EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

[redacted]

Technology & Privacy Unit (EDPS)

Data protection in your daily tasks: how to effectively handle your duties as controller and **how to deal with a personal data breach?**

05 December 2022

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

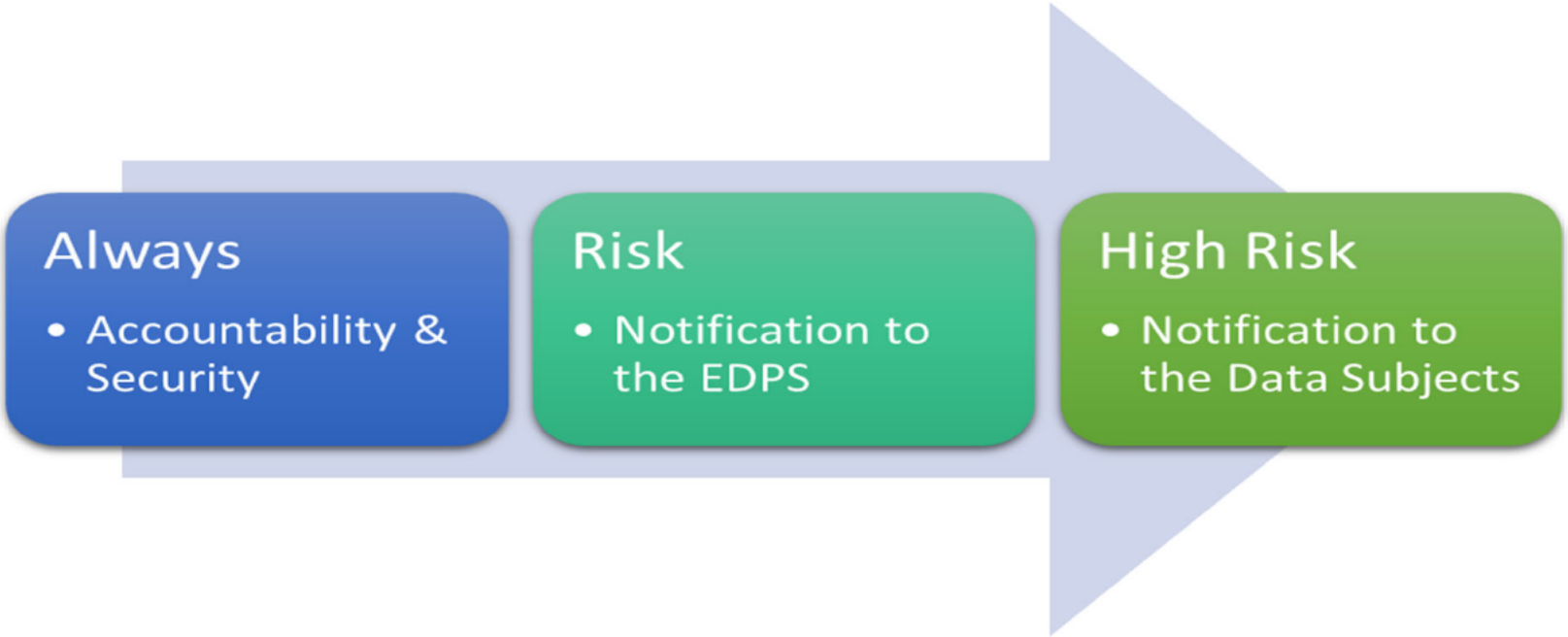
The data controller should be able to identify a personal data breach and assess its impact as to the risks to the rights and freedoms of the data subjects.

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 9/2022 on personal data breach notification under GDPR

https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

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

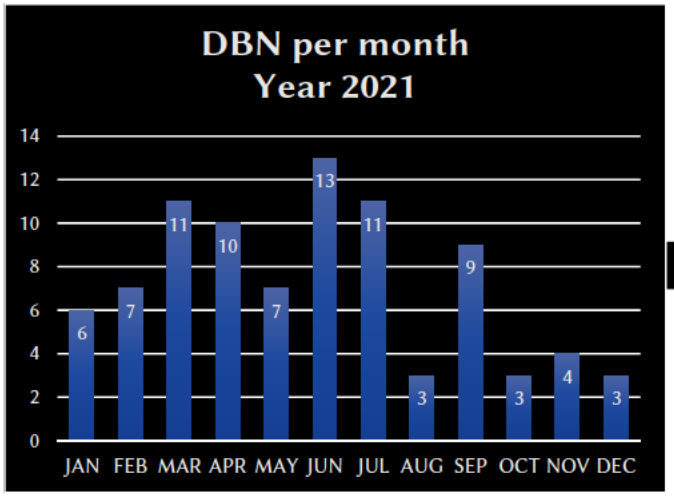
EDPS will be more resolute on notification, supervision and enforcement

