computer emergency response team CERT-EU
for the EU institutions, bodies and agencies

Guidelines – Notification of cyber-security incident response processes to Data Protection Officers

CERT-EU White Paper – 2014-011
Version 1.0 – 06/01/2015

Introduction

In a number of EU institutions, bodies and agencies, processes have been established to respond to cyber-security incidents. Such processes involve the handling of personal data and therefore they must be subject to a formal notification to the relevant Data Protection Officer. The present document offers a model and recommendations for such a notification. It is intended to be used by cyber-security incident response teams of EU institutions, bodies and agencies.

Reference

REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000.

General Guidelines

Before initiating the notification of data processing, the cyber-security incident response entity should check that:

- The entity is formally established within the organisation and has a documented mandate.
- The list of services delivered by this entity is well known and documented. A model of services for a computer security incident response team is available on ENISA website :

  http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/framework/service-types
- The head of the entity is aware of applicable documents related to data protection (Regulation n°45/2001 and any specific reference within the organisation).
- Staff members of the cyber-security incident response entity are aware on the issues related to data processing.
- The stake-holders of data processing and transfer are well identified (sub-contractors if any, recipients, partners for transfer).
- The incident response team will not pro-actively collect personal data. Personal data that might be accessed by the team will be those technical data normally handled during incident investigation and response (see para 10 of the template).
- IT systems used for processing as well as associated security controls are well identified.
- An individual in the entity has been designated to draft and maintain the notification.
- The processing of personal data must be notified by the data controller to the data protection officer.
- Relations with data subjects have been anticipated (point of contact and process to respond to requests).

Specific Guidelines - Notification Model

The notification model is based on the Notification template used within the European Commission. Specific recommendations in the context of cyber-security incident response have been elaborated based on the experience of CERT-EU and contributions from some other incident response teams.

For each chapter of the Notification template:

- Guidance is provided on how to fill this specific chapter in the context of cyber-security incident response,
- A model of text is provided.

TEMPLATE NOTIFICATION

SUBMISION DATE

[GUIDANCE] – Date at which the notification to the DPO was made.

[TEMPLATE TEXT] - <DD/MM/YYYY>

CONTROLLER

[GUIDANCE] – Mention here the function of individual which is responsible for data protection within the entity in charge of incident response – usually it is the Head of Unit.

[TEMPLATE TEXT] - <Function of the individual>

DIRECTORATE GENERAL TO WHICH THE CONTROLLER IS ATTACHED

[GUIDANCE] – Mention here the Directorate General or equivalent to which the incident response team is attached.

[TEMPLATE TEXT] - <Name of Directorate General of equivalent>

PROCESSING

1. Name of Processing

[GUIDANCE] – Mention here the name of the process during which personal data are handled.

[TEMPLATE TEXT] - IT security incident response within <Insert name of institution / body / agency>

2. Description of Processing

[GUIDANCE] – Indicate here the name and description of services that include the processing of personal data. Typical services of a computer emergency response team (CERT) / computer security incident response team (CSIRT) / security operating center (SOC) are listed below with an indication if personal data could possibly be handled. Pick-up the relevant services and associated template data processing description. Customize as required. Delete services that are not delivered in your organisation and for which no data processing is involved.

Service Name [TEMPLATE TEXT]	**Personal data likely to be involved**	**Data processing description** [TEMPLATE TEXT]
Reactive services		
Alerts and warnings	Yes	• Collection of professional contact details (name, organisation, role, phone number, email address) for people in receiving alerts and warnings, creation of contact / mailing lists • Maintenance of contact / mailing lists
Incident handling	Yes	The is no structured process to collect any personal data during incident handling Personal data might however be communicated to the incident response team during ▪ Incident notification. If the identity of victim of the incident is not removed before notification or if it is possible to access to this identity from the assets details communicated during incident report (Asset inventory number, IP address, email account, etc). ▪ Incident investigation. when the incident response team needs access to artefacts / files contained in, transmitted to / from the IT device(s) involved in this incident
Vulnerability handling	No	
Artefact handling	No	Comment: An artefact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artefacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits. No personal data processing as part of this service.

