EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

[redacted]

Technology & Privacy Unit (EDPS)

Online talk: EDPS - Personal Data Breaches in EU Institutions : examples of common data breaches

17 May 2022

Goal of this Online Talk

OnLine Talk Outline

- Introduction to personal data breaches and the legal obligations
- Elements to consider when assessing a personal data breach
- Statistics on personal data breach notifications
- Examples of personal data breaches (analysis)
- How to avoid personal data beaches – common mistakes
- Questions and Answers

Introduction to personal data breaches (and the legal obligations)

Definitions

personal data:

"any information relating to an identified or identifiable natural person"

personal data breach:

*"a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

Types of personal data breaches

Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data, which is about getting knowledge of personal data by an entity not entitled to this knowledge

Integrity breach – where there is an unauthorised or accidental alteration of personal data, which is about inappropriate modifications of personal data.

Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which is about losing control of access to personal data, or inappropriate deletion of personal data, and

A personal breach could be any combination of the above types.

Legal Obligations Art 34-35 REG(EU) 2018/1725

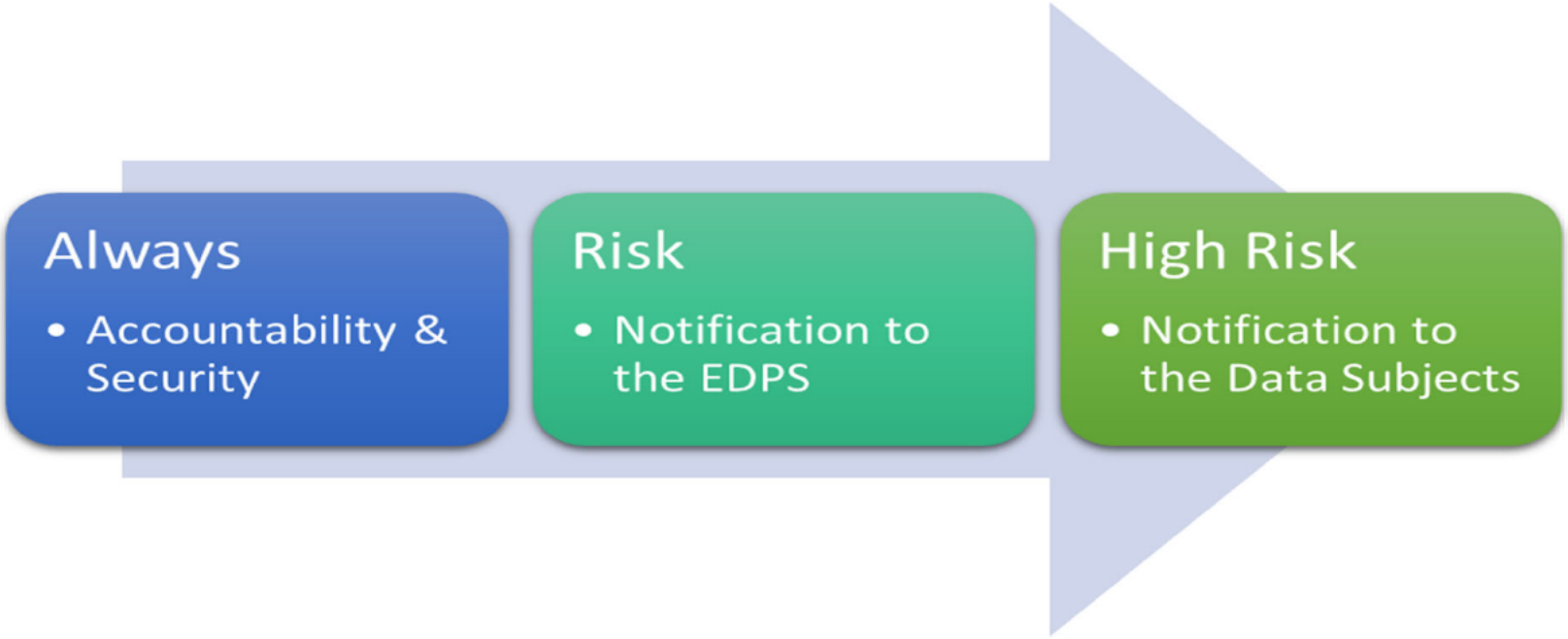
The data controller should be able to identify a personal data breach and assess its impact as to the risks to the rights and freedoms of the data subjects.

