU Login at EMSA

<b>1) Controller(s)<sup>1</sup> of data processing operation (Article 31.1(a))</b>
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit <b>responsible</b> for the processing activity: Unit 4.1, Human Resources and Internal Support</p> <p>Contact person: Head of Unit 4.1, Human Resources and Internal Support</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: <a href="mailto:dpo@emsa.europa.eu">dpo@emsa.europa.eu</a></p>
<b>2) Who is actually conducting the processing? (Article 31.1(a))<sup>2</sup></b>
<p>The data is processed by EMSA itself <span style="float: right;"><input checked="" type="checkbox"/></span></p> <p>The organisational unit conducting the processing activity is: 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 checked="" type="checkbox"/>:</p> <p>European Commission:</p> <ul style="list-style-type: none"> <li>- DG DIGIT COMREF team for the management of COMREF database</li> <li>- PMO (Paymaster's Office of the European Commission) for the management of RETO database</li> </ul> <p>Privacy Statements:</p> <p><a href="#">COMREF</a></p> <p><a href="#">EU Login Privacy Statement</a></p> <p>Contact point at external third party: European Commission Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu)</p>

<sup>1</sup> In case of more than one controller (e.g. joint operations), all controllers need to be listed here

<sup>2</sup> 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.*

EU Login is the European Commission's user authentication system. It allows authorised users to access a wide range of Commission services such as the EU applications: ABAC, JSIS, Ares, EU login Mobile App, JSIS online, PMO Contact (this list is not exhaustive). It is composed of an email address and a password.

**The Management of EU Login at EMSA activity** consists in facilitating the transfer of personal data to enable the access of EMSA staff to EU Login, as EMSA does not use Sysper (European Commission Human Resources System), which provides this service automatically.

Individual steps used for the processing:

Newcomers at EMSA may create his/her password to the EU login account, but previously, their data must be registered in RETO and COMREF databases, databases managed by the European Commission.

Before a new staff member takes functions at EMSA, the Payroll/HR Officer requests the PMO team to create the EMSA newcomer's PER\_ID and their Sysper number in RETO database.

Once PMO sends the requested information to the Payroll/HR Officer, the information is forwarded to the Document Management Officer (DMO). The DMO completes an excel sheet with the following data of the newcomer:

- Sysper number:
- Birth Date
- EMSA Email address
- Surname
- Name
- Place of work (City)
- Working Telephone Number
- Personal Mobile Number

The DMO converts the excel sheet to txt file and sends the file via WinSCP to COMREF team who creates the new user in COMREF database in 24 hours. COMREF database plays the role of data hub in this context by providing HR reference data to a large amount and wide variety of European Commission systems.

As soon as new staff member data are registered in COMREF database, the new colleague can proceed to create his/her EU login account.

The personal mobile number is needed to enable the double factor authentication of the EU Login. In case of changing the mobile phone number, EMSA staff member sends the new number to the DMO who updates the excel sheet and send it to COMREF team via WinSCP again.

4) Lawfulness of the processing (Article 5(a)–(d)): Processing necessary for:

Mention the legal basis which justifies the processing	
<p>(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) <input checked="" type="checkbox"/></p> <ul style="list-style-type: none"> <li>2019 EMSA SLA DIGIT 026 <a href="#">Ares(2018)6017096</a></li> <li>This processing operation is also in line with Regulation (EU) 2018/1724 on establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 and within the scope of the EC's eGovernment Action Plan 2016-2020 on accelerating the digital transformation of governments.</li> </ul>	
(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)) Whose personal data are being processed?	
<p>EMSA staff <input checked="" type="checkbox"/></p> <p>Officials, TAs, CAs</p>	
<p>Non-EMSA staff (contractors staff, external experts, trainees)</p> <p>SNEs, Trainees and Interims</p>	<input checked="" type="checkbox"/>
<p>Visitors to EMSA building</p> <p>Relatives of the data subject</p> <p>Other (please specify):</p>	<input type="checkbox"/>
6) Categories of personal data processed (Article 31.1(c)) Please tick all that apply and give details where appropriate	
<p>(a) <b>General personal data:</b></p> <p>The personal data contains:</p>	

Personal details (name, e-mail address)	<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> <li>• Sysper number</li> <li>• Birth Date</li> <li>• Surname</li> <li>• Name</li> <li>• Personal Mobile Number:</li> </ul>	
Education & Training details	<input type="checkbox"/>
Employment details	<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> <li>• Place of work (City)</li> <li>• EMSA Email address</li> <li>• Working Telephone Number</li> </ul>	
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) <b>Sensitive personal data</b> (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"/>
<b>7) Recipient(s) of the data (Article 31.1 (d))</b> <i>Recipients are all parties who have access to the personal data</i>	
Data subjects themselves	<input checked="" type="checkbox"/>
Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	<input checked="" type="checkbox"/>
DMO	
Backup of DMO	
Payroll/HR Officer	
Backup of the Payroll Officer	
ICT Senior Project Officer in charge of the WinSCP	
Designated Contractors' staff members	<input type="checkbox"/>
Other (please specify): <input checked="" type="checkbox"/>	
European Commission PMO and COMREF teams	
Also, if appropriate, access will be given to EU staff with the statutory right to access the data required by their function, i.e. the European Ombudsman, the Civil Service Tribunal, the Internal Audit Service, the European Court of Auditors, OLAF and the European Data Protection Supervisor.	
<b>8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))</b> <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>	
Data are transferred to third country recipients:	
Yes	<input type="checkbox"/>

No	<input checked="" type="checkbox"/>
<b>If yes, specify to which country:</b>	
<b>If yes, specify under which safeguards:</b>	
Adequacy Decision of the European Commission	<input type="checkbox"/>
Standard Contractual Clauses	<input type="checkbox"/>
Binding Corporate Rules	<input type="checkbox"/>
Memorandum of Understanding between public authorities	<input type="checkbox"/>
9) Technical and organisational security measures (Article 31.1(g)) <i>Please specify where the data are stored during and after the processing</i>	
How is the data stored?	
EMSA network shared drive	<input checked="" type="checkbox"/>
An excel file and a copy in txt file is kept in P drive restricted to the DMO and her backup	
Outlook Folder(s)	<input checked="" type="checkbox"/>
Hardcoy file <input type="checkbox"/>	
Cloud (give details, e.g. public cloud)	<input type="checkbox"/>
Other (please specify): <input checked="" type="checkbox"/>	
WinSCP	
JIRA Records management help-desk	
Servers of the European Commission as per their Privacy Notice	

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.*

Information related to this process is kept for 1 year in the P-drive, in Jira system and in Outlook, after that period, information is deleted by the DMO from all repositories.

For the data retention for the management of the EU Login in the European Commission, can be found in their privacy statement: [EU Login Privacy Statement](#)