

CHECKLISTE · TOMORIS TOOLBOX

Datenpanne nach DSGVO: Checkliste für die ersten 72 Stunden

Feststellen, Risiko bewerten, an die Datenschutzbehörde melden, Betroffene benachrichtigen und dokumentieren, nach Art. 33 und 34 DSGVO und den EDSA-Leitlinien

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/dsgvo-datenpanne-checkliste

AUF EINEN BLICK

72 h

Meldung an die Datenschutzbehörde ab Kenntnis

3

Arten: Vertraulichkeit, Integrität, Verfügbarkeit

4

Mindestangaben der Meldung (Art. 33 Abs. 3)

Alle

Verletzungen sind zu dokumentieren

FÜR WEN

- Verantwortliche nach der DSGVO: Geschäftsführung kleiner und mittlerer Unternehmen
- Datenschutzbeauftragte und Datenschutzkoordination
- IT-Leitung, die Sicherheitsvorfälle erkennt und bearbeitet
- Auftragsverarbeiter, die Verletzungen an ihre Auftraggeber melden müssen

WURUM ES GEHT

Ein falsch adressiertes E-Mail, ein gestohlenes Notebook oder ein Angriff auf den Server: Wenn personenbezogene Daten betroffen sind, beginnt mit der Kenntnis eine Frist von 72 Stunden. Diese Checkliste führt Sie durch die Schritte nach Art. 33 und 34 DSGVO: feststellen, ob eine Verletzung vorliegt, das Risiko für die betroffenen Personen bewerten, an die Österreichische Datenschutzbehörde melden, die Betroffenen benachrichtigen und jede Verletzung dokumentieren. Sie stützt sich auf die Leitlinien 9/2022 und 01/2021 des Europäischen Datenschutzausschusses und die Hinweise der Datenschutzbehörde.

Diese Checkliste ist eine Empfehlung von TOMORIS und ersetzt keine Rechtsberatung. Maßgeblich sind die DSGVO und das NISG 2026 in der jeweils geltenden Fassung sowie die Entscheidung im Einzelfall. Die Leitlinien des EDSA sind eine Orientierungshilfe, auf die auch die Datenschutzbehörde verweist; Meldewege und Formulare der Datenschutzbehörde können sich ändern.

INHALT

01	Was eine Datenpanne ist	2
02	Die ersten 72 Stunden im Überblick	3
03	Risiko bewerten	4
04	Beispiele aus den Leitlinien des EDSA	5
05	Meldung an die Datenschutzbehörde	5
06	Betroffene benachrichtigen	6
07	Jede Datenpanne dokumentieren	7
08	Zusammenspiel mit NIS2, Polizei und Reform	8
09	Quellen	8

01 —

Was eine Datenpanne ist

Begriff, die drei Arten und wann die Frist zu laufen beginnt

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt (Art. 4 Z 12 DSGVO). Ob sie unbeabsichtigt oder schuldhaft passiert, spielt laut Datenschutzbehörde keine Rolle. Der EDSA unterscheidet drei Arten (Leitlinien 9/2022):

Vertraulichkeit	Unbefugte oder versehentliche Offenlegung von oder Zugriff auf personenbezogene Daten, etwa ein E-Mail an den falschen Empfänger oder ein Datenabfluss.
Integrität	Unbefugte oder versehentliche Veränderung personenbezogener Daten.
Verfügbarkeit	Vorsehentlich oder unbefugter Verlust des Zugriffs auf personenbezogene Daten oder ihre Vernichtung, etwa durch Ransomware oder einen verlorenen USB-Stick ohne weitere Kopie.

Wann beginnen die 72 Stunden? Laut EDSA, sobald der Verantwortliche mit hinreichender Sicherheit weiß, dass ein Sicherheitsvorfall personenbezogene Daten beeinträchtigt hat. Eine kurze Untersuchung, ob überhaupt eine Verletzung vorliegt, ist zulässig und sollte so bald wie möglich beginnen. Ein Vorfall kann Vertraulichkeit, Integrität und Verfügbarkeit zugleich betreffen.

