DSGVO-Vorlagenpaket zur Meldung von Datenpannen

Behördenmeldung nach Artikel 33 · Betroffenen-Anschreiben nach Artikel 34 · Pannenregister nach Artikel 33(5)

KOSTENLOSE VORLAGE — DOCX · PDF · MD | Version 1.0 · Stand 2026-07-22

Dokument A — binnen 72 Stunden nach Kenntnis bei Ihrer Aufsichtsbehörde einreichen (DSGVO Art 33).

Dokument B — bei hohem Risiko unverzüglich an die betroffenen Personen senden (DSGVO Art 34).

Dokument C — jede Verletzung protokollieren, gemeldet oder nicht (DSGVO Art 33(5)).

Dokument D — die Entscheidungshilfe: melden oder nicht.

Deutschland: Meldung an die Landesdatenschutzbehörde Ihrer Niederlassung (Online-Meldeformular). UK: Meldung an die ICO (Online-Formular / Telefon). Norwegen: Meldung an das Datatilsynet über Altinn.

Grenzüberschreitend in EU/EWR: Meldung an Ihre federführende Aufsichtsbehörde (Art 56).

Dokument A — Meldung an die Aufsichtsbehörde (Artikel 33)

Füllen Sie jeden Abschnitt aus. Die Abschnitte 2–5 bilden Artikel 33(3)(a)–(d) ab — den gesetzlichen Mindestinhalt. Die 72-Stunden-Uhr läuft ab Kenntnis (EDSA-Leitlinien 9/2022): dem Moment, in dem eine verantwortliche Person mit hinreichender Sicherheit feststellt, dass personenbezogene Daten kompromittiert wurden.

A.1 Angaben zur Einreichung

An (Aufsichtsbehörde)	Zuständige Behörde; federführende Aufsichtsbehörde bei grenzüberschreitenden Fällen (Art 56); in Deutschland die Landesdatenschutzbehörde Ihrer Niederlassung
Von (Verantwortlicher)	Name der juristischen Person und eingetragene Anschrift
Vorfallsreferenz	Interne ID, z. B. BREACH-2026-007
Meldetyp	Erstmeldung / Aktualisierung / Abschluss (gestufte Meldung nach Art 33(4))
Eingereicht (Datum & Uhrzeit)	Zeitstempel dieser Einreichung

A.2 Kenntnis und zeitlicher Ablauf (Art 33(1))

Zeitpunkt der Kenntnis	Wann eine verantwortliche Person feststellte, dass wahrscheinlich eine Verletzung vorliegt — startet die 72-Stunden-Uhr
Wie wir Kenntnis erlangten	Alarm, Mitteilung des Auftragsverarbeiters nach Art 33(2), Kundenhinweis, Audit-Feststellung…
Gründe für die Verzögerung	PFLICHT, wenn diese Einreichung später als 72 Stunden nach Kenntnis erfolgt; sonst n/a

A.3 Art der Verletzung (Art 33(3)(a))

Was passiert ist	Beschreiben Sie den Vorfall und seine Ursache; Verletzung der Vertraulichkeit, Integrität und/oder Verfügbarkeit
Kategorien der betroffenen Personen	Z. B. Kunden, Beschäftigte, Endnutzer von Kunden
Ungefähre Zahl der betroffenen Personen	Zahl oder Spanne; in späteren Einreichungen aktualisieren, falls sie sich ändert
Kategorien der personenbezogenen Daten	Z. B. Kontaktdaten, Zugangsdaten, Finanzdaten — besondere Kategorien (Art 9) ausdrücklich kennzeichnen
Ungefähre Zahl der Datensätze	Zahl oder Spanne

A.4 Anlaufstelle (Art 33(3)(b))

DSB / Anlaufstelle	Name, Funktion, E-Mail, Telefon — wo die Behörde weitere Informationen erhalten kann

A.5 Wahrscheinliche Folgen (Art 33(3)(c))

Wahrscheinliche Folgen	Realistische Schäden: Identitätsdiebstahl, Betrug, finanzieller Verlust, Reputationsschaden, Offenlegung besonderer Kategorien

A.6 Ergriffene oder vorgeschlagene Maßnahmen (Art 33(3)(d))

Eindämmung & Behebung	Was zur Bewältigung der Verletzung unternommen wurde
Abmilderung nachteiliger Auswirkungen	Maßnahmen, die den Schaden für die Betroffenen verringern, z. B. erzwungener Passwort-Reset, Sperrung von Zugangsdaten

A.7 Position zur Benachrichtigung der betroffenen Personen

Risikobewertung	Voraussichtlich kein Risiko / Risiko / hohes Risiko — mit kurzer Begründung
Position zu Artikel 34	Benachrichtigung versandt oder geplant (Datum), oder Ausnahme: 34(3)(a) unverständlich gemachte Daten, 34(3)(b) Risiko beseitigt, 34(3)(c) öffentliche Bekanntmachung

A.8 Grenzüberschreitende Verarbeitung (Art 56)

Grenzüberschreitend?	Sind betroffene Personen in mehr als einem Mitgliedstaat betroffen?
Grundlage der federführenden Behörde	Begründung der Hauptniederlassung, die die federführende Aufsichtsbehörde bestimmt

Dokument B — Benachrichtigung der betroffenen Personen (Artikel 34)

Erforderlich unverzüglich, wenn die Verletzung voraussichtlich ein HOHES Risiko zur Folge hat. Klare und einfache Sprache; muss mindestens Anlaufstelle, wahrscheinliche Folgen und Maßnahmen enthalten (Art 34(2) → Art 33(3)(b),(c),(d)). Text in eckigen Klammern ersetzen; Sätze kurz halten; Fachjargon vermeiden.