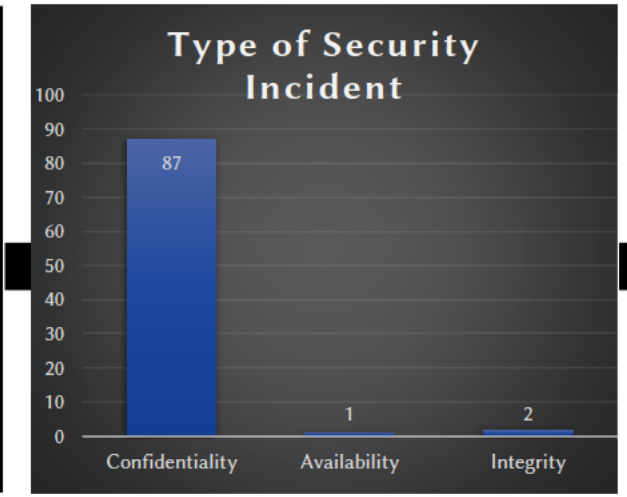
assign resources: 1 full time assistant

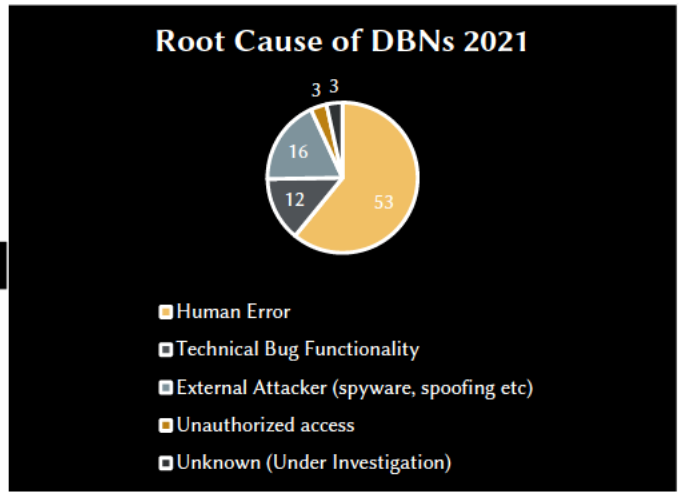
e.g. recurrent or serious omissions in the personal data breach handling,
negligence from an EUI to implement security measures following our specific recommendations on previous cases that the same EUI had.

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 – Trusted recipient

A staff member responsible for organising a press conference, wished to send the selected menu for the catering to the staff member tasked with the procurement of such services. However, the sender selected a wrong file and instead attached to the sent email the list of attendants to the event and their contact details. The recipient informed about the error and confirmed the deletion and not further use of the file.

Analysis:

- The other staff member became aware of the contact details (names, position, telephone numbers and email addresses) of the people attending the event.
- Risk of misusing or revealing to others this information (spam, etc). However the recipient confirmed deletion and not further dissemination of the file. The staff member is under obligation of confidentiality.
- Unlikely risk.

The assistant should directly recall the message, ask the recipient to confirm they deleted received information and remind them of their confidentiality obligation.

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 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 system for events organisation, a user could access the profile of another applicant and edit any of their data. The system was used to declare group members for accreditation to visit the EUI's premises. 1 user per group would be allowed to enter the names and emails of a group of up to 50 visitors and they would receive via email the badges to enter the premises.

Analysis:

- Personal data from the other applicant's inserted data, including names and birthdates of a group of visitors to the EUI were available to the user. He could edit or withdraw the application for the visit, as if he was the other user. At the same time, the user was not able to access their own application for a group visit. He immediately informed the controller of the error.
- Risk of misusing this information, including using the email addresses of the other visitors to send them spam messages and promote other tours. Risk of not being able to submit their own application for the visit.
- No 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 – unclear requirements

An EUI has an online system for the accreditation of journalists, in order to receive invitations to press conferences. In the first use of the system, invitations for an online event were sent out to a list of 100 journalists. However, their email addresses were put in cc instead of bcc. The controller understood the mistake when one of the recipients complained.

Analysis:

- Email addresses of a list of journalists were available to all other participants. Such information would not be acceptable as the journalists had not consented to such a publication.
- Risk of misusing this information, including using the email addresses to send spam messages or to understand that a journalist is following a specific topic.
- No high risk.

The EUI should directly investigate the source of this error and apply any necessary fixes. The EUI should also inform the recipients of the error and ask them to delete the invitation and not further use or disseminate the list of emails. A new invitation should be sent with the recipients in bcc.

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 – 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 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.

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 and ongoing telework

- 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