02

Die ersten 72 Stunden im Überblick

Vom ersten Hinweis bis zur Meldung und Benachrichtigung

Ablauf nach Art. 33 und 34 DSGVO



- ☐ Hinweis aufgenommen (wer, wann, was), Leitung und Datenschutzbeauftragte verständigt.
- ☐ Kurz untersucht, ob personenbezogene Daten betroffen sind; Zeitpunkt der Kenntnis festgehalten.
- ☐ Art der Verletzung bestimmt: Vertraulichkeit, Integrität, Verfügbarkeit oder mehrere.
- ☐ Sofortmaßnahmen gesetzt, um die Verletzung zu beheben und Folgen abzumildern, etwa Zugang sperren, Empfänger um Löschung ersuchen, Daten aus Sicherung wiederherstellen.

- ☐ Risiko bewertet und Entscheidung über Meldung und Benachrichtigung mit Begründung dokumentiert.
- ☐ Bei Auftragsverarbeitung: Auftragsverarbeiter hat unverzüglich gemeldet (Art. 33 Abs. 2) bzw. wurde zur Mitwirkung aufgefordert.

03

Risiko bewerten

Kriterien des EDSA und die drei möglichen Ergebnisse

Zu bewerten sind Eintrittswahrscheinlichkeit und Schwere möglicher Folgen für die betroffenen Personen, nicht für das Unternehmen. Anders als bei einer Datenschutz-Folgenabschätzung geht es um ein Ereignis, das bereits eingetreten ist. Der EDSA empfiehlt, diese Kriterien zu berücksichtigen (Leitlinien 9/2022, Abschnitt IV):

- Art der Verletzung: Offenlegung von Gesundheitsdaten wirkt anders als ihr Verlust.
- Art, Sensibilität und Umfang der Daten: Gesundheits-, Ausweis- und Finanzdaten, Kombinationen von Daten, auch scheinbar harmlose Daten mit verräterischem Inhalt.
- Wie leicht sich Personen identifizieren lassen; angemessen verschlüsselte Daten sind für Unbefugte ohne Schlüssel unverständlich.
- Schwere und Dauer der Folgen: Identitätsdiebstahl, Betrug, körperlicher Schaden, psychische Belastung, Rufschaden; ob die Daten bei vertrauenswürdigen oder unbekannten Empfängern sind.
- Besondere Merkmale der Betroffenen, etwa Kinder oder andere schutzbedürftige Personen, und des Verantwortlichen, etwa eine medizinische Einrichtung.
- Zahl der betroffenen Personen.

Ergebnis der Bewertung und Folgen

ERGEBNIS	WAS ZU TUN IST	FUNDSTELLE
Voraussichtlich kein Risiko	Nur intern dokumentieren; Risiko neu bewerten, wenn sich die Lage ändert.	Art. 33 Abs. 1 und 5 DSGVO
Risiko	Zusätzlich an die Datenschutzbehörde melden, unverzüglich und möglichst binnen 72 Stunden.	Art. 33 Abs. 1 DSGVO
Voraussichtlich hohes Risiko	Zusätzlich die betroffenen Personen unverzüglich benachrichtigen, außer eine Ausnahme greift.	Art. 34 Abs. 1 und 3 DSGVO

Im Zweifel rät der EDSA, vorsichtig zu sein und zu melden (Leitlinien 9/2022, Rn. 119).

04 —

Beispiele aus den Leitlinien des EDSA

Wie der EDSA typische Fälle beurteilt

Fälle aus den Leitlinien 01/2021 (Ergebnis jeweils unter den dort beschriebenen Umständen)

FALL	DOKU	DSB	BETROFFENE
Ransomware, Daten verschlüsselt gespeichert, Sicherung binnen Stunden eingespielt, kein Abfluss, wenige Betroffene (Fall 1)	ja	nein	nein
Ransomware mit Sicherung und ohne Abfluss, aber in einem Krankenhaus mit Gesundheitsdaten (Fall 3)	ja	ja	ja
Ransomware, Sicherung ebenfalls betroffen, Datenabfluss mit Ausweis- und Finanzdaten (Fall 4)	ja	ja	ja
Versehentlich an einen vertrauenswürdigen Dritten gesendet, Löschung schriftlich bestätigt (Fall 9)	ja	nein	nein
Verschlüsselte, kennwortgeschützte Geräte mit Sicherung gestohlen (Fall 10)	ja	nein	nein
Notebook ohne Kennwort und Verschlüsselung gestohlen, Gefahr von Identitätsbetrug (Fall 11)	ja	ja	ja

Die Beispiele zeigen die Logik, ersetzen aber nicht die Prüfung im Einzelfall: Schon kleine Unterschiede, etwa ob eine Sicherung vorhanden ist, ob Daten abgeflossen sind oder ob sie verschlüsselt waren, ändern das Ergebnis.

