# EDPS - IT POLICY
# CASE STUDY ON DATA BREACH

**17 May 2019**

## OVERVIEW

### 1. Background and description

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

*The purpose of the exercise is to signal and discuss some of the most difficult and controversial points related to personal data breaches, the way they are notified and best practices to mitigate the impact on data subject's privacy and prevent the breach from happening again.*

*The audience will split into teams of 4-6 people to discuss the topics that the case study will present.*

*[Time of the exercise is **60 minutes**: 3 blocks, each consisting of 5 minutes preparation; 10 minutes group exercise, 5 minutes for discussion.]*

### 2. First incident - initial stage

*Your institution is organizing a big conference. The conference is composed of panels, workshops and talks, some of these events will be held in rooms with very limited seats so booking a seat for these agenda items will be mandatory. The event also has a social part that includes lunches and dinners.*

*You decide to contract an external company to develop an app and a web service that will be used by attendees and speakers to manage the registration for the conference, seat reservation for certain events, the side events organized by other organizations and the social events (lunch & dinner).*

*Your institution has several users with a role that allows them to access and manage the data of any attendees. The technical support of the app is managed by the external company that has access to the data for those support tasks and, if necessary, for administrative tasks (e.g. massive data updates). The data is hosted in a server controlled by your institution, to which*

*the external company is granted access. Only the data related to the event is hosted in that server. Daily backups are stored on a different server.*

*The event registration is going really well, and you have collected the personal data of more than 500 attendees.*

*Incident timeline:*

1. *Friday 9:00. Two weeks before the conference, the external company starts receiving emails on the app support mailbox. The app is opening on their devices, but returns an error message when users try to log in.*
2. *Friday 10:00. The external company support team checks the access to the server where registered user's data is stored. The access is slow but works. The support team sends an email to the official in your institution who helped them design the app, but he/she is out of the office on mission. Meanwhile they continue testing the app and the database.*
3. *Friday 12:30. The support team end up calling the general help desk of your institution and they finally get in touch with the system administrator of your institution's IT Unit.*
4. *Friday 13:00. The system administrator concludes that the system is slow because the hard disc is almost full when it shouldn't be. The system administrator calls your organization's Local Information Security Officer (LISO) and the rest of the incident response team.*
5. *Friday 13:45. The incident response team finds an unexpected file causing the disk to be almost full and the system to be so slow that registered users can't access their data.*
6. *Friday 16:00. The incident response team checks the backup database and verifies that it has not lost any records. Afterwards they stop the affected server and switch it for a new server where the last database backup is restored. The app and the web service are both up and running.*

## 3. Questions and answers related to the first stage

### *a) Do article 34 & 35 of the Regulation apply to this situation?*

Registered users are not able to access the personal data in their accounts but, at this stage, it is unclear if there is a risk for the rights and freedoms of the data subjects. The nature and consequences of the big file are still unknown and no test have been done on the integrity of the database.

It is necessary to obtain further information before performing a data breach notification (DBN).

**b) *How is the personal data affected?***

The available information shows a lack of availability, but we can't discard that there is an issue with the confidentiality or the integrity of the personal data.

**c) *Are all the necessary stakeholders involved?***

The DPO and the data controller (business owner) are missing.

Since the moment that the incident response team has high certainty that personal data are affected, the DP should be notified of the incident. The person in charge of the Unit declared as data controller should also be involved.

**d) *What would be your risk assessment at this point?***

Elements to consider: Sensitivity and volume of data, categories of data subjects, context of the breach.

The types of data affected are name, surname, address and contact data and the events the attendees plan to assist to. The number of affected data subjects (those who tried to access their data and couldn't) is currently unknown, but the worst case scenario is 500.

The operational consequence of the incident is that registered attendees that tried to access their data couldn't do it for 7 hours, but that period is two weeks before the conference so there is plenty for any data subject to access or modify their data as needed before the conference.

According to this elements, there is no meaningful risk to the rights and freedoms of the data subjects.

