EDPB European Data Protection Board

March 2025

Personal data breaches
what to do

GUIDELINES AT A GLANCE

When processing personal data, an organisation must implement appropriate technical and organisational measures to ensure an adequate level of security.

Despite this, breaches can still occur, so it is important to know how to respond.

The GDPR defines a **personal data breach** as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

A data breach can lead to **physical, material, or non material damage** for individuals. This can include loss of control over personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, reputation damage, and loss of confidentiality of personal data protected by professional secrecy.

You must document all data breaches in a record, known as **data breach register or documentation**, by adding information about the facts relating to the personal data breach, its effects and the remedial action taken. In the event of an inspection, this documentation can be checked by the competent Data Protection Authority (DPA) to verify compliance with the GDPR.

Many personal data breaches must also be **notified to the DPA and, in certain cases, they must be notified to the individuals** whose personal data have been affected. As a personal data breach is not necessarily an infringement of the GDPR, DPAs are not obliged to exercise their corrective powers.

In case you have fallen victim of cybercrime, you are advised to report it to law enforcement. Europol lists the **reporting procedures in EU countries**.

The **EDPB guidelines on personal data breach notification under GDPR:**

- explain when an organisation should report a breach
- provide examples of different types of breaches
- specify who needs to be notified.

These guidelines are complemented by **the guidelines on examples regarding personal data breach notification** that provide additional examples to help organisations decide how to manage breaches and assess the risks involved.

There are three kinds of personal data breaches:

Confidential breach
Unauthorised or accidental **disclosure** of, or **access** to, personal data.

Integrity breach
Unauthorised or accidental **alteration** of personal data.

Availability breach
Accidental or unauthorised **loss of access** to, or **destruction** of personal data.

It is always better **to prevent data breaches and reduce the risks by adopting several measures** such as training employees on data protection, using up-to date anti-virus and anti-malware, keeping systems up to date, implementing access control policies and regularly reviewing employees' access policy, requiring multi-factor authentication for sensitive data access, monitoring unusual data flows, enforcing disk encryption, making and testing backups regularly, and setting computers to auto-lock after inactivity.

A step-by-step approach

1 Identify the breach

Organisations should have **internal processes in place to be able to detect and address a breach**, for instance by analysing appropriate logs or network traffic. When a breach is detected, it should be **reported upwards to the appropriate level of management** so it can be addressed and, if required, notified.

If you rely on processors (who process data under your instructions), they have an important role to help you comply with your obligations, for instance by assisting you in identifying and assessing the breach. You must have a proper agreement in place with them such as a contract or a legal act. It must stipulate, in particular, that processors should assist you in ensuring compliance with your obligations related to personal data breach notification. In the event of a breach, they have an obligation to notify you in a prompt way.

Organisations should **act on any initial alert and establish whether a breach has occurred**.

2 Document the breach

All personal data breaches must be documented in a **register**.

3 Notify the breach to the Data Protection Authority (DPA)

When an organisation is of the opinion that a breach **it is likely to result in a risk to the rights and freedoms of the individual**, it should **notify the relevant DPA no later than 72 hours** after having become aware of the breach. If only limited information is available, an initial notification should be performed within this timeframe, and complemented later, as the breach is being investigated. Notifications sent to the DPA after more than 72 hours must be accompanied by reasons for the delay.

The information that should be shared with the DPA includes:

- the **nature of the personal data breach**
- the **name and contact details of the data protection officer** or of another **contact point** where more information can be obtained
- the **possible consequences of the personal data breach**
- the **measures taken** or **proposed to be taken to address the breach.**

To facilitate this notification, DPAs have implemented **procedures and online forms** guiding you through this process. If the breach involves cross-border processing, it should be notified to the lead DPA or, at a minimum, the local DPA where the breach has taken place. At the same time, the organisation should act to contain and recover from the breach.

EXAMPLE 1

Context and purpose of processing

An organisation stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.

How to respond

As long as the data are encrypted with a state of the art algorithm, backups of the data exist, the decryption key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, **if it is later compromised, notification would be required**. In any case, **personal data breaches need to be documented.**

EXAMPLE 2

Context and purpose of processing

An insurance agent noticed that, due to faulty settings of an Excel file received by e-mail, he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. Following the conditions of the arrangement between the organisation and the insurance agent, the agent signalled the breach without undue delay to the organisation. The latter corrected the file and sent it out again, asking the agent to delete the former message and to confirm the deletion in a written statement, which he did.

How to respond

This data breach only affects the confidentiality of the data, while its integrity and accessibility remain unaffected. The data breach affected only about two dozen customers, which can be considered a relatively small number of individuals. Furthermore, the personal data affected does not contain any sensitive data.

The fact that the data processor immediately contacted the data controller after becoming aware of the data breach can be considered a risk mitigating factor. Due to the appropriate steps taken after the data breach, it will probably not have any impact on the individuals' rights and freedoms.

Therefore, **this case should not be notified to the Data Protection Authority and individuals. Data breach documentation remains a legal obligation.**

The examples provided above are simplified versions of examples included in the guidelines. Please refer to the full examples in the original document, if appropriate, before taking a decision on a similar case.

4 Notify the breach to affected individuals

Where the breach is **likely to result in a high risk to the rights and freedoms of individuals**, **affected individuals must also be informed as soon as possible** in order to be able to protect themselves from any negative consequences of the breach.

In some cases, and based on law enforcement authorities' advice, the organisation may delay informing affected individuals about the breach if it could interfere with an investigation. However, individuals should still be notified as soon as possible after that delay.

