The GDPR 72-Hour Battle-Card

First hours of a personal-data breach under the General Data Protection Regulation (GDPR) — Article 33, the 72-hour clock, Article 34 individual notification, the do-not-touch list

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-09-03

Contents

The GDPR 72-Hour Battle-Card **1**

Page 1 — The 72-Hour Clock (Article 33) **2**
- First 30 minutes — Establish the awareness moment . . . 2
- Next 4 hours — Risk assessment . . . 2
- Hours 4–24 — Coordination . . . 3
- Hours 24–72 — Submission . . . 3
- Regulatory clocks at a glance . . . 3

Page 2 — Article 34 Individual Notification + Do-Not-Touch **4**
- When Article 34 individual notification applies . . . 4
- Required contents of the Article 34 individual notification . . . 4
- Do not touch — the six common mistakes . . . 4
- Five standards worth knowing by name . . . 5

Want the Full Triage? **5**

About This Guide **6**

The GDPR 72-Hour Battle-Card

A printable two-page reference for a Data Protection Officer (DPO), a fractional DPO, or a privacy lead handling a personal-data breach. Page one covers the first 72 hours under GDPR Article 33. Page two covers Article 34 individual notification and the do-not-touch list.

If you are reading this during an actual breach: scroll to the page that matches where you are. Take a slow breath. Work the list in order.

Page 1 — The 72-Hour Clock (Article 33)

First 30 minutes — Establish the awareness moment

1. **Record the awareness timestamp.** The 72-hour clock starts when you become aware of the breach. "Aware" means you have a reasonable degree of certainty that a breach affecting personal data has happened. It is not the moment of compromise. It is not the moment of discovery. It is the moment of reasonable certainty. Write the date and hour somewhere you cannot lose them. The European Data Protection Board (EDPB) Guidelines 9/2022 cover this in detail.
2. **Confirm scope: is it personal data?** Per Article 4(1), personal data is any information that relates to an identified or identifiable natural person. If the affected data is not personal data, Articles 33 and 34 do not apply.
3. **Determine your role: controller, processor, or both?** Processors must notify their controller "without undue delay" under Article 33(2). The 72-hour clock to the supervisory authority is the controller's, not the processor's.
4. **Engage the DPO and counsel.** Article 39 requires DPO involvement in personal-data incidents. Counsel typically reviews supervisory-authority submissions before they go.

Next 4 hours — Risk assessment

5. **Classify the data categories.** Some data categories push the risk assessment toward "high risk." Article 9 covers health, biometric, racial / ethnic origin, sexual orientation, religious beliefs, trade-union membership, and political opinions. Article 10 covers criminal-conviction data.
6. **Map the data subjects affected.** Get an approximate count. Get the approximate categories (customers, employees, prospects). The EDPB severity matrix considers volume, sensitivity, and identifiability together.
7. **Assess the risk to data subjects.** The EDPB uses a three-band framework:
    - **High risk**: likely material consequences (financial loss, identity theft, discrimination, reputational damage). Triggers Articles 33 AND 34.
    - **Risk but not high risk**: Article 33 only.
    - **Unlikely to result in a risk**: internal documentation under Article 33(5) only. No notification.
8. **Check the Article 34(3) exemptions.** Even a high-risk breach may not require individual notification if one of these applies:
    - **(a)** The affected data was rendered unintelligible (for example: strong encryption with uncompromised keys).
    - **(b)** Subsequent measures eliminate the high risk.
    - **(c)** Individual notification would involve disproportionate effort. A public communication can substitute.

Hours 4–24 — Coordination

9. **Identify the lead supervisory authority (SA).** Cross-border breaches involve data subjects in multiple Member States. The EDPB one-stop-shop mechanism applies. You notify the SA of your main EU establishment. That SA then coordinates with concerned supervisory authorities.
10. **Begin drafting the Article 33(3) notification.** Four required contents:
    - **(a)** Nature of the breach, plus categories, plus approximate numbers.
    - **(b)** DPO contact details.
    - **(c)** Likely consequences.
    - **(d)** Measures taken or proposed. Article 33(4) explicitly permits notification in phases. The initial submission can be partial.
11. **Begin drafting the Article 34 individual notification** (if applicable). It must describe the breach in clear and plain language. It must include the DPO contact details, the likely consequences, and the measures taken or proposed.
12. **Preserve evidence.** Forensic preservation supports both the SA's investigation and any later litigation.