**e) *What should the following steps be?***

- Incident response team to involve on time the DPO and the data controller as soon as possible
- DPO to coordinate the conduct of a risk assessment with the currently available data, by involving members of the incident response team and other competent persons as appropriate
- Notify the DPO and data controller
- Conduct a risk assessment with the currently available data

- Register the personal data breach
- Incident response team to continue with the investigation, e.g. by conducting a forensic analysis of the file and the server.
- LISO (with the proper advice from in the DPO) to continue the incident handling in order to conclude to an official incident report with the root cause of the incident, the impact, the mitigating actions that were taken, the residual risks, the proposed corrective actions with a time plan and action owners.

***f) Would you send a DBN to the EDPS? If so, when?***

According to our risk assessment, there is no meaningful risk to the rights and freedoms of the data subjects, so the incident should be included in the data controller personal data breach register but not notified to the EDPS.

However, the more than 3-hour gap leads to questions on the way the information on the incident is handled.

- Once the support team knows about the incident, why they didn't notify the controller?
- Which contact data were provided to the processor? Review the contact data provided in the contract, DPA or elsewhere.
- Why no one did contact the DPO or the data controller?

## 4. First incident - second stage

*Incident timeline:*

7. *Monday 9:45. The incident response team analyzes the big file to find out that it is a database dump file, a binary file containing a full copy of the database with the personal data of the conference attendees.*
8. *Monday 10:30. The incident response team concludes that an unknown third party has copied the data of all registered attendees to the file and transmitted it to external servers.*
9. *Monday 11:45. The DPO reviews all the data available and notices that, against his recommendation, the database stored health data (allergies) of 50 of the attendees that registered for the social events. Furthermore,*

*some of the attendees are VIPs in their respective fields. At least, the passwords were hashed[1] before storing them.*

10. *Monday 15:00. The incident response team concludes that the unauthorized third party took advantage of an unpatched vulnerability to access the server containing the data. The institution informs the police about the incident.*

.

## 5. Questions and answers related to the second stage

***g) With the current information, how is the personal data affected?***

The data breach affects now the confidentiality of the data.

Health data of 50 data subjects have been disclosed. Some of the just attendees, especially the VIPs, will feel their right to privacy may be strongly affected because their assistance to the conference will be known to third parties. Moreover, while some attendees provided their professional address and contact data for the registration, some others provided their private address and contact data.

To make sure that the integrity of the data has not been affected, it will be necessary to ascertain that the backup server was not hacked. This should be supported with evidence.

***h) What would your risk assessment be at this point?***

The nature of the breach has changed. It's not only the lack of availability for 7 hours, but also a confidentiality breach.

The types of data affected include now the health data of 50 attendees.

The number of affected data subjects is now clearly 500.

We have no knowledge of who accessed those data, for what purposes or if the data are going to be transmitted to another third parties.

For the first 50 cases at least, it is sure that the risk is high. In any case the high number of affected individuals is also significant for the risk assessment. Consequently, the risk for data subjects is considered high.

***i) Would you send a DBN to the EDPS? If so, when?***

[1] not in clear text.

Of course. The nature of the incident and the impact on data subjects has dramatically changed.

We now have more information on the breach, but it is still the same breach. The institution was made aware of it by Friday 12:30. Therefore, the data breach notification should be sent before Monday 12:30, two hours after the institution is aware of the hacking.

***j) Would you inform the data subjects? Which ones?***

You should inform all data subjects.

Even if the passwords were hashed, it is possible that some users chose easy to remember passwords that could be guessed by a dictionary attack. Therefore, you should decide to notify all attendees and also propose them to change their passwords.

***k) Which mitigation measures would you apply?***

To prevent the impersonation of attendees in the conference web service and app, you could reset the passwords to force all users to change them or following the previous statement to send them a link for changing their password. Both proposals are good.

Since many users tend to reuse passwords, a successful attack on the stolen password data could allow to impersonate data subjects on different web services and apps. The data breach notification should make aware the data subjects of this fact and recommend them to change the password in any other web service where it was used.

***l) Which preventive measures would you apply?***

In the context of the lessons learned topic (proposed corrective actions) of the incident handling you could for example:

1. Update your policies and procedures in handling security incidents in order to make sure that the DPO and the data controller are timely involved when personal data are affected.
2. Include in your incident handling process information on whom and how to contact, preferably by phone and functional mailboxes according to the urgency.
3. Review business continuity policies and procedures, to ensure that incident response is timely.

