TOMORIS
MORE THAN IT

FREE DOWNLOAD

CHECKLIST · TOMORIS TOOLBOX

Data Breach Under the GDPR: Checklist for the First 72 Hours

Establish, assess the risk, notify the Data Protection Authority, inform data subjects and document, under Art. 33 and 34 GDPR and the EDPB guidelines

UPDATED
Oct 25, 2026

LENGTH
PDF, 8 pages

ONLINE
tomoris.com/en/downloads/dsgvo-datenpanne-checkliste

AT A GLANCE

72 h
Data Protection Authority notification after awareness

3
types: confidentiality, integrity, availability

4
minimum contents of the notification (Art. 33(3))

All
breaches must be documented

WHO IT IS FOR

- Controllers under the GDPR: management of small and medium-sized businesses
- Data protection officers and data protection coordinators
- IT management that detects and handles security incidents
- Processors that must report breaches to their controllers

Redistribution in unchanged form permitted

WHAT THIS COVERS

A misaddressed email, a stolen laptop or an attack on the server: if personal data is affected, a 72-hour deadline starts as soon as you become aware. This checklist guides you through the steps under Art. 33 and 34 GDPR: establish whether a breach has occurred, assess the risk to the data subjects, notify the Data Protection Authority, inform the data subjects and document every breach. It is based on Guidelines 9/2022 and 01/2021 of the European Data Protection Board and the guidance of the Data Protection Authority.

This checklist is a TOMORIS recommendation and does not replace legal advice. The GDPR and the NISG 2026 as currently in force and the decision in the individual case are authoritative. The EDPB guidelines are guidance that the Data Protection Authority also refers to; notification channels and forms of the Data Protection Authority may change.

CONTENTS

01 What a data breach is 2
02 The first 72 hours at a glance 3
03 Assessing the risk 4
04 Examples from the EDPB guidelines 5
05 Notifying the Data Protection Authority 5
06 Informing data subjects 6
07 Document every data breach 7
08 Interaction with NIS2, the police and the reform 7
09 Sources 8

01

What a data breach is

Definition, the three types and when the deadline starts

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data (Art. 4(12) GDPR). According to the Data Protection Authority, it does not matter whether it happens accidentally or through fault. The EDPB distinguishes three types (Guidelines 9/2022):

Confidentiality	Unauthorized or accidental disclosure of, or access to, personal data, such as an email to the wrong recipient or data exfiltration.
Integrity	Unauthorized or accidental alteration of personal data.

Availability	Accidental or unauthorized loss of access to personal data or its destruction, for example through ransomware or a lost USB stick with no other copy.

When do the 72 hours start? According to the EDPB, as soon as the controller has a reasonable degree of certainty that a security incident has compromised personal data. A short investigation into whether a breach has occurred at all is permitted and should start as soon as possible. One incident can affect confidentiality, integrity and availability at the same time.

02

The first 72 hours at a glance

From the first indication to notification and communication

Process under Art. 33 and 34 GDPR

Indication

Investigate briefly

Check the indication immediately: has a breach occurred, which data and people are affected? Contain it at the same time.

Awareness

Deadline starts

Once you have reasonable certainty about the breach, the deadline runs; assess the risk to the data subjects.

up to 72 h

Notify the Data Protection Authority

Without undue delay and, where feasible, within 72 hours, unless there is unlikely to be a risk; later only with reasons (Art. 33(1)).

Art. 34

Inform data subjects

Without undue delay if there is likely to be a high risk, unless an exception under Art. 34(3) applies.

always

Document

Record every breach with the facts, effects and remedial action, even without notification (Art. 33(5)).

- [ ] Indication recorded (who, when, what), management and data protection officer informed.
- [ ] Briefly investigated whether personal data is affected; time of awareness recorded.
- [ ] Type of breach determined: confidentiality, integrity, availability or several.
- [ ] Immediate measures taken to address the breach and mitigate its effects, such as blocking access, asking the recipient to delete the data, restoring data from backup.
- [ ] Risk assessed and decision on notification and communication documented with reasons.
- [ ] Where a data processing agreement (DPA) is in place: the processor has reported without undue delay (Art. 33(2)) or has been asked to cooperate.

