EDPS - IT POLICY
CASE STUDY ON DATA BREACH

12 December 2018

OVERVIEW

1. Background and description

This case study is about a data breach incident that takes place within your organization and how it has to be tackled in order to comply with the legal requirements of Articles 34 and 35 of Regulation 2018/1725.

The purpose of the exercise is to understand the life cycle of a security incident that is a personal data breach and how the different stakeholders/roles within the organization have to effectively communicate and cooperate in order to comply with the notification and communication obligations.

[Time of the exercise is ***40 minutes****: 5 minutes preparation; 30 minutes group exercise, 5 minutes wrap-up and discussion.]*

2. The incident

Your organization is running its own IT infrastructure. The information systems mainly process personal data of the personnel (150 employees). A part of it also processes health data from individuals that participate in a European research programme (total number 4250 individuals). There are regular back-ups: file server backup data are taken daily and copied to backup servers in the network. There is an Information security Officer receiving all security alerts within the organization

Incident timeline:

Day 1, 9 a.m.: A colleague calls the Information security Officer and describes a computer malfunction. His screen is displaying strange messages: it's probably some malware that is running on the machine. The colleague has to explain that he plugged in the computer a personal USB Stick and opened a file just before the incident happens.

Day 1, 9:30 a.m.: All file servers are blocked. Access is denied for all users to the file servers and back-up servers.

3. Stakeholders

ℹ *During this personal data breach incident, the following roles will have to work together to comply with the legal requirements.*

The audience will split into teams where all different roles will be assigned within each team. Each role may be taken by more than one person. In addition to the roles, participants may be observers, who will record and analyses the interaction of the other roles. Each team will have to describe the different roles and interactions that are important for the successful handling of the personal data breach incident. The following roles shall be considered:

- Responsible for the Processing (e.g. unit in charge of the operation),
- Information security officer,
- Data Protection Officer,
- IT Management,
- Communications Team,
- Management (top level).

4. Notification obligation to the EDPS

ℹ *Describe how article 34 & 35 is applied to this case. If you have to comply with the notification obligation of 72 hours to the EDPS and if so how you do it (complete or notification in phases).*

In case a notification has to be sent to the EDPS, please complete the attached Notification Form of the EDPS describing the incident.

5. Describe the impact

ℹ *List how you have been impacted by the incident and what actions you have to take*

Following a preliminary impact analysis and your above list, describe the relevant actions for each role.

6. Implementation Plan

> *Include recommendations on how you are going to meet the goals of the regulation.*

1.

2.

3.

4.

7. Timeline

> *Propose a timeline for the internal administration of the personal data breach*

TEAM NUMBER ____

Name	Title	Date

EUROPEAN DATA PROTECTION SUPERVISOR

PERSONAL DATA BREACH NOTIFICATION FORM[1]

(ARTICLE 34 OF THE REGULATION (EU) 2018/1725)

DATE:

A. TYPE OF NOTIFICATION

A.1 COMPREHENSIVE[2] ☐

A.2 IN PHASES[3]: INITIAL:☐ FOLLOW-UP[4] ☐ CONCLUSIVE[5]☐

Reference Case File[6] :

A.3 REGISTRATION NUMBER[7] OF DATA BREACH IN YOUR REGISTER:

YES ☐ REG.NO: NO☐

B. DATA CONTROLLER EUI :

B.1 NAME OF THE ORGANIZATION (EUI):

B.2 ADDRESS:

B.3 CONTACT PERSON:

B.4 TELEPHONE: B.5 EMAIL:

B.6 DATA PROTECTION OFFICER

B.7 TELEPHONE: B.8 EMAIL:

[1] All communications shall be encrypted. Therefore, when sending the form and any other attachment by email to the functional mailbox **data-breach-notification@edps.europa.eu** it shall be encrypted (zip), and the password shared with the EDPS by alternate means (by SMS or call). Please add a separate telephone number in the email where we can reach you for the password.

[2] Select when this is a complete notification.

[3] Select when this is an initial, incomplete, notification, further information to follow (Art.34(4) of the Regulation 2018/1725)

[4] This is a follow-up to initial notification

[5] This is the final information for the incident

[6] In case of a follow-up or conclusive type of notification, please indicate if available the Case File number provided by the EDPS.

[7] Art 34(6) of the Regulation 2018/1725

C. DATA PROCESSOR: (indicate if the data breach was reported by the processor)

C.1 NAME OF THE ORGANIZATION:

C.2 ADDRESS:

C.3 CONTACT PERSON:

C.4 TELEPHONE: C.5 EMAIL:

C.6 DATA PROTECTION OFFICER :

C.7 TELEPHONE: C.8 EMAIL:

D. DATA BREACH SECTION

D.1 Briefly explain the incident and how the data breach was detected:

D.2 Security criteria affected (tick one or more boxes)

I.CONFIDENTIALITY	☐	(potential) unauthorized disclosure or access
II.INTEGRITY	☐	accidental or unlawful alteration
III. AVAILABILITY	☐	accidental or unlawful destruction or loss

D.3 EXACT DATE OR PERIOD OF THE DATA BREACH:

D.4 DETECTION DATE[8]: TIME :

D.5 NOTIFICATION DATE[9]: TIME :

D.6 If more than 72 hours have passed between detection and notification, explain why you did not notify in time: Click here to enter text.

D.7 WHO WAS INFORMED/ INVOLVED IN THE INCIDENT[10]:

[8] Indicate the date when you become aware of the personal data breach.

[9] The notification date should be less than 72 hours after you become aware of the breach. If this is not the case the reasons for the delay shall be presented.

[10] Indicate the persons involved in the handling of the incident (internal and external) of the EU institution

D.8 CATEGORIES OF PERSONAL DATA AFFECTED[11]

D.9 APPROXIMATE NUMBER OF PERSONAL DATA AFFECTED:

Please Specify the exact number if possible:

D.10 CATEGORIES OF PERSONS AFFECTED[12]:

D.11 APPROXIMATE NUMBER OF PERSONS AFFECTED:

D.12 LIKELY or ACTUAL CONCEQUENCES OF THE DATA BREACH FOR THE DATA SUBJECTS:

D.13 ESTIMATION OF THE RISK TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS:

RISK □ HIGH RISK□

D.14 Briefly explain how the assessment of the risk to the rights and freedoms of natural persons was done.

D.15 Have you informed the persons affected about the breach? YES[13] □ if yes, WHEN:

NO□, If no, explain why not (yet)

D.16 ACTION MEASURES TO ADDRESS THE RISK AND TO LIMIT ITS IMPACT[14]:

D.17 LAUNCH OF A FORMAL SECURITY INCIDENT PROCESS: YES □ NO□ if no, motivate why not:

D.18 ROOT CAUSE OF THE DATA BREACH[15]:

[11] List all elements/fields of data that were compromised e.g. first and last names, date of birth, financial data, health data, etc.

[12] List all the categories of the data subjects affected, e.g. EU staff, , MEPs, European citizens, children, vulnerable groups such as handicapped people etc.

[13] If yes, attach a copy of the communication sent to the data subject

[14] List of security and mitigation measures to address the risk e.g. data was encrypted, redundant system allowed the organisation to have an access to the data for business continuity purposes. .

[15] Explain the root cause of the security incident that lead to the data breach.