4. Include in the security training, data protection incidents simulations. Request the processor to organize data protection awareness raising activities.
5. Review your access control policy and in particular the password complexity. Make sure also that best practices are enforced in password management. Salt the hashed passwords so they are not vulnerable to a dictionary attack.
6. Review technical vulnerability management policies and procedures in order to minimize the risk of system compromise because of vulnerable systems.
7. Contact CERT-EU to plan and conduct a vulnerability assessment of our servers. For those systems whose DPIA show that there is a high risk for data subjects, consider conducting a penetration testing.

## 6. Second incident

*Your institution contracted with five IT consultancy firms the services of a number of contractors, experts in different IT and project management fields. Your institution pays the providers a daily fee for each expert that depends on their professional category.*

*Once a month your procurement unit sends an email to each provider with a file containing personal data of the contractors working in your institution (name, surname, professional category and data of the contractors' presence on your premises). The data are sent in an attached unencrypted Excel file.*

*Incident timeline:*

1. *Tuesday 10:30. An email with an Excel file containing data of 10 experts is sent by mistake to the email of the five service providers.*
2. *Tuesday 10:35. The service provider whose contractor's data where sent, contacts the sender and informs them of the mistake.*
3. *Tuesday 10:37. The sender tries to recall the email.*
4. *Tuesday 10:50. Two of the emails are successfully recalled, while the other three (the intended recipient and two other providers) recall attempts fail.*

5. *Tuesday 10:55. The sender informs his Head of Unit, who immediately informs the LISO and the DPO.*

6. *Tuesday 12:00. The institution decides to play on the safe side and notifies the data subjects sending them the following email from the procurement functional mailbox:*

   *Dear colleagues,*

   *We regret to inform you that an email containing personal data regarding your work as contractor in this institution was sent this morning to unintended recipients due to a human error.*

   *We have successfully recalled two of the emails and are taking steps to recover the pending two.*

   *We will keep you updated.*

   *Best regards,*

   *The procurement team*

## 7. Questions and answers related to the second stage

***m) Which mitigation measures would you apply?***

Send a new email to the pending recipients requesting them to delete the previous email and reply to this email confirming the deletion of the previous one.

***n) Would you send a DBN to the EDPS? If so, when?***

By 10:55 the institution has knowledge of the data breach, so it could be notified. It is understandable if the institution wants to include in the notification the results of any mitigation measures, but that does not justify a late notification.

***o) What is your risk assessment?***

From a quantitative perspective the data disclosed concerns 10 data subjects.

From a qualitative perspective the data disclosed contains no special categories of data.

The context is in this case the determining factor.

If the recipient of the data would have been a third-party with no interest at all in the data and they have confirmed the deletion of the emails, it wouldn't be necessary to notify the EDPS, although the data breach should be registered by the institution.

In this case the recipients of the data are IT consultancy firms who compete for the experts they could hire. The affected experts could have worked in the past or could work in the future for any of the recipients. Consequently, the impact on their privacy is greater. It is for this reason that the data breach should be notified to the EDPS.

***p) Do you think the notification to the data subject complies with the Regulation?***

No, it does not.

The notification does not contain the name a contact data of the DPO.

By not specifying the type data disclosed and the nature of the recipients of those data, the affected data subjects are not informed of the likely consequences of the breach (e.g. it is possible that a former employer gains knowledge that you now work for a specific competitor).

***q) Which preventive measures that would you apply?***

Review your user acceptable use policy and relevant procedures and training in order to make sure that information is protected when sent over untrusted channels. For example, when sending personal data to recipients external to the Institution, always send them encrypted. If symmetric encryption (shared secret) is used, the encryption key should be exchanged by a different means (e.g. SMS or telephone call).

Avoid using email to exchange personal data. Assess alternatives like developing a tailored solution or search for a commercial solution that allows you to ensure that data are delivered to the correct recipients. An information exchange policy and procedures would be the best practice in order to identify the exchange categories and the appropriate procedures and means.