To inform individuals about a data breach, organisations should send dedicated messages via appropriate channels such as e-mails, SMS, direct messages, website banners or notifications. Communication channels compromised by the breach should be avoided. If needed, the communication should be done in different languages.

EXAMPLE 3

Context and purpose of processing

A hospital's information system was hit by a ransomware attack, encrypting much of its data. The hospital is working with an external cybersecurity firm to monitor its network. Logs of all data leaving the hospital, including outbound email, were reviewed. The investigation, supported by the cybersecurity firm, confirmed that the attacker only encrypted the data, not exfiltrated it.

How to respond

The type of the breach, nature, sensitivity, and volume of personal data affected in the breach are important. Even though a backup for the data existed and it could be restored in a few days, a high risk still exists as the breach led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering of the level of service due to the unavailability of the systems.

In this case, **the data breach should be notified both to the Data Protection Authority and the affected individuals. Data breach documentation is also a legal obligation.**

EXAMPLE 4

Context and purpose of processing

A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals were exfiltrated.

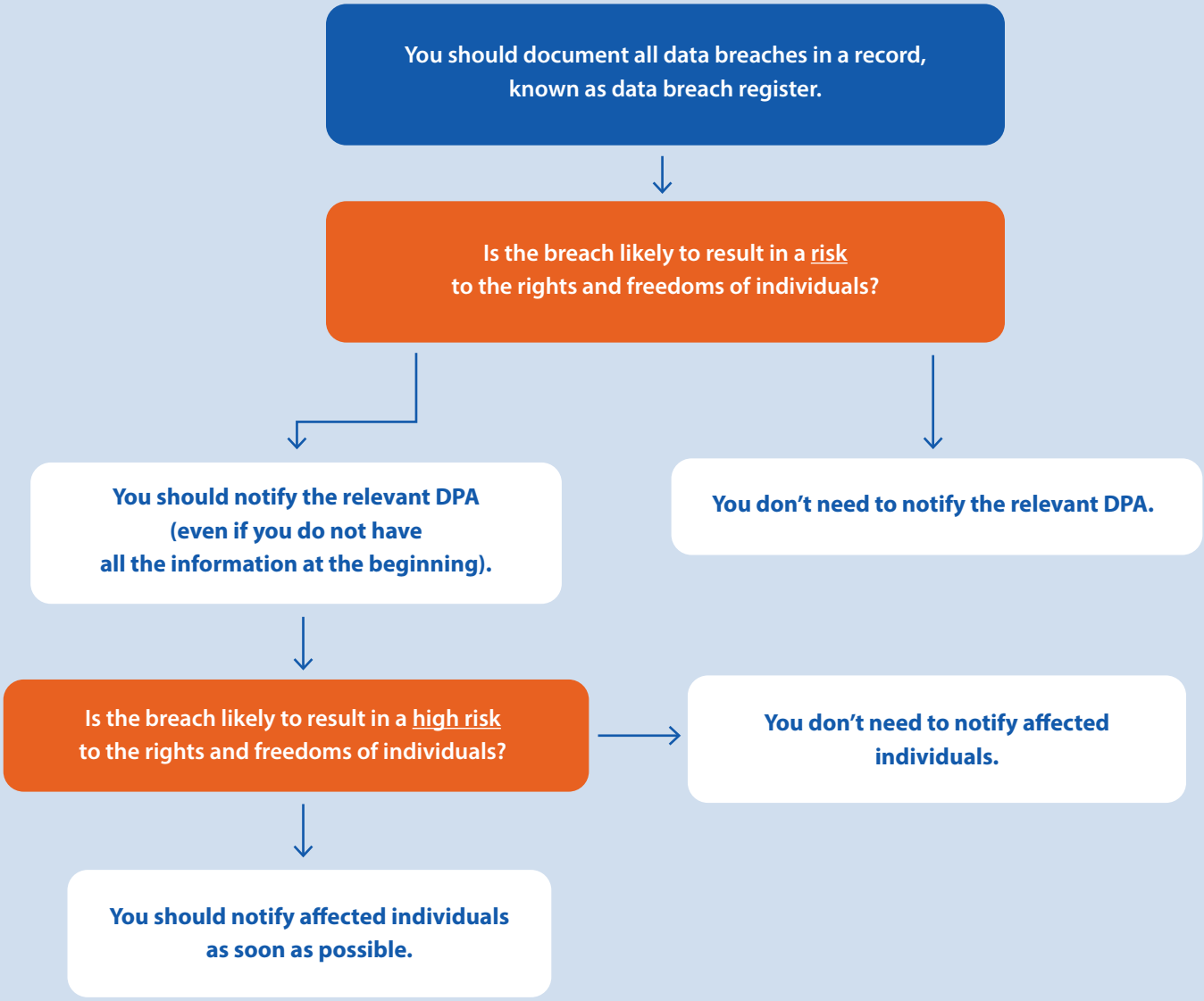
How to respond

A notification to the supervisory authority is needed if there are likely consequences to individuals. Notification to individuals depends on the nature of the personal data affected and if the severity of the consequences to individuals is high.

Data breach documentation is also a legal obligation.

The examples provided above are simplified versions of examples included in the guidelines. Please refer to the full examples in the original document, if appropriate, before taking a decision on a similar case.

In a nutshell:



If you rely on processors (who process data under your instructions), they have an important role to help you comply with your obligations, for instance by assisting you in identifying and assessing the breach.

Read more

Guidelines 9/2022

Guidelines 01/2021