05 —

Meldung an die Datenschutzbehörde

Inhalt, Meldeweg in Österreich und schrittweise Meldung

- ☐ Art der Verletzung beschrieben, soweit möglich mit Kategorien und ungefährender Zahl der betroffenen Personen und Datensätze (Art. 33 Abs. 3 lit. a).
- ☐ Name und Kontaktdaten der Datenschutzbeauftragten oder einer anderen Anlaufstelle angegeben (lit. b).
- ☐ Wahrscheinliche Folgen beschrieben (lit. c).
- ☐ Ergriffene oder vorgeschlagene Maßnahmen zur Behebung und gegebenenfalls zur Abmilderung beschrieben (lit. d).

- ☐ Fehlen noch Informationen: schrittweise melden, ohne unangemessene weitere Verzögerung nachreichen (Art. 33 Abs. 4).
- ☐ Nach Ablauf von 72 Stunden: Begründung für die Verzögerung beigelegt (Art. 33 Abs. 1).
- ☐ Meldeweg gewählt: Onlineformular oder PDF-Formular der Datenschutzbehörde, E-Mail an dsb@dsb.gv.at oder Brief an die Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien.
- ☐ Grenzüberschreitende Verarbeitung: an die federführende Aufsichtsbehörde gemeldet (EDSA 9/2022, Rn. 69).
- ☐ Kopie der Meldung und, falls vorhanden, ein Sendenachweis abgelegt.

Nach der Meldung prüft die Datenschutzbehörde, ob die Mindestangaben vorliegen und geeignete Maßnahmen gesetzt wurden. Nur wenn das nicht der Fall ist, meldet sie sich und verlangt eine Ergänzung; sonst stellt sie das Verfahren formlos ein. Auftragsverarbeiter melden dem Verantwortlichen unverzüglich (Art. 33 Abs. 2); der EDSA empfiehlt, das im Vertrag zu regeln und Informationen schrittweise nachzuliefern.

06

Betroffene benachrichtigen

Wann, mit welchem Inhalt und welche Ausnahmen gelten

- ☐ Bei voraussichtlich hohem Risiko die betroffenen Personen unverzüglich benachrichtigt (Art. 34 Abs. 1).
- ☐ In klarer und einfacher Sprache die Art der Verletzung beschrieben (Art. 34 Abs. 2).
- ☐ Kontaktstelle, wahrscheinliche Folgen und ergriffene Maßnahmen genannt (Art. 34 Abs. 2 mit Art. 33 Abs. 3 lit. b bis d).
- ☐ Konkrete Empfehlungen gegeben, etwa Kennwort ändern oder auf Betrugsversuche achten (EDSA 9/2022, Rn. 87).

Keine Benachrichtigung nötig, wenn (Art. 34 Abs. 3 DSGVO)

- | | |
|---------------|---|
| lit. a | Geeignete Vorkehrungen machten die betroffenen Daten für Unbefugte unzugänglich, etwa durch Verschlüsselung. |
| lit. b | Nachfolgende Maßnahmen stellen sicher, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht. |

lit. c

Die Benachrichtigung wäre mit unverhältnismäßigem Aufwand verbunden; dann ist stattdessen eine öffentliche Bekanntmachung oder ähnlich wirksame Maßnahme nötig.

Die Datenschutzbehörde kann verlangen, dass Sie die Benachrichtigung nachholen (Art. 34 Abs. 4); laut ihren Hinweisen geschieht das mit Bescheid. Verstöße gegen Art. 33 und 34 können Geldbußen bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes nach sich ziehen, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 4 lit. a DSGVO).

