

Data Breach Procedure *FAQs*



What is a data breach?

A data breach is a security violation - accidental or malicious - that results in the erasure, loss, alteration, unauthorized disclosure of or access to data that have been transmitted, stored or processed in any way. A data breach can undermine the confidentiality, integrity or availability of personal data



Which data breaches should be recorded and communicated?

Only breaches that could result in **significant adverse effects on Persons Concerned**, such as those causing physical, material or immaterial damages



Who should be informed in case of a suspected data breach?

The Data Breach Team Head

- The Data Breach Team is a multidisciplinary team of skilled and expert members led by the Data Breach Team Head
- The team takes immediate measures to address any potential or actual personal data breach

Data Breach Procedure

FAQs



Who makes up the Data Breach Team?

Data Controller

- Assesses probability that data breach will lead to a risk to rights and freedoms of natural persons
- Undertakes essential measures

Data Breach Team Head

- Determines scope and significance of data breach
- Notifies Team
- Issues adequate instructions and coordinates activities
- Advises legal representative
- Examines the incident and suggests possible countermeasures
- Documents event in the Data Breach Register

Data Breach Team Delegate

- In the absence of Team Head, works with Data Controller and other persons in charge

Data Protection Officer (DPO)

- Provides support to Data Controller
- Advises on choosing remedies and notifying Persons Concerned

IT System Manager

- Responsible for mitigating effect of data breach on computer systems
- Examines data breach and assists Data Controller in assessing consequences and choosing potential remedies
- Works to minimize impact of data breach

Internal Data Processor

- Provides advice about the breach or potential accident
- In case of emergency or DPO's absence, is contact point for interested parties
- In cooperation with the DPO, communicates data breach to Persons Concerned

External suppliers (IT, CCTV)

- Share information and cooperate to identify remedies

Data Breach Procedure

FAQs





What happens in case of a suspected Data Breach?



Step 1

Any member of the Organization who becomes aware of a data breach immediately notifies the Data Breach Team Head

The notice shall include:

-  **Which** databases or records have been breached
-  **What** happened: a short description of the data breach
-  **When** the violation occurred or became known
-  **How** the data breach supposedly took place



Step 2

The Data Breach Team Head checks the data breach reliability and notifies the Data Breach team

-  If checks reveal a data breach, the Data Breach Team Head must promptly inform the Data Controller



Step 3

The Data Breach Team Head assists the Data Controller in assessing:

- the seriousness of the violation
- its impact on the rights of Persons Concerned


They shall define:


-  Type of breach
-  Breached devices
-  Measures applied to assess severity of the breach
-  Whether data breach entails a risk to rights and freedoms of Persons Concerned
-  Categories of affected data
-  Number of Persons Concerned
-  Possible measures to be taken
-  Whether Persons Concerned shall be informed




Step 4

Data Controller

-  The Data Controller can adopt measures that it considers essential, unless it is improbable that the data breach will result in a risk to rights of natural persons or to corporate image or institutional operations

-  If the Data Breach results in a high risk for natural persons' rights, the Data Controller must notify the Persons Concerned utilizing appropriate channels

Data Breach Team Head

-  The Data Breach Team Head establishes potential measures to contain data breach or to prevent future breaches, and documents the breach in the Data Breach Register