Betreff	Wichtiger Sicherheitshinweis zu Ihren personenbezogenen Daten
Was passiert ist	[Ein bis zwei Sätze in einfacher Sprache: was passiert ist, wann es entdeckt und eingedämmt wurde.]
Welche Daten betroffen sind	[Die betroffenen Datenkategorien der Empfängerin / des Empfängers. Sagen Sie klar, was NICHT betroffen ist, z. B. Zahlungsdaten.]
Was das für Sie bedeuten kann	[Realistische Folgen — z. B. Phishing-E-Mails, die aussehen, als kämen sie von uns, oder Anmeldeversuche.]
Was wir tun	[Eindämmung, Untersuchung, Meldung an die Aufsichtsbehörde, Sicherheitsverbesserungen.]
Was Sie tun können	[Konkrete Schritte: Passwort zurücksetzen, Zwei-Faktor-Authentifizierung aktivieren, auf verdächtige E-Mails achten, Kontoauszüge prüfen.]
Wo Sie weitere Informationen erhalten	[DSB / Anlaufstelle: Name, E-Mail, Telefon — und eine Statusseite, falls vorhanden.]
Schluss	Wir entschuldigen uns für die Beunruhigung, die dieser Vorfall auslösen kann. Wir halten Sie über den Fortgang unserer Untersuchung auf dem Laufenden.

Variante öffentliche Bekanntmachung (Art 34(3)(c))

Wäre die individuelle Benachrichtigung jeder betroffenen Person mit unverhältnismäßigem Aufwand verbunden, veröffentlichen Sie denselben Inhalt als öffentliche Mitteilung (Website-Banner, Pressemitteilung), die die Betroffenen ebenso wirksam informiert — und dokumentieren Sie Kanalwahl und Begründung in Dokument C.

Dokument C — Interner Pannenregister-Eintrag (Artikel 33(5))

Erstellen Sie einen Eintrag pro Vorfall — einschließlich der Verletzungen, die Sie bewusst NICHT melden. Über dieses Register überprüft eine Aufsichtsbehörde die Einhaltung des Artikels 33.

Vorfallsreferenz	Interne ID
Zeitpunkt der Kenntnis / wie	Wann die Uhr startete und was die Kenntnis auslöste
Fakten der Verletzung	Art, Ursache, betroffene Personen und Datensätze
Auswirkungen	Tatsächliche und wahrscheinliche beobachtete Folgen

Risikobewertung & Begründung	Voraussichtlich kein Risiko / Risiko / hohes Risiko — und warum
Behörde gemeldet?	Ja (Datum, Referenz) / Nein — Begründung: voraussichtlich kein Risiko
Betroffene benachrichtigt?	Ja (Datum, Kanal) / Nein — welche Ausnahme nach Art 34(3) und warum
Mitteilung des Auftragsverarbeiters (Art 33(2))	Welcher Auftragsverarbeiter uns wann informierte — falls die Verletzung bei einem Auftragsverarbeiter entstand
Abhilfemaßnahmen	Was infolgedessen behoben, geändert oder verbessert wurde
Meldeprotokoll	Erst-/Aktualisierungs-/Abschlussmeldungen: Daten und Referenzen

Dokument D — Entscheidungshilfe: melden oder nicht

Situation	Was Sie vorlegen müssen
Verletzung führt voraussichtlich nicht zu einem Risiko	Nur Dokument C — mit Ihrer Begründung protokollieren
Verletzung führt voraussichtlich zu einem Risiko	Dokument A binnen 72 h + Dokument C
Verletzung führt voraussichtlich zu einem HOHEN Risiko	Dokument A + Dokument B unverzüglich + Dokument C
Hohes Risiko, aber Daten unverständlich gemacht (verschlüsselt, Schlüssel sicher) — Art 34(3)(a)	Dokument A + Dokument C; kein Dokument B
Hohes Risiko, aber durch nachträgliche Maßnahmen beseitigt — Art 34(3)(b)	Dokument A + Dokument C; kein Dokument B
Individuelle Anschreiben = unverhältnismäßiger Aufwand — Art 34(3)(c)	Dokument A + öffentliche Bekanntmachung + Dokument C

Die Aufsichtsbehörde kann die Benachrichtigung der betroffenen Personen nach Art 34(4) auch dann anordnen, wenn Sie zu dem Schluss kamen, dass sie nicht erforderlich ist. Bußgelder für Verstöße gegen Art 33/34: bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes (Art 83(4)(a)).