

## TEMPLATE FOR DATA PROTECTION PRIVACY STATEMENT

### **Data Protection Statement/Privacy Statement on the processing of personal data in the procedure/context of Security Incident Detection and Response**

The protection of privacy is of high importance to the European Maritime Safety Agency ('EMSA'). EMSA is responsible for the personal data it processes. Therefore, we are committed to respecting and protecting the personal data of every individual and to ensuring efficient exercising of data subject's rights. All the data of personal nature, namely data that can identify an individual directly or indirectly, will be handled fairly and lawfully with the necessary due care.

This processing operation is subject to Regulation number 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. The information in this Privacy Statement is given pursuant to Articles 15 and 16 of the Regulation number 2018/1725.

#### **1. Nature and the purpose(s) of the processing operation<sup>1</sup>**

The purpose(s) of the processing of personal data is/are: IT Security Incident Detection and Response with CERT-EU and GMV under FWC RES/01/2017.

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.

EMSA will not reuse the personal data for another purpose that is different to the one stated above.

The processing is not intended to be used for any automated decision making, including profiling.

#### **2. Categories/types of personal data processed**

The categories/types of personal data processed are the following: username, IP address, email address.

<sup>1</sup> Please, provide a brief description of the processing operation and clearly define the purpose(s).

### **3. Processing the personal data**

The processing of the personal data is carried out under the responsibility of the Head of Department 3, acting as delegated EMSA data controller. Personal data are processed by<sup>2</sup> CERT-EU under SLA CERTEU-039-02, GMV Security Operations Centre under FWC RES/01/2017, EMSA staff responsible for and operating IT Service and Applications and Service Desk on a per need basis.

#### **1. Access to and disclosure of personal data**

The personal data is disclosed to the following recipients: Designated EMSA staff members, CERT-EU and designated Contractors' staff members

The information concerning Security Incident Detection and Response will be shared *on a need to know* basis with the above-mentioned recipients for the implementation of mitigation and contention measures. Personal data is not harvested from logs nor used for any other purposes nor disclosed to any other recipient.

The information in question will not be communicated to third parties, except where necessary for the purpose(s) outlined above.

Personal data are not intended to be transferred to third countries.

#### **2. Protecting and safeguarding personal information**

EMSA implements appropriate technical and organisational measures in order to safeguard and protect data subjects' personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to them.

All personal data related to Security Incident Detection and Response are stored in secure IT applications according to the security standards of the Agency as well as in specific electronic folders accessible only to the authorised recipients. Appropriate levels of *access are granted* individually only to the above recipients.

The database is password protected under single sign-on system and automatically connected to the user ID. The e-records are held securely so as to safeguard the confidentiality and privacy of the data therein.

#### **3. Access, rectification, erasure or restriction of processing of personal data**

Data subjects have the right to access, rectify, erase, and receive their personal data, as well as to restrict and object to the processing of the data, in the cases foreseen by Articles 17 to 24 of the Regulation number 2018/1725.

If data subjects would like to exercise any of these rights, they should send a written request explicitly specifying their query to the delegated data controller, Head of Department 3.

The above requests will be answered without undue delay, and in any event within one month of receipt of the request. However, according to article 14 (3) of the Regulation number 2018/1725, that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. EMSA shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

---

<sup>2</sup> Please, indicate all the processors (i.e. contractors or other institutions).

#### **4. Legal basis for Data processing**

The personal data are collected and processed in accordance with:

- a) Article 5 (a) of Regulation 2018/1725;
- b) Article 2 'Core tasks of the Agency', par.4, EMSA founding regulation 1406/2002;
- c) EU Directive 2016/1148 on security of network and information systems (NIS Directive);
- d) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission;

#### **5. Storing Personal data**

EMSA does not keep personal data longer than necessary for the purpose(s) for which that personal data is collected.

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.

In the event of a formal appeal, all data held at the time of the formal appeal should be retained until the completion of the appeal procedures.

#### **6. Data protection points of contact**

Should data subjects have any queries/questions concerning the processing of your personal data, they should address them to the data controller, Head of Department 3, under the following mailbox attended by Department 3 Secretariat: [DPO-Queries-Dept3@emsa.europa.eu](mailto:DPO-Queries-Dept3@emsa.europa.eu).

Any data subject may also consult EMSA Data Protection Officer at: [DPO@emsa.europa.eu](mailto:DPO@emsa.europa.eu).

#### **Recourse:**

Complaints, in cases where the conflict is not resolved by the Data Controller and/or the Data Protection Officer, can be addressed at any time to the European Data Protection Supervisor: [edps@edps.europa.eu](mailto:edps@edps.europa.eu).