Updated Oct 25, 2026 · Redistribution unchanged permitted

03

Assessing the risk

EDPB criteria and the three possible outcomes

You must assess the likelihood and severity of possible consequences for the data subjects, not for the business. Unlike a data protection impact assessment, this concerns an event that has already occurred. The EDPB recommends considering these criteria (Guidelines 9/2022, Section IV):

- Type of breach: disclosure of health data has a different impact than its loss.
- Nature, sensitivity and volume of the data: health, identity and financial data, combinations of data, even seemingly harmless data with revealing content.
- How easily individuals can be identified; appropriately encrypted data is unintelligible to unauthorized persons without the key.
- Severity and duration of the consequences: identity theft, fraud, physical harm, psychological distress, reputational damage; whether the data is with trusted or unknown recipients.
- Special characteristics of the data subjects, such as children or other vulnerable individuals, and of the controller, such as a medical institution.
- Number of affected individuals.

Outcome of the assessment and consequences

OUTCOME	WHAT TO DO	REFERENCE
Unlikely to result in a risk	Document internally only; reassess the risk if the situation changes.	Art. 33(1) and (5) GDPR
Risk	Also notify the Data Protection Authority, without undue delay and, where feasible, within 72 hours.	Art. 33(1) GDPR
Likely to result in a high risk	Also inform the data subjects without undue delay, unless an exception applies.	Art. 34(1) and (3) GDPR

> When in doubt, the EDPB advises erring on the side of caution and notifying (Guidelines 9/2022, para. 119).

04

Examples from the EDPB guidelines

How the EDPB assesses typical cases

Cases from Guidelines 01/2021 (outcome in each case under the circumstances described there)

CASE	DOCS	DATA PROTECTION AUTHORITY	DATA SUBJECTS
Ransomware, data stored encrypted, backup restored within hours, no exfiltration, few data subjects (case 1)	yes	no	no
Ransomware with backup and without exfiltration, but in a hospital with health data (case 3)	yes	yes	yes
Ransomware, backup also affected, exfiltration of identity and financial data (case 4)	yes	yes	yes
Accidentally sent to a trusted third party, deletion confirmed in writing (case 9)	yes	no	no
Encrypted, password-protected devices with backup stolen (case 10)	yes	no	no
Laptop without password or encryption stolen, risk of identity fraud (case 11)	yes	yes	yes

> The examples show the logic but do not replace a case-by-case assessment. Even small differences, such as whether a backup exists, whether data was exfiltrated or whether it was encrypted, change the outcome.

05

Notifying the Data Protection Authority

Contents, notification channels in Austria and notification in phases

- [ ] Nature of the breach described, where possible with the categories and approximate number of data subjects and records concerned (Art. 33(3)(a)).
- [ ] Name and contact details of the data protection officer or another contact point provided (point (b)).
- [ ] Likely consequences described (point (c)).
- [ ] Measures taken or proposed to address the breach and, where appropriate, to mitigate its effects described (point (d)).
- [ ] If information is still missing: notify in phases and provide the rest without undue further delay (Art. 33(4)).

Updated Oct 25, 2026 · Redistribution unchanged permitted

- [ ] After 72 hours have passed: reasons for the delay attached (Art. 33(1)).
- [ ] Notification channel chosen: online form or PDF form of the Data Protection Authority, email to dsb@dsb.gv.at or letter to the Data Protection Authority, Barichgasse 40-42, 1030 Vienna.
- [ ] Cross-border processing: notified to the lead supervisory authority (EDPB 9/2022, para. 69).
- [ ] Copy of the notification and, if available, proof of sending filed.

After notification, the Data Protection Authority checks whether the minimum information has been provided and appropriate measures have been taken. Only if this is not the case will it contact you and request additional information; otherwise it closes the proceedings informally. Processors notify the controller without undue delay (Art. 33(2)); the EDPB recommends regulating this in the contract and providing information in phases.

06

Informing data subjects

When, with what content and which exceptions apply

- [ ] If there is likely to be a high risk, data subjects informed without undue delay (Art. 34(1)).
- [ ] Nature of the breach described in clear and plain language (Art. 34(2)).
- [ ] Contact point, likely consequences and measures taken stated (Art. 34(2) with Art. 33(3)(b) to (d)).
- [ ] Specific recommendations given, such as changing passwords or watching out for fraud attempts (EDPB 9/2022, para. 87).