The data controller must notify the breach to the European Data Protection Supervisor without undue delay, not later than **72 hours** after becoming aware of it (unless it is unlikely to result in a risk to the rights and freedoms of natural persons)

The data controller must communicate the breach to the data subject without undue delay in case that it is likely to result in a high risk to the rights and freedoms of them

The data controller must document all personal data breaches internally (UPDATED REGISTRY!)

Accountability



Assessing the Risk - Criteria

When assessing a personal data breach you need to think of **the fundamental rights of the individuals** and assess the risks to them.

What type of breach? Specific context

What data?

- Nature of personal data
- Special categories of personal data? Sensitivity
- Special categories of individuals (e.g. children or other vulnerable individuals)

Volume of data

- How many data subjects?
- How much data?

Mitigating measures?

- Was the data encrypted?
- Pseudonymized?

Which freedoms and rights are affected?

High-Risk indicators

Categories of data:

- special categories of data
- ids/passports
- manual signatures
- unencrypted passwords to access staff accounts or systems (emails, etc)

Sensitive context:

- performance appraisals at work
- recruitment process
- political context (e.g. usernames in a political party's website).

How to notify the EDPS?

You can report a personal data breach by filling in the online form on the EDPS website: https://edps.europa.eu/form/personal-data-breach-notificatio_en

You can also report by downloading a specific form and sending it to the following email address: [redacted]

All communication must be **encrypted**.
When sending an email about a personal data breach to the EDPS data breach notification email address, any attachments must be encrypted (zip) and the password shared with the EDPS by alternate means (by text message or telephone call).

Guidelines

EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification

https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

EDPS Guidelines on Personal Data Breach Notification

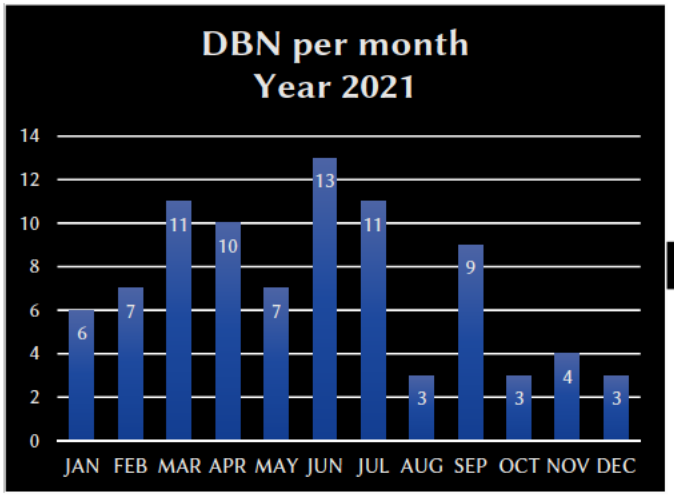
Under Revision

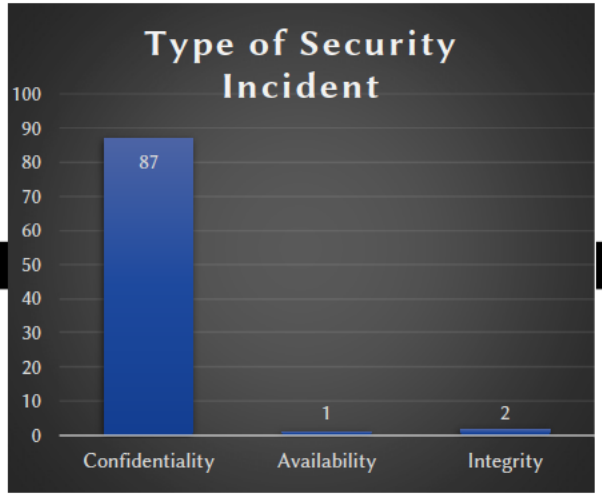
EDPS will be more resolute on notification, supervision and enforcement

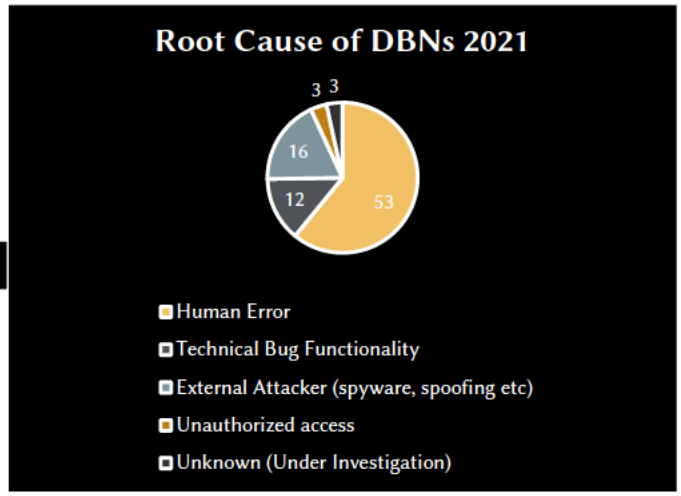
e.g. recurrent or serious omissions in the personal data breach handling, negligence from an EUI to implement security measures following our specific recommendations on previous cases that the same EUI had.