Proactive services		
Announcements	Yes (1)	• Collection of professional contact details (name, organisation, email address) for mailing lists • Maintenance of contact / mailing lists
Technology watch	No	Comment: No personal data processing as part of this service.
Security audit or assessments	Yes	There is no structured process to collect any personal data during security audit or assessment Personal data might however be accessed to security audit or assessment teams. Identification details (Asset inventory number, IP address, MAC address, etc) of host subject to specific vulnerabilities or infections revealed during the audit process. This information remains anonym (no reference to the name of the owner). Audit reports containing such data are subject to protective security marking to avoid publication.
Configuration & maintenance of security tools, applications & infrastructures	No	Comment: No personal data processing as part of this service.
Development of security tools	No	Comment: No personal data processing as part of this service.
Intrusion detection services	Yes	There is no structured process to collect any personal data during intrusion detection services operations. Personal data might however be accessed by operators of IDS services. In case of alert triggered by the IDS, alert message include identification details (IP address, hostname, etc) of host involved in suspicious network traffic / activities. This information remains anonym (no reference to the name of the owner) and no research of identity is proactively made as part of the IDS operations. IDS alert files are subject to protective security marking to avoid publication.
Security-related information dissemination	No	Comment: No personal data processing as part of this service.
Security Quality Management Services		
Risk analysis	No	Comment: No personal data processing as part of this service.
Business continuity & disaster recovery planning	Yes	• Collection of professional contact details (name, organisation, role, email address) for individuals playing a special role in business continuity & disaster recovery planning. • Maintenance of role lists
Security consulting	No	Comment: No personal data processing as part of this service.
Awareness building	Yes	• Collection of professional contact details (name, organisation, role, email address) for individuals targeted by awareness actions. • Maintenance of such lists
Education / training	Yes	• Collection of professional contact details (name, organisation, role, email address) for individuals targeted by education and training actions. • Maintenance of such lists
Product evaluation or certification	No	Comment: No personal data processing as part of this service.

(1) If distributed via mailing list

3. Sub-contractor

[GUIDANCE] – Indicate if one or more of the services implying personal data processing is/are subject to sub-contracting. Sub-contracting can be made to another entity of your organisation (example: 'Intrusion detection services operations is sub-contracted to the network security team'), or to an external entity (example: 'security audit is sub-contracted to firm xxx').

[TEMPLATE TEXT 1] – No sub-contractor.

[TEMPLATE TEXT 2] – The following service(s) is/are subject sub- contacting

- <Name of service – see para 2. above> is sub-contracted to <Name of third party>

Sub-contracting is made in accordance with article 23 Article 5(a) of the REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000.

4. Manual / automated processing

[GUIDANCE] – Indicate if processing is manual or automated. Since personal data collection is only occasional not pro-active, processing is normally manual.

[TEMPLATE TEXT] – Automated processing (with human intervention for the incident response phase).

5. Storage

[GUIDANCE] – Indicate whether personal data is stored in a paper or digital form and where data are stored. Usually servers and backup on electronic media.

[TEMPLATE TEXT] – Servers and backup on electronic media.

6. Comments

[GUIDANCE] – Usually no additional information is required.

[TEMPLATE TEXT] – None.

PURPOSES AND LEGAL BASIS

7. Purpose

[GUIDANCE] – Indicate here the purpose of data processing in the context of IT security incident response.

[TEMPLATE TEXT] - The purpose of processing is to assist <Name of your organisation> to detect, prevent and recover from cyber-attacks.

8. Legal basis of Processing

[GUIDANCE] – Insert reference to the document, including the mandate that formally establishes your IT security incident response team. The service list of the incident response team should be established based on the ENISA catalogue (see http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/framework/service-types). The legal ground for processing personal data in the context of cyber-security incident response is usually found in article 5(a) of the EU Regulation.

[TEMPLATE TEXT] –

The IT security incident response team is formally established and mandated by <name and reference of the internal document>.
The IT security incident response team complies with <name and reference of internal decision or regulation on security for the organisation>.
For lawfulness of data processing operations, refer to Article 5(a) of the REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000.

9. Data subjects

[GUIDANCE] - Indicate categories of individuals whose personal data might be subject to processing. Be as specific as possible when describing who the data subjects are (staff members, public, etc).

[TEMPLATE TEXT] –

Data subjects are:

- 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 detected during security audit or assessments,
- Individual owners of IT assets involved in malicious traffic or activities and thereby triggering alert in an Intrusion Detection Service,
- Individuals subject to awareness, education or training actions in the field of cyber-security,
- Individuals receiving cyber-security announcements.