07

Jede Datenpanne dokumentieren

Register der Verletzungen, auch wenn nicht gemeldet wird

Der Verantwortliche dokumentiert jede Verletzung mit allen Fakten, ihren Auswirkungen und den ergriffenen Abhilfemaßnahmen; die Datenschutzbehörde muss damit die Einhaltung prüfen können (Art. 33 Abs. 5). Der EDSA empfiehlt ein internes Register aller Verletzungen, auch der nicht meldepflichtigen; es darf Teil des Verzeichnisses von Verarbeitungstätigkeiten sein, wenn die Einträge klar erkennbar sind.

Eintrag im Register der Datenschutzverletzungen (Muster)

FELD	EINTRAG
Nummer, Zeitpunkt des Vorfalls und der Kenntnis	_____
Was ist passiert, Ursache	_____
Art: Vertraulichkeit, Integrität, Verfügbarkeit	_____
Betroffene Daten und Personen, ungefähre Zahl	_____
Bewertung: kein Risiko, Risiko, hohes Risiko, mit Begründung	_____
Meldung an die DSB: am, Weg, Aktenzeichen falls vergeben, oder Begründung, warum nicht	_____
Benachrichtigung der Betroffenen: am, wie, oder angewandte Ausnahme	_____
Auswirkungen und Abhilfemaßnahmen	_____
Erledigt am, verantwortlich	_____

08

Zusammenspiel mit NIS2, Polizei und Reform

Weitere Meldewege und was sich ändern könnte

- NIS2: Wesentliche und wichtige Einrichtungen melden erhebliche Cybersicherheitsvorfälle zusätzlich dem CSIRT: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht spätestens einen Monat nach der Meldung (§ 34 NISG 2026). Beide Pflichten gelten nebeneinander; die Behörden arbeiten nach § 21 NISG 2026 zusammen.
- Polizei: Wer Opfer von Cyberkriminalität wird, sollte laut EDSA Anzeige bei den Strafverfolgungsbehörden erstatten.

Reform in Arbeit: Der Digital-Omnibus-Vorschlag COM(2025) 837 würde die Meldung auf Verletzungen mit voraussichtlich hohem Risiko beschränken, die Frist auf 96 Stunden verlängern und eine zentrale Meldestelle vorsehen. Am 25.10.2026 wartete das Verfahren 2025/0360(COD) im Parlament auf die Ausschussentscheidung. Bis die Änderung gilt (laut Vorschlag 18 Monate nach Inkrafttreten), bleibt Art. 33 DSGVO maßgeblich.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Meldefristen-Rechner

tomoris.com/tools/meldefristen-rechner

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- Verordnung (EU) 2016/679 (DSGVO), deutsche Fassung auf EUR-Lex**
Art. 4 Z 12, Art. 33, 34 und 83 Abs. 4, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- EDSA: Leitlinien 9/2022 zur Meldung von Datenschutzverletzungen, Version 2.0 (28.03.2023)**
Arten, Kenntnis, Inhalt, Risiko, Dokumentation; Rn. 34, 69, 87, 119; gelesen am 25.10.2026
www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelin...
- EDSA: Leitlinien 01/2021, Beispiele zur Meldung, Version 2.0 (14.12.2021)**
Fälle 1, 3, 4, 9, 10 und 11, gelesen am 25.10.2026
www.edpb.europa.eu/system/files/documents/2022-01/edpb_guidelin...
- EDSA: Guidelines at a glance, Data breaches**
Register aller Verletzungen, Anzeige bei Cyberkriminalität, gelesen am 25.10.2026
www.edpb.europa.eu/system/files/2026-10/edpb_guidelines-at-a-gl...
- Österreichische Datenschutzbehörde: Meldung Data Breach**
Meldewege, Ablauf des Verfahrens, schrittweise Meldung, gelesen am 25.10.2026
dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach
- NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 21 Zusammenarbeit mit der Datenschutzbehörde, § 34 Berichtspflichten, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- Kommission: Digital-Omnibus-Vorschlag COM(2025) 837**
Art. 3 Nr. 8, Änderung von Art. 33 DSGVO, gelesen am 25.10.2026
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837
- EU-Parlament, Legislative Observatory: 2025/0360(COD)**
Verfahrensstand am 25.10.2026
oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference...