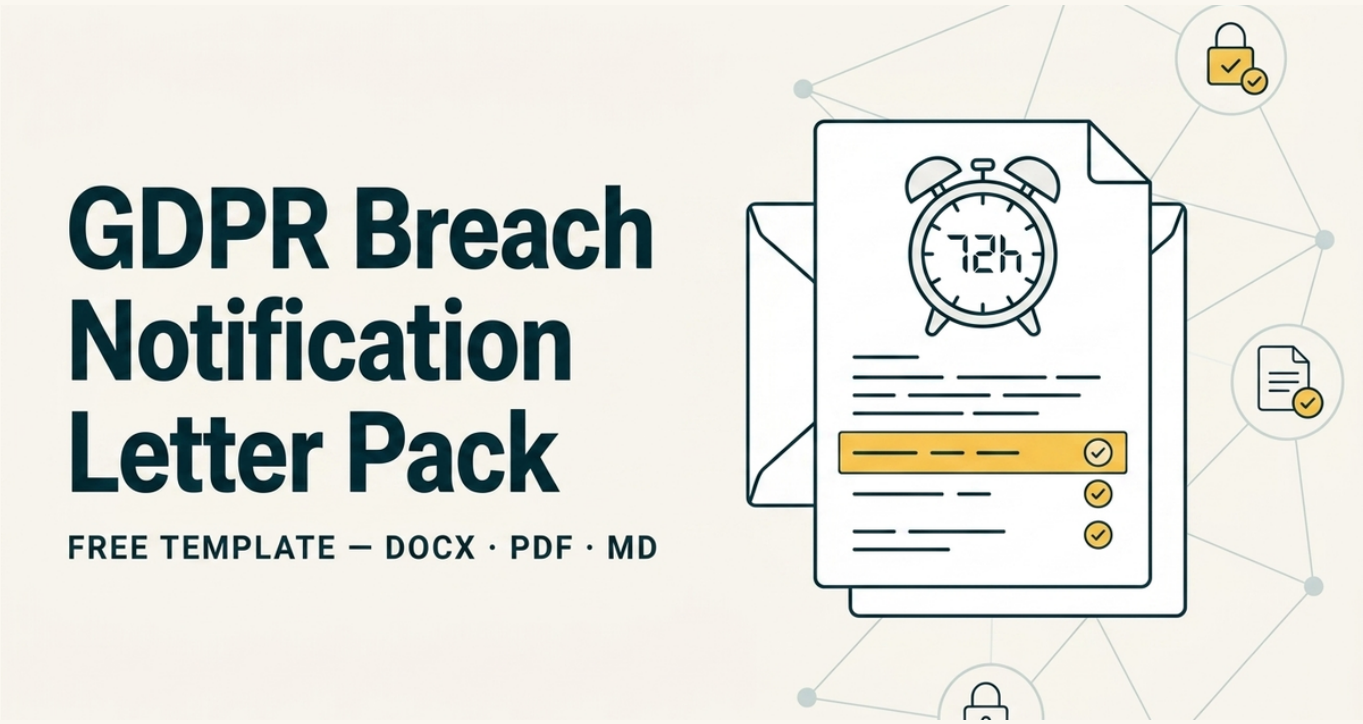

GDPR Breach Notification Letter Pack

Article 33 authority notification · Article 34 data-subject letter · Article 33(5) breach log

FREE TEMPLATE — DOCX · PDF · MD | Version 1.0 · Updated 2026-07-15

Document A — file with your supervisory authority within 72 hours of awareness (GDPR Art 33).
Document B — send to data subjects without undue delay when the risk is high (GDPR Art 34).
Document C — log every breach, notified or not (GDPR Art 33(5)).
Document D — the notify-or-not decision aid.

UK: report to the ICO (online form / phone). Norway: report to Datatilsynet via Altinn.
Cross-border in the EU/EEA: report to your lead supervisory authority (Art 56).

Document A — Notification to the Supervisory Authority (Article 33)

Complete every section. Sections 2–5 map to Article 33(3)(a)–(d) — the legal minimum content. The 72-hour clock runs from awareness (EDPB Guidelines 9/2022): the moment a responsible person concludes with reasonable certainty that personal data was compromised.