10. Scope of data

[GUIDANCE] – Indicate categories of personal data that might be subject to processing.

[TEMPLATE TEXT] –

Personal data subject to processing are:

- Any file (with user-id included) stored in, transmitted from / to a host involved in an incident (as victim, relay or perpetrator),
- Email addresses, phone number, role, name, organisation of individuals targeted by awareness, education, training related to cyber-security, or receiving cyber-security announcements,
- Technical data (IP address, MAC address, etc) identifying an IT asset involved in an incident, an audit or an intrusion detection alert,
- Traffic data/logged data linked to identifiable individuals containing, number called, device identification, URL, sender, destination, subject, date, time, location, application name, volume, file name, data volume.

RIGHTS OF DATA SUBJECTS

11. Information

[GUIDANCE] – Indicate where the privacy statement can be accessed by all users in your organisation. This is typically the URL to your web portal. Furthermore, when the security of personal data is at stake, the incident response team must inform the victim(s) of the existence of an incident and its potential consequences.

[TEMPLATE TEXT] – The privacy statement can be accessed at <URL>. When the incident handled by the incident response team concerns the security of personal data, the incident response team informs the victim(s) of the existence of an incident and its potential consequences.

12. Rights

[GUIDANCE] – Indicate how data subject can obtain information on the processing, how they can request an access, rectification, blocking and/or erasure of their personal data.

[TEMPLATE TEXT] – Data subject (see paragraph 9) may obtain copy of personal data by contacting <Insert your contact details for data subjects>. Data subjects have the right to request the correction, blocking or erase of their personal data, within the limits of what is technically allowed by the automatic generation and/or collection during the incident collection phase. This right may usually be exercised after the closure of the incident response.

Additionally, data subject shall have the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to Articles 13 to 16 unless this proves impossible or involves a disproportionate effort.

13. Retention

[GUIDANCE] – Indicate how long personal data might be retained.

[TEMPLATE TEXT] –

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

They are retained for 5 years after closure of the incident procedure, for security reason (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).

14. Time limit

[GUIDANCE] – Indicate the time limit for accessing their personal data by data subject. Justify any difference between the retention time and time data subjects can access their data.

[TEMPLATE TEXT] –

The time limit for data subject to access their personal data is one year after <Name of IT security incident response team> has received them.

For any request for locking or erasure of data, an answer will be sent within 15 working days from the date of reception of the request.

15. Historical purposes

[GUIDANCE] – Indicate any historical considerations related to data subjects rights. In the context of cyber-security incident response, this is usually not applicable.

[TEMPLATE TEXT] – Not applicable.

RECIPIENTS

16. Recipient(s) of the Processing

[GUIDANCE] – Indicate recipients of the processing. This includes at least your team, the (general) security incident response entity (if distinct from your team) and any other internal entity to which your team may communicate files or reports. You should however restrict to the strict minimum internal transfers of personal data.

[TEMPLATE TEXT] –

Cyber-security incident response team staff.
<Security incident response entity>
<Other internal entity(ies) receiving incident response reports>
European Data Protection Supervisor/DPO/Ombudsman, when required.
Court of Justice, Court of Auditors and national public prosecutors, when required.

17. Transfer

[GUIDANCE] – Indicate recipient of the processing outside your organisation. This should at minimum include CERT-EU. In case your organisation envisages to initiate forensic investigation with the participation of the relevant national authorities where your organisation is implanted, this should be mentioned here.

[TEMPLATE TEXT] –

Information related to cyber-security incident might be transferred to CERT-EU in case of assistance request or simple notification.
Information related to cyber-security incident might be transferred to <Name of relevant national forensic authorities> in cases where <name of your organisation> initiated forensic investigations in view of prosecution or other purposes.

SECURITY MEASURES

18. Technical and organisational measures

[GUIDANCE] – Indicate security measures taken to protect personal data. You will usually rely on security standards adopted by your organisation plus a series of appropriate IT security measures.

[TEMPLATE TEXT] –

Security measures comply with <Your organisation' security standards> for organisational, physical and IT security.

More specifically the following security measures are applied <list of specific security measures within the cyber-security incident response team>

19. Other information

None.