EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Personal Data Breaches In A Nutshell



WHAT IS A PERSONAL DATA BREACH?



A **personal data breach** is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Not every information security incident is a personal data breach, but every personal data breach is an information security incident.

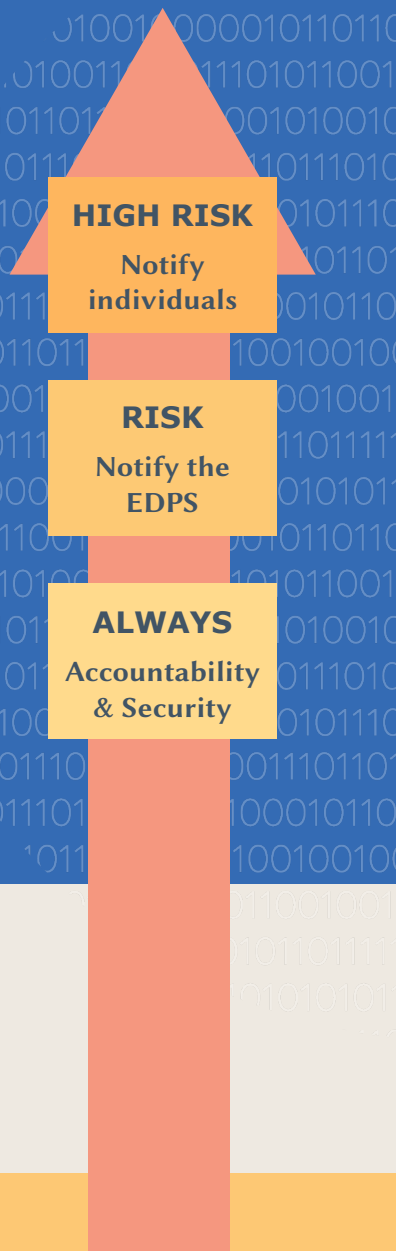
Personal data breaches may occur due to:

- human errors, when information is emailed to the wrong person;
- loss or theft of devices containing non-encrypted personal data;
- weak authentication methods which allow unauthorised access to databases.

WHAT TO DO IN CASE OF A PERSONAL DATA BREACH?

- Identify the personal data breach incident.
- Notify the breach to your Data Protection Officer (DPO), this is an **obligation** under EU data protection law.
- Handle the data breach **immediately** to mitigate any immediate risks for individuals' personal data.
- Document the breach, this is the principle of **accountability**.
- Assess the impact of the personal data breach on individuals' rights and freedoms.
- If you are a **processor**, you must immediately notify the controller of your organisation or EU institution.
- As an EU institution, office, body or agency (EUI), you are obliged to notify the European Data Protection Supervisor without undue delay and, where feasible, no later than 72 hours after the breach.
- Communicate the personal data breach to the impacted individuals if necessary.
- Review your procedures and update your measures.



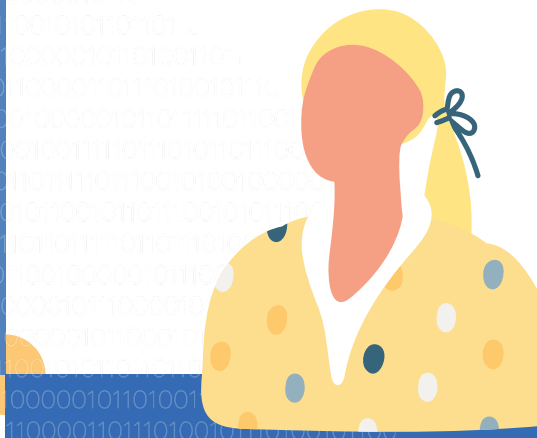


WHAT ARE THE TYPES OF BREACHES THAT MAY OCCUR?

Confidentiality breach: an entity or person accessing personal data that they are not entitled to.

Availability breach: losing access to and control of their personal data, or deleting misappropriated personal data.

Integrity breach: whenever there is an inappropriate modification of personal data.





WHO IS INVOLVED WHEN A PERSONAL DATA BREACH OCCURS?

- Top management (accountable)
- Business owner
- DPO
- IT department (if needed)
- Processors (if needed)
- Communication team (if needed)

WHAT DOES A DPO DO?

A DPO:

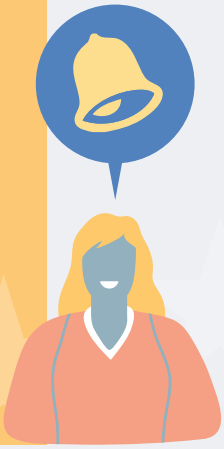
- provides advice on the assessment of the impact to the data subjects and on the necessity of Personal Data Breach notifications, when requested;
- recommends mitigation measures;
- is the contact person for individuals;
- is the contact person for the EDPS;
- communicates with security officers on Information Security Risk Management and data breach policy;
- prepares and delivers awareness programmes for employees.



HOW TO NOTIFY THE EDPS ABOUT A PERSONAL DATA BREACH?

All EUIs need to notify the EDPS in case of a personal data breach by:

- using the specific web form where communication is encrypted;
- notifying as soon as possible and no later than 72 hours (if feasible) after the detection of the breach. If you are delayed in notifying the breach, you should explain why this is the case;
- If not all information is available regarding the incident, you should notify the breach in phases. This means sending an initial notification and an initial assessment of the risk, then, as soon as possible, send any follow-up information to supplement your first notification breach.





WHEN TO COMMUNICATE A DATA BREACH TO INDIVIDUALS?

The communication of a personal data breach to individuals is mandatory when the personal data breach is likely to result in **high risks to the rights and freedoms of the individuals concerned by the breach**.

However, some exemptions exist, for example:

- when technical or organisational measures have already been implemented on the data affected by the breach, such as encryption;
- when subsequent measures have been taken to ensure that the high risk to the rights and freedoms of the individuals concerned is no longer a threat.

HOW TO COMMUNICATE A PERSONAL DATA BREACH TO INDIVIDUALS?

- Use clear and plain language, preferably in written form. Avoid technical terms that will confuse individuals.
- Describe the incident, explain what has happened and why, how the individuals' data has been affected and its consequences.
- Communicate the contact details of your DPO and the measures that you, as a controller, have taken to address the personal data breach.
- If necessary, propose measures to the individuals to protect themselves (e.g. if passwords were stolen, advise them to change the passwords if they use the same ones for other websites).

In the event that communicating this breach involves a disproportionate amount of effort, a public communication or similar measure is possible, but must ensure that individuals are informed in an equally effective manner.





WORK PROACTIVELY TO MINIMISE PERSONAL DATA BREACHES!

To minimise the potential of personal data breaches, the EDPS recommends that you establish a culture of data protection, including data security within your organisation. In other words, redesign your data processing operations so that security considerations are at the heart of them by default. Most importantly, these considerations should include:

- an email policy and staff training for the careful use of emails;
- the use of secure passwords and a second authentication factor;
- back-up copies of your systems;
- regular and mandatory system updates;
- avoiding the exposure of your services on the Internet;
- the use of encryption on your devices.



IF YOU HAVE ANY DOUBTS, PLEASE CONTACT US!

For more information:

- check out our informative video on Personal Data Breaches;
- consult the EDPS webpage on Personal Data Breaches;
- read the EDPS Guidelines on Personal Data Breach Notification.







edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

© European Union, 2021
Reproduction is authorised provided the source is acknowledged

QT-02-21-587-EN-N ISBN: 978-92-9242-692-7 DOI: 10.2804/493919