## Record of processing activity

### Part 1

<table>
<thead>
<tr>
<th>Name of the data processing</th>
<th>IT Incident handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created on</td>
<td>02/10/2018</td>
</tr>
<tr>
<td>Last update</td>
<td>11/09/2020</td>
</tr>
<tr>
<td>Reference number</td>
<td>014</td>
</tr>
<tr>
<td>Year</td>
<td>2018</td>
</tr>
</tbody>
</table>

1. Controller: European Economic and Social Committee

2.a) Service responsible:

2b) contact details:

helpdesk@eesc.europa.eu

3. Joint controller:

Not applicable

4. DPO: contact details:

data.protection@eesc.europa.eu

5. Processor(s) (where applicable):

Not applicable

6. Purpose(s) of the data processing:

The purpose of processing is to assist EU institutions, bodies and agencies to detect, prevent and recover from cyber-attacks.

7. Description of the categories of persons whose data are processed:

- Individuals involved in IT security incident (perpetrator, victims or relays of a cyber-attacks),
- Individual owners of IT assets subject to specific vulnerability or infection,
- Individual owners of IT assets involved in malicious web or email traffic.
### 8. Description of data categories processed

Security incident handling includes machine-based, automated processing of personal data, in particular for log management and correlation as well as network intrusion detection. Human intervention, in the form of security engineer or system administrator inspection or investigation, is far more limited. The information processed may contain personal data. The personal data that is collected is in connection with security incident handling tasks and operations. Below is an overview of these types of personal data:

- Any file (with user-id included) stored in, transmitted from / to a host involved in an incident (as victim, relay or perpetrator),
- Email addresses,
- User account name (for operating system, applications, centralised authentication services, etc.),
- Technical data (IP address, MAC address, etc.)

### 9. Time limit for retaining the data

Information and files used during incident handling are retained during the incident response procedure.

The maximum duration of any retention for archival purposes will not exceed 2 years. This is for security reasons (e.g. an incident which seems initially benign may a posteriori be considered as the origin of a significant infection. The latter may be revealed several years after the original 'benign' incident).

### 10. Recipients of the data

The IT Security Officer, IT security engineers and IT system administrators who may be called on to handle a security incident and who therefore need access to the technical details of the incident. Only the IT Security Officer and IT security engineers have access to the "CERT-EESC-CDR" functional mailbox.

Information related to cyber-security incident might be transferred to CERT-EU in case of assistance request or simple notification.

### 11. Transfers of personal data to a third country or an international organisation

Not Applicable

### 12. General description of security measures, where possible

In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.

### 13. Privacy statement

IT Incident handling
## Part 2
### Compliance check and risk screening

**1.a) Legal basis and reason for processing**

- **(a)** necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body
- **(b)** necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below
- **(c)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- **(d)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- **(e)** necessary in order to protect the vital interests of the data subject or of another natural person

Tick (at least) one of the boxes

**1b) Legal basis**

2. Are the purposes specified, explicit and legitimate?  
   - **Yes**

3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?  
   - **Not applicable**

4. Do you really need all the data items you plan to collect?  
   - **Yes, all the data processed is necessary.**

5. How do you ensure that the information you process is accurate?  
   - **Not applicable. (automated processing of technical information)**

6. How do you rectify inaccurate information?  
   - **Not applicable.**

7. Are they limited according to the maxim “as long as necessary, as short as possible”?  
   - **Yes**

8. If you need to store certain information for longer, can you split the storage periods?  
   - **Not applicable**

9. How do you inform data subjects?  
   - A privacy statement is published on the Intranet.  
     A link to the CERT EU privacy statement is included in emails exchanged during the incident response procedure. (http://cert.europa.eu/cert/plainedition/en/cert_privacy.html)
10. Access and other rights of persons whose data are processed

<table>
<thead>
<tr>
<th>Individuals involved in incident handling (as victim, perpetrator or relay of a cyber-attack) may exercise their rights by sending an email to the CERT-EESC-CDR functional mailbox.</th>
</tr>
</thead>
</table>

11. Does this process involve any of the following?

|☐ | (a) data relating to health, (suspected) criminal offences or other special categories of personal data |
|☐ | (b) evaluation, automated decision-making or profiling |
|☐ | (c) monitoring data subjects |
|☐ | (d) new technologies that may be considered intrusive |

**Part 3**

**Linked documentation**

1. Links to threshold assessment and DPIA (where applicable)

| No hyperlink inserted |

2. Where are your information security measures documented?

| No hyperlink inserted |

**Organisational Security measures**


**Specific policy on Security incident management:**


**Technical security measures**


3. Links to other documentation

| No hyperlink inserted |

4. Other relevant documents