Statistics on Personal Data breach Notifications

Data breach notifications in 2021







Total Number of Received Notifications in 2021: 87

Examples of personal data breaches (analysis)*

*not real cases, inspired from real data breach notifications

Mispostal

Mispostal

- **Send an email/postal mail containing personal data to a wrong recipient**
- **Send an email/postal mail with an attachment containing another person's data**
  (common in HR and Medical services, but also in recruitment cases when members of the committee mistakenly send their evaluations to applicants)

- **Send an email by putting all recipients in cc**
  (common in newsletters, invitations to events, with external attendees, recruitment processes revealing all applicants).

Mispostal Example – Recruitment process

Due to Covid-19, an EUI held an online, remote recruitment process for a position. Interviews and exam were foreseen.
On the day of the exam, the assistant of the selection committee sent the topics for the exam to all 10 applicants simultaneously. Some applicants contacted the assistant and said they did not receive the topics. The assistant sent an email to all applicants asking them to confirm they well received the topics (this time due to urgency, all applicants in cc).

Analysis:

- Other applicants became aware of the contact details (usually containing the names) of the other applicants.
- Risk of misusing this information and even for some applicants to have their candidature revealed to their current employers.
- No high risk, but sensitive context.

The assistant should directly recall the message and ask everyone to confirm they deleted received information. Advice to inform the data subjects for transparency.

Mispostal Example – Covid-19 contact tracing

A staff member from an EUI contracted Covid-19. As he had been to the office, he informed with an email the crisis management team of the institution and copied in 6 people he had been in contact.
The crisis management team continued contact tracing, identified 10 employees as secondary contacts and informed them to self-quarantine. However, this notification was done by forwarding the original email of the staff member.

[redacted]

Analysis:

- The fact that this staff member contracted the virus was revealed to these employees (health data).
- The contacts of this person were revealed to the secondary contacts.
- Risk of misusing this information and risk of discriminating behaviour towards the staff member.
- High risk as health data are revealed.

The crisis management team should directly recall the message and ask everyone to confirm deletion of the erroneously received information. The first 7 people (at least) should be notified of the data breach.

Mispostal – how to avoid/mitigate

- **Awareness training**

- **Adopt email policies:**
  - **when sensitive or confidential data, encrypt the attachment**
  - **attention to group email addresses (they may contain recipients who must not receive the content)**

- **Use technology:**
  - **Automate the process with a system sending a link to the document (user has to authenticate)**
  - **use outlook alerts (similar to out of office indications, when too many recipients in cc)**

- **Revisit all processes to ensure steps of manual postal are adequately described.**
- **Ensure that system generated email invitations are sent with recipients in bcc (set it as a requirement to your contractors)**

Recall message and/or confirm deletion of erroneously received information.

Transparency

Transparency errors

- **Publish a list of beneficiaries for financial transparency, containing more data than necessary or without a legal basis**
- **Access to documents requests - by not removing personal data** from released documents or by revealing the identity of the person requesting access
- **Publish the list of participants to an event without their consent**
- Apply **non reversible removal/anonymization** on released documents

Transparency Example – Access2documents

An EUI received an access to documents request. The EUI staff member dealing with the request replied to the applicant by email and then proceeded to upload the documents to the public registry of requests. However, the requested documents also included a presentation from a training session and the name of the trainer was not removed. The trainer was coming from a sensitive function in a Member State and did not wish his position to be publicly available.

Analysis:

- The name and position of the trainer was made public.
- Risk of receiving unsolicited communications and risks related to being employed in this sensitive function.
- High risk

The EUI staff member should quickly inform the website's administrators to remove the document and upload a new one without the trainer's data. Also, ask the applicant to delete the received information. The trainer should also be informed of the data breach.

Transparency Example – Financial transparency

An EUI published on its website information on selected beneficiaries for a research financing program. The information published included the beneficiaries' names, origin, but also contact details.
Also, the names of all other applicants were published for transparency (it seems there was a legal basis).

Analysis:

- Contact details data of the beneficiaries (and applicants) were published, instead of just their names.
- Risk of receiving spam emails.
- No high risk

The EUI should quickly withdraw the data from the internet and upload a version where these are removed. Also, the EUI should check the legal basis of publishing information on runners up. In any case, only the necessary data should be published.