A.1 Filing details

To (supervisory authority)	*Competent authority; lead supervisory authority if cross-border (Art 56)*
From (controller)	*Legal entity name and registered address*
Incident reference	*Internal ID, e.g. BREACH-2026-007*
Notification type	*Initial / Update / Final (Art 33(4) phased notification)*
Filed (date & time)	*Timestamp of this filing*

A.2 Awareness and timing (Art 33(1))

Awareness timestamp	*When a responsible person concluded a breach had likely occurred — starts the 72-hour clock*
How we became aware	*Alert, processor notice under Art 33(2), customer report, audit finding…*
Reasons for delay	*MANDATORY if this filing is later than 72 hours after awareness; otherwise n/a*

A.3 Nature of the breach (Art 33(3)(a))

What happened	*Describe the incident and its cause; confidentiality, integrity and/or availability breach*
Categories of data subjects	*E.g. customers, employees, end-users of customers*
Approx. number of data subjects	*Number or range; update in later filings if it changes*
Categories of personal data	*E.g. contact data, credentials, financial data — flag special categories (Art 9) explicitly*
Approx. number of records	*Number or range*

A.4 Contact point (Art 33(3)(b))

DPO / contact point	*Name, role, email, phone — where the authority can obtain more information*

A.5 Likely consequences (Art 33(3)(c))

Likely consequences	*Realistic harms: identity theft, fraud, financial loss, reputational damage, exposure of special categories*

A.6 Measures taken or proposed (Art 33(3)(d))

Containment & remediation	*What has been done to address the breach*
Mitigation of adverse effects	*Measures reducing harm to data subjects, e.g. forced password reset, credential revocation*

A.7 Data-subject communication position

Risk assessment	*Unlikely risk / risk / high risk — with brief reasoning*
Article 34 position	*Communication sent or planned (date), or exception: 34(3)(a) unintelligible data, 34(3)(b) risk removed, 34(3)(c) public communication*

A.8 Cross-border processing (Art 56)

Cross-border?	*Are data subjects in more than one Member State affected?*
Lead authority basis	*Main-establishment reasoning identifying the lead supervisory authority*

Document B — Communication to Data Subjects (Article 34)

Required without undue delay when the breach is likely to result in a HIGH risk. Clear and plain language; must contain at least the contact point, likely consequences and measures (Art 34(2) → Art 33(3)(b),(c),(d)). Replace bracketed text; keep sentences short; avoid jargon.

Subject	*Important security notice about your personal data*
What happened	*[One or two plain-language sentences: what happened, when it was discovered and contained.]*
What information was involved	*[The categories of the recipient's data affected. State clearly what was NOT affected, e.g. payment data.]*
What this could mean for you	*[Realistic consequences — e.g. phishing emails that look like they come from us, attempted log-ins.]*
What we are doing	*[Containment, investigation, notification of the supervisory authority, security improvements.]*
What you can do	*[Concrete steps: reset your password, enable two-factor authentication, watch for suspicious emails, monitor statements.]*
Where to get more information	*[DPO / contact point: name, email, phone — and a status page if available.]*
Closing	*We apologise for the concern this incident may cause. We will keep you informed as our investigation progresses.*

Public-communication variant (Art 34(3)(c))

If contacting each data subject individually would involve disproportionate effort, publish the same content as a public communication (website banner, press notice) that informs data subjects in an equally effective manner — and record the channel choice and reasoning in Document C.

Document C — Internal Breach Log Entry (Article 33(5))

Complete one entry per incident — including breaches you decide NOT to notify. This register is how a supervisory authority verifies Article 33 compliance.

Incident reference	*Internal ID*
Awareness timestamp / how	*When the clock started and what triggered awareness*
Facts of the breach	*Nature, cause, data subjects and records affected*
Effects	*Actual and likely consequences observed*
Risk assessment & reasoning	*Unlikely risk / risk / high risk — and why*
Authority notified?	*Yes (date, reference) / No — reasoning: unlikely to result in a risk*
Data subjects notified?	*Yes (date, channel) / No — which Art 34(3) exception and why*
Processor notice (Art 33(2))	*Which processor informed us and when — if the breach originated at a processor*
Remedial action	*What was fixed, changed, or improved as a result*
Filings log	*Initial / update / final notifications: dates and references*

Document D — Notify-or-Not Decision Aid

Situation	*What you must produce*
Breach unlikely to result in a risk	*Document C only — log it with your reasoning*
Breach likely to result in a risk	*Document A within 72h + Document C*
Breach likely to result in a HIGH risk	*Document A + Document B without undue delay + Document C*
High risk, but data unintelligible (encrypted, keys safe) — Art 34(3)(a)	*Document A + Document C; no Document B*
High risk, but subsequent measures removed it — Art 34(3)(b)	*Document A + Document C; no Document B*
Individual letters = disproportionate effort — Art 34(3)(c)	*Document A + public communication + Document C*

The supervisory authority can order communication to data subjects under Art 34(4) even where you concluded it was not required. Fines for Art 33/34 infringements: up to EUR 10 million or 2% of total worldwide annual turnover (Art 83(4)(a)).