



PERSONAL DATA BREACH: THE 72-HOUR RULE

1

IDENTIFY A PERSONAL DATA BREACH

A personal data breach is a security incident that leads to personal data being accidentally or unlawfully:

- lost or destroyed;
- altered;
- disclosed;
- accessed by unauthorised persons;
- temporarily or permanently unavailable.

2

WHEN DOES THE 72-HOUR PERIOD START?

The 72-hour period starts when the data controller has sufficient reason to believe that a security incident has occurred and that personal data have been affected.



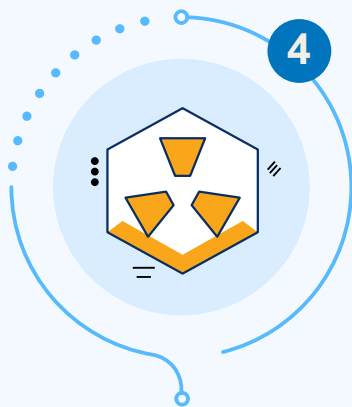
Remember:

- The time is counted in calendar hours;
- Weekends and public holidays are included.

3

ACT WITHOUT DELAY

- Stop and contain the breach.
- Inform responsible staff and the Data Protection Officer (if one has been appointed).
- Identify the affected data and individuals.
- Assess the risks to people's rights and freedoms.
- Start documenting the breach.



ASSESS THE RISK

Risk is unlikely

- There is no need to notify the supervisory authority or the affected individuals;
- However, the decision and the reasons for it must be documented.

There may be a risk

- Notify the supervisory authority without undue delay and, where possible, no later than 72 hours after becoming aware of the breach.

A high risk is likely

- Notify the supervisory authority within 72 hours.
- Inform the affected individuals without undue delay, using clear and plain language.



WHAT SHOULD BE INCLUDED IN THE NOTIFICATION?

The notification should include:

- the nature of the breach;
- the categories and approximate number of affected individuals and personal data records;
- contact details of the Data Protection Officer or another contact person;
- the likely consequences of the breach;
- measures taken to address the breach and reduce possible harm.

If all information is not yet available, submit an initial notification and provide additional information later.

If the notification is submitted late, explain the reasons for the delay.



REMEMBER

Every personal data breach must be documented, even if it is not reported to the supervisory authority or to the affected individuals.

A data processor must inform the data controller of a personal data breach without undue delay.

- **Note:** Article 4 of the [Republic of Lithuania Law on Legal Protection of Personal Data](#) provides specific exceptions for certain processing activities, such as journalism or academic, artistic, or literary expression.