

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

NAME OF PROCESSING ACTIVITY¹:

Security Incident Detection and Response with CERT-EU under SLA CERTEU-039-02 and GMV under FWC RES/01/2017²

1) Controller(s) ³ of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit responsible⁴ for the processing activity: Department 3</p> <p>Contact person: Simone Balboni</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)) ⁵
<p>The data is processed by EMSA itself <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is: [...]</p> <hr/> <p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party: CERT-EU and GMV Security Operations Center <input checked="" type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer): data-protection-officer@ec.europa.eu for CERT-EU, and 'Jairo Montero Santos' (jmontero@gmv.com) for GMV_SoC.</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 And related contract amendments, renewals, extension, new contracts.

³ In case of more than one controller (e.g. joint operations), all controllers need to be listed here

⁴ This is the unit that decides that the processing takes place and why.

⁵ 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.

The purpose and the nature of the processing is related to the mitigation and containment in a timely manner of cyber threats to Continuity/Integrity/Availability of EMSA information assets. This activity will be implemented by monitoring on 24x7x365 basis the logs produced by EMSA services and applications and underlying infrastructure and middleware for the detection of significant security events, incidents, and signs of potential breaches. In order to put in place adequate response measures to mitigate and contain the impact of such threats on EMSA data assets, the processing shall be conducted.

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) ☒
- a) Article 2 ‘Core tasks of the Agency’, par.4, EMSA founding regulation 1406/2002;
b) EU Directive 2016/1148 on security of network and information systems (NIS Directive);
c) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission;
- (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)) <i>Whose personal data are being processed?</i>	
EMSA staff	<input checked="" type="checkbox"/>
Non-EMSA staff (contractors staff, external experts, trainees)	<input checked="" type="checkbox"/>
Visitors to EMSA building	<input type="checkbox"/>
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 (username, IP address, email address)	<input checked="" type="checkbox"/>
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): personal data from logs generated by the interaction of EMSA users with EMSA systems and applications, and PCs registered under EMSA Active Directory service such as: IP address, network traffic, antivirus events, usernames, email addresses. Reports and alerts might also come from	

automated inspection operated on a regular basis by CERT-EU of the Dark Web for records of information related to EMSA.

(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): CERT-EU staff members

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):

The process of “Security Incident Detection and Response” doesn’t collect logs by itself, but rather processes logs already collected for operational purposes by various EMSA services and applications and scans them looking for signs of significant security events, incidents, and breaches. Personal data is not harvested from the logs which are used only for the purpose of anomalies detections and investigations. PCs, applications, network and antivirus logs are collected and handled by the respective services as part of their operations and mainly processed for the scope of this process under the SIEM=Security Event and Incident Management platform [currently operated on Splunk in EMSA premises], as well as in EMSA Intrusion Detection and Prevention systems inside the EMSA perimeter, and in the EMSA corporate services Microsoft tenancy. As EMSA will deploy applications in the Cloud, those logs as well will be inspected by this process for sign of compromise and breaches in the scope of Security Incident Detection and Response.

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.

Security related logs are preserved for up to 5 years, as data processed can be assimilated to the categories of 8.7.3.A and 8.7.4.B of the EMSA Retention List, and in consideration of the need to detect ‘post-mortem’ intrusion situations arising from ATP=Advanced Persistent Threats which is currently the most popular form of hacking and it foresees long timeframe to perpetrate intrusions, in order for the attacker not to be detected by Intrusion Detection Systems and other countermeasures.

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