Transparency errors – how to avoid/mitigate

- **Raise awareness** to employees to **validate the legal basis**, before publishing any information.
- **Revisit the processes of transparency to ensure data minimization is clearly described as a step.** Examples of accepted categories should be included.
- **Revisit the processes of events organization** to ensure the list of attendants is not made known. If data need to be revealed (to other attendants or publicly), **ensure data protection notices inform them accordingly and ask for consent when necessary.**
- **Revisit access2documents processes** to ensure personal data removal is described as a step. Clearly describe examples of such data.
- **Clear internal guidelines on removal/anonymization techniques** (which and how to apply them)

Remove the public documents as soon as possible and replace with the anonymized ones.

Technical Errors

Technical errors

- Technical errors of a system:
  - **Information being automatically emailed to wrong recipients**
  - **Access allowed to documents the user should not be able to access**
- Misconfiguration of user roles (also human error)

Technical error – software upgrade

After a software upgrade in an EUI's online recruitment system, a user could access the profile of another applicant and edit any of their data.

Analysis:

- Personal data from the other applicant's CV were available to the user. He could edit or withdraw the application of the other user. At the same time, the user was not able to access their own application. He immediately informed the controller of the error.
- Risk of misusing this information, including revealing the candidature to the other applicants' current employer. Risk of not being able to submit their own application for the post.
- No high risk, but sensitive context. (If they had edited the other users' application, then high risk.)

The EUI should directly investigate the source of this error and apply any necessary fixes. The EUI should also inform the other applicant of the breach and ensure both applicants have the chance to correct and submit their applications. In addition, investigate whether there are similar cases.

Technical error – misconfiguration

Due to misconfiguration of access rights in the folders of a file server, all staff members of an EUI could access HR folders, containing personal data of other employees, such as family composition, payrolls, special leaves and appraisals.

Analysis:

- Personal data for other staff members, including special categories such as health data, were accessible to all staff.
- Risk of misusing this information.
- High risk

The EUI should directly stop the unauthorised access to these folders, inform the data subjects of the error and investigate from the logs which such data were actually accessed. If all people who accessed the data confirm they did not copy or use them and if they are bound by confidentiality obligation, then the assessment can result in risk instead of high risk (if not on the same team/career path).

Technical errors – how to avoid/mitigate

- **Thorough testing for new systems or new functionalities**
- **Regression testing to verify that the changes from a new release did not impact the existing functionality**
- **Robust authorisation processes for the assignment of roles.**
  - Avoid manual assignment of roles
  - Use automated workflows where 4 eyes have approved and assignment of the role is done automatically.

Take the system offline to investigate and apply patches as soon as possible. Logs are important.

External attacks

External attacks

- Ransomware (encrypting data on the device and other connected devices to the network)
- Malware (e.g. capturing keystrokes, sending information from emails)
- Access to a testing environment with less security measures
- Taking advantage of vulnerabilities to software or devices (enter a system or the whole network)
- Phishing attacks

External attack – revealed passwords

An external attacker gained access to email addresses, ids and passwords belonging to the users of a system (accessible via internet), by taking advantage of a vulnerability of the system. The system was unpatched.

Analysis:

- The id, password, contact details and the content the users had access to was accessible by the attackers.
- Risk of external attackers having accessed the information available to the users, including more personal data.
- Risk of use of the contact details in combination with revealed information to send targeted phishing emails.
- Risk of accessing other online services of the users, if they had used the same password.
- High Risk

The EUI should inform data subjects of the data breach and potential risks. Then, take the system offline, patch, apply changes to ensure any passwords are stored in encrypted form and enforce password change once the system is again online.

External attack – Malware

A staff member has opened an attachment or clicked a link in a malicious message, while the antivirus failed to detect anything malicious. The malware copied both the emails and the contacts of the staff members' email account and used them in spam messages to further spread the malware.

Analysis:

- The contacts and the content of the user emails was accessed by the malware.
- Risk of exfiltration and misuse of personal data included in the users' mailboxes, as well as further misuse of contacts' information.
- High Risk

Apart from other security incident response actions, the EUI should inform the user and their contacts of the incident and its risks. The EUI should further investigate whether other personal data were accessed by the attacker (stored on the device or other resources on the network) and assess risks to data subjects.

External attack – Obsolete server (personal data)

An external attacker accessed an old file server that was used by HR services before the HR system was launched and accessed a folder containing personal data of 100 staff members from previous years.

