
**EUROPEAN DATA PROTECTION SUPERVISOR**

The EU's independent data protection authority

KONSTANTINA VEMOU
Technology & Privacy Unit (EDPS)

Elena TELLADO VÁZQUEZ
Deputy DPO (EASA)

# REVISION OF THE EDPS GUIDELINES ON PERSONAL DATA BREACHES

## Workshop - 49th meeting EDPS/DPOs

04 June 2021

# Goal of this workshop

# Workshop Outline

- Inclusion: Get to know each other
- EDPS Experience from personal data breach notifications
- Data breach notification Guidelines Update
- Discussion
- Feedback on the notification handling process
- Discussion
- Next Steps

# Inclusion:
# Get to know each other

# EDPS Experience from personal data breach notifications

# EDPS experience from personal data breach notifications

Differences in the way EUIs handle and notify personal data breaches.

- time to report
- information provided in the notification form
- maturity of assessment
- actions to mitigate the risk to the data subject

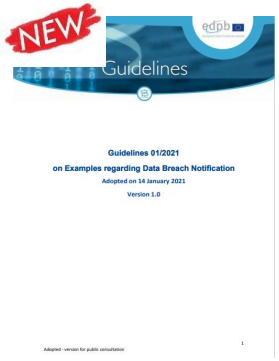
Some EUIs have never submitted DBNs

Questions on assessment (e.g. unlikely to result in risk)
Identified errors on the assessment of the risk to the data subjects (Risk/High Risk)

DPO relation with the Information security officer and IT management

Processor's reaction to personal data breaches

# News on guidelines and supervision practices

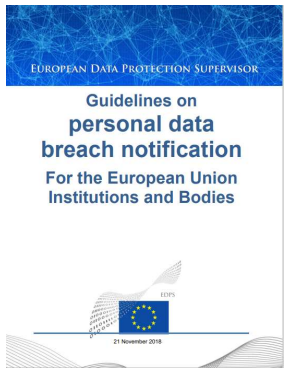



**EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification**

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_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.

# EDPS Guidelines on Personal Data Breach Notification: Update

# Guidelines on Personal Data Breach Notification: Update (1/4)

**Scope of EDPS updated guidelines**

- All Union institutions, offices, bodies and agencies
- Operational data processing operations

**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).

**Elements to include in the notification**

- explanation of the system or the process in 1-2 lines.
- description of the equipment compromised during an external attack
- source of the data breach

# Guidelines on Personal Data Breach Notification: Update (2/4)

**When to *not* notify?**

Threshold of "unlikely to result in a risk to the rights and freedoms of natural persons".

- Elements that may contribute to unlikely risk:
  - **public information**,
  - **trusted recipient**, e.g. contractually bound to confidentiality
  - **security measures** that make access to the personal data extremely difficult
  - **time period of unavailability** of personal data in relation to the provided service and effect to the individuals rights
  - other mitigating measures such as successful recall of an erroneously sent email.

- Always in relation to the **context**.

- In any case you always need to **document the data breach to your registry** along with any relevant information, e.g. the assessment and taken measures. (must be accessible to EDPS on demand)

# Guidelines on Personal Data Breach Notification: Update (3/4)

**Should you notify when you are not sure?**

Cases in which the controller is not yet sure of the data breach, but there high indications of one. Usually in cases of external attacks, but also in cases of technical errors.

- Important **asset related to user management and authentication** is breached (e.g. domain controller)
- A system containing a **large amount of personal data** is breached.
- A system containing **special categories of data** is breached.
- If you have **indications that personal data were copied**, do not wait to see if the copies were extracted.
- If **you do not have log data** for all the period the data breach has taken place.
- If **data has been made public** and you do not know if they were accessed.