Hours 24–72 — Submission

13. **Submit the Article 33 notification to the lead supervisory authority.** Use the SA's prescribed channel (online portal, secure email). Article 33(4) permits phased submission. The initial filing can be partial as long as further information follows without undue delay.
14. **If notifying data subjects under Article 34**, time the communication to coincide with or follow the supervisory notification. Your SA may have a view on sequencing.
15. **Document everything under Article 33(5).** Even for non-notifiable breaches, document the facts, the effects, and the remedial action. The SA may inspect this record.

Regulatory clocks at a glance

Window	Trigger	Notes
Without undue delay	Processor → controller notification (Art. 33(2))	Processor obligation. Upstream of the 72-hour clock.
72 hours	Controller → supervisory authority (Art. 33(1))	From awareness, not from incident.
Without undue delay	Controller → data subjects (Art. 34(1))	Only when "likely to result in a high risk."
One month	Final supplementary information (if filed in phases)	EDPB guidance. Not a hard statutory deadline.

Page 2 — Article 34 Individual Notification + Do-Not-Touch

When Article 34 individual notification applies

Article 34(1) requires the controller to tell the data subject about the breach "without undue delay" when the breach is "likely to result in a high risk to the rights and freedoms of natural persons."

The Article 34(3) exemptions:

Exemption	What it means in practice
(a) Data rendered unintelligible	Strong encryption at rest with uncompromised keys. Or effective pseudonymisation. The supervisory authority may still disagree. Verify with counsel.
(b) Risk eliminated	Subsequent measures have made the high risk no longer likely. For example: the attacker's access was blocked before they exfiltrated data.
(c) Disproportionate effort	A public communication or similar measure can substitute. Used sparingly. Always consult the SA first.

Required contents of the Article 34 individual notification

- **Plain-language description of the nature of the breach.**
- **DPO contact details.**
- **Likely consequences for the individual.**
- **Measures taken or proposed by the controller.**
- **Optionally** but commonly: what the individual can do (change password, monitor financial statements, freeze credit, contact specific support).

Tone matters. The Article 34 communication is consumer-facing. Counsel's review is non-negotiable.

Do not touch — the six common mistakes

- **Do not delay the 72-hour notification to wait for complete information.** Article 33(4) explicitly permits notification in phases. A partial timely notification beats a complete late one.
- **Do not assume the 72-hour clock starts at incident discovery.** It starts at awareness per EDPB Guidelines 9/2022. Awareness means reasonable certainty that a breach affecting personal data occurred.
- **Do not notify the wrong supervisory authority.** For cross-border breaches, your lead SA is the SA of your main EU establishment. Use the one-stop-shop mechanism.
- **Do not over-disclose to data subjects without counsel.** The Article 34 notification has specific required contents. Broader detail can create unnecessary exposure.
- **Do not destroy logs, original evidence, or compromised systems.** Forensic preservation supports both the SA's investigation and any later litigation.

- **Do not assume encryption is a complete defence under Article 34(3)(a).** The encryption must have rendered the data unintelligible. The keys must not have been compromised. The supervisory authority may still disagree.

Five standards worth knowing by name

The recommendations above are drawn from these. Knowing the names, not the contents, is enough for the first 72 hours.

1. **General Data Protection Regulation: Regulation (EU) 2016/679**, Articles 33 (notification to supervisory authority) and 34 (communication to data subjects). The statutory text is short. It is worth reading directly.
2. **EDPB Guidelines 9/2022** on personal-data-breach notification under Regulation 2016/679. The single most useful interpretation source. It includes the severity matrix and worked examples.
3. **EDPB Guidelines 02/2019** on Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Less directly applicable to breach response. Still useful for risk assessment.
4. **ENISA Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches.** The de facto severity-scoring methodology.
5. **The supervisory authority's own breach-notification