Analysis:

- Personal data of current and former staff members, including names, birthdates, bank accounts, identification documents and contact details were accessed by the external attacker.
- Risk of misuse of these information.
- High Risk

The EUI should take the old file server offline and delete documents containing personal data. They should also launch an investigation to see if similar attacks applied to other resources connected to their network. Data subjects should immediately be informed.

External attacks– how to avoid/mitigate

- Have a patching process and thoroughly follow it.
- Do not use unsupported operational systems or software.
- Ensure testing is not done with real data.
- Ensure data are deleted from retired systems.
- Ensure contractors' devices are secure (if they gain access to your network).
- Monitor network traffic (to identify unusual traffic from devices).
- Encrypt stored passwords.
- Raise users' awareness.

Ensure you inform users and enforce change of their passwords.
Security incident response team in close collaboration with the DPO.
Do not stay in the obvious (e.g. ransomware encrypting), investigate if other actions have taken place (e.g. exfiltration).
Do not wait to finish the forensic investigation to notify the EDPS, if there are indications.

Unauthorised access

Unauthorised access

- **Misuse of access privileges** a user may have, to access information they do not need to access, regardless if they will use them afterwards.

Unauthorised access– Privileged access rights misuse

An IT support officer used maliciously his privileged access rights to access files, including pictures and information on personal online purchases, stored on corporate devices of other staff members.
No ticket had been submitted concerning problems on these devices.
This was discovered by the security team.

Analysis:

- Personal data, including online purchases, personal address and family members' photos were accessed by the IT support officer.
- Risk of misuse of accessed information.
- Potential high risk

The EUI, as soon as they discovered the incident, should remove elevated access privileges from the user and start an investigation to see if he had accessed other information without a reason. Disciplinary actions may apply. Also, the data subjects should be informed.

Unauthorised access– how to avoid/mitigate

- **Strict policies on accessing information on a need to know basis.**
- **Awareness and monitoring.**
- **Special attention should be given to contractors of IT support (contractual clauses and monitoring).**

Remove access privileges and investigate.

Other cases

Account credentials found on the internet

The security team of an EUI received information that 10 user account credentials from one of their systems were found in a database published on a website. The system's functionality allowed users to select topics for receipt of email newsletters.

Analysis:

- The email address and newsletter preferences were accessible to whoever could access the account.
- Risk of user credentials to be used to access information from the user account.
- Risk of accessing other online services of the users, if they had used the same password.
- High risk

The EUI should investigate the issue to see if this was a result of an attack to their systems. Even if no indications of attack were evident, they should enforce immediately password changes for all accounts on the system.
They should also inform the data subjects of the incident and the risks and provide security advice for their devices.

Corporate devices sold online

An EUI was informed by a person who bought a laptop online, that the EUI's logo appeared as soon as they turned it on and asked for a password to access it. As it turned out, this device was returned to a contractor who did not follow the deletion procedures.
The device was encrypted and the EUI had a policy to store information on dedicated network drives instead of the device's hard disk.

Analysis:

- No personal data were accessed by third parties. Even if after some time the receiver could decrypt the device, the risk of having access to personal data would be low.
- Unlikely to result in a risk for the data subjects.

As soon as the EUI ensured the data breach was unlikely to result in a risk, they should launch another investigation to see if other devices were sold. They also should contact the contractor to investigate the root cause of this action. The data breach should be documented to the data breach registry of the controller.

How to avoid personal data breaches

Organization and preparation

Data Protection by design

- Data minimization to all processes
- Apply security measures (from the design)
- Data retention mechanisms

Strong security management system

Personal data breach handling

- Clear processes and reporting lines
- Manuals with mitigation actions to quickly apply
- Awareness trainings to staff members

Common mistakes causing data breaches (1/2)

Processes description

- Not updated processes to ensure legal basis is checked and to hint steps where errors could be made.
- Data minimization not applied.

Email use

- Non existence of policies for correct use of emails (avoid cc, add links to a system).
- No automation of processes whenever possible.

Covid-19

- Make services available via internet without additional safeguards.
- Deviation from standard procedures.
- Users not reminded of risks related to spam attacks.

Mapping of personal data

- Not obvious processes/systems involving personal data.
- No adequate measures applied, data retention policies not applied.
- Obsolete applications and servers left in the network.

Common mistakes causing data breaches (2/2)

Testing

- Testing with real data.
- Contractors given datasets of real data.

Security management

- Patching policies not thoroughly applied.
- Unsupported systems.
- Non active review of logs.
- Not using multi-factor authentication.

Lack of training and awareness

- Similar human errors in the same organization.

Questions

?

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

@EU_EDPS

European Data Protection Supervisor

EDPS