Qualitative assessment and **proactive actions** are important!
For example when a breach of personal data can definitely create significant damage to the data subject(s). e.g. appraisals, complaints

# Guidelines on Personal Data Breach Notification: Update (4/4)

**<u>"Not your usual DBN cases"</u>**

Examples of cases when a personal data breach takes place but the EUI is not in control of the device or the system:

- EUI is informed of user account credentials found in the darkweb
- An email containing sensitive personal data is accessed via an attack to the recipients' server.
- Employees telephone numbers leaked from a chat application on compromised mobile device (used in the context of work)

# Discussion:

elements missing from the guidelines

# Feedback on the notification handling process

# Feedback on the notification handling process (1/2)

**EDPS feedback to your assessment**

- Main goal to **quickly assess the case and inform the controller** in case we see quick mitigation measures or inform if we see high risk and you need to inform the data subjects.
- **Closure letters** with feedback on your application of the process and proposals for measures to avoid similar incidents in the future.

**Copy of your notification when it is submitted via the webform**

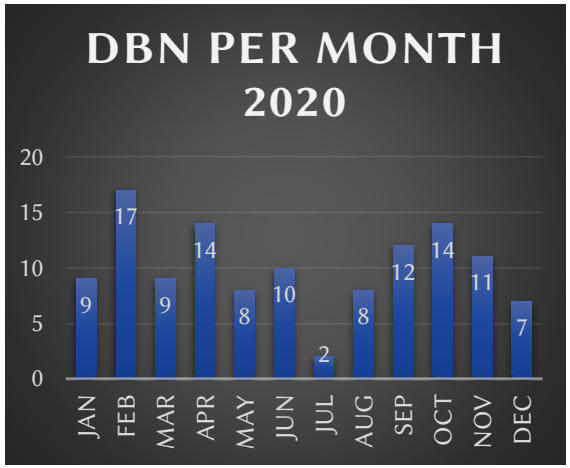
- **Requests for providing a copy of your submission.**
- **Technical difficulties, mainly for security reasons.**

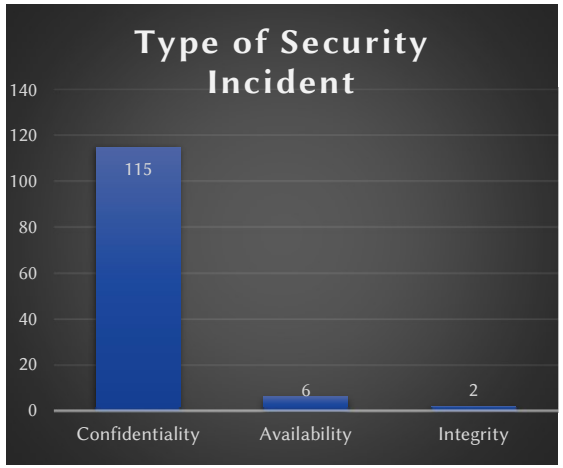
**For the moment, we advise you to print or save the form before you submit it, as also indicated in the website. Otherwise, you need to contact us to ask for a copy of your submission.**

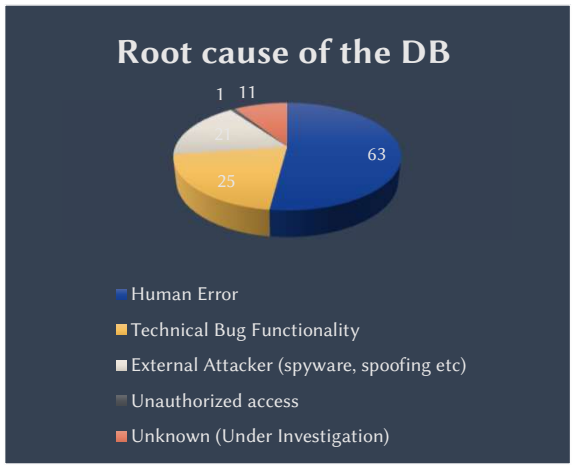
# Feedback on the notification handling process (2/2)

**Intelligence from EDPS DBN registry**

- statistics in the annual report of EDPS
- your ideas for enrichment and/or needs for other publications



# Discussion:

EDPS feedback

# Give us your feedback

## What?

- Proposals for missing elements in the guidelines
- Examples of personal data breaches (not obvious, difficulty in assessment)

## When?

- by 18 June 2021

## Where?

- **DATA-BREACH-NOTIFICATION@edps.europa.eu**


# EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

@EU_EDPS

European Data Protection Supervisor

EDPS