No communication required if (Art. 34(3) GDPR)

point (a)	Appropriate safeguards rendered the affected data unintelligible to unauthorized persons, for example through encryption.
point (b)	Subsequent measures ensure that the high risk is no longer likely to materialize.
point (c)	Communication would involve disproportionate effort; in that case a public communication or a similarly effective measure is required instead.

The Data Protection Authority can require you to communicate the breach after the fact (Art. 34(4)); according to its guidance, it does so by official decision. Infringements of Art. 33 and 34 can lead to fines of up to €10 million or 2% of worldwide annual turnover, whichever is higher (Art. 83(4)(a) GDPR).

07

Document every data breach

Register of breaches, even if no notification is made

The controller documents every breach with all the facts, its effects and the remedial action taken; this must enable the Data Protection Authority to verify compliance (Art. 33(5)). The EDPB recommends an internal register of all breaches, including those not subject to notification; it may be part of the record of processing activities if the entries are clearly identifiable.

Entry in the register of data breaches (template)

FIELD	ENTRY
Number, time of the incident and of awareness	_____
What happened, cause	_____
Type: confidentiality, integrity, availability	_____
Affected data and individuals, approximate number	_____
Assessment: no risk, risk, high risk, with reasons	_____
Notification to the Data Protection Authority: date, channel, case number if assigned, or reasons for not notifying	_____
Communication to data subjects: date, how, or exception applied	_____
Effects and remedial action	_____
Completed on, responsible	_____

08

Interaction with NIS2, the police and the reform

Other reporting channels and what could change

- NIS2: Essential and important entities also report significant cybersecurity incidents to the CSIRT: early warning within 24 hours, notification within 72 hours, final report no later than one month after the notification (§ 34 NISG 2026, Austrian Network and Information Systems Security Act 2026). Both obligations apply side by side; the authorities cooperate under § 21 NISG 2026.
- Police: According to the EDPB, victims of cybercrime should file a report with the law enforcement authorities.

Updated Oct 25, 2026 · Redistribution unchanged permitted

Reform in progress: The Digital Omnibus proposal COM(2025) 837 would limit notification to breaches likely to result in a high risk, extend the deadline to 96 hours and provide for a single reporting point. On October 25, 2026, procedure 2025/0360(COD) was awaiting the committee decision in Parliament. Until the change applies (according to the proposal, 18 months after entry into force), Art. 33 GDPR remains authoritative.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 reporting deadline calculator (German)
tomoris.com/tools/meldefristen-rechner

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

09

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **Regulation (EU) 2016/679 (GDPR), German version on EUR-Lex**
Art. 4(12), Art. 33, 34 and 83(4), accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu

2 **EDPB: Guidelines 9/2022 on personal data breach notification, version 2.0 (March 28, 2023)**
Types, awareness, content, risk, documentation; paras. 34, 69, 87, 119; accessed October 25, 2026
www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelin...

3 **EDPB: Guidelines 01/2021, examples regarding notification, version 2.0 (December 14, 2021)**
Cases 1, 3, 4, 9, 10 and 11, accessed October 25, 2026
www.edpb.europa.eu/system/files/documents/2022-01/edpb_guidelin...

4 **EDPB: Guidelines at a glance, Data breaches**
Register of all breaches, reporting cybercrime, accessed October 25, 2026
www.edpb.europa.eu/system/files/2026-10/edpb_guidelines-at-a-gl...

5 **Austrian Data Protection Authority: Data breach notification**
Notification channels, procedure, notification in phases, accessed October 25, 2026
dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach

6 **NISG 2026, BGBl. I No. 94/2025, version in force in the RIS**
§ 21 cooperation with the Data Protection Authority, § 34 reporting obligations, accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

7 **European Commission: Digital Omnibus proposal COM(2025) 837**
Art. 3(8), amendment of Art. 33 GDPR, accessed October 25, 2026
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837

8 **European Parliament, Legislative Observatory: 2025/0360(COD)**
Status of the procedure on October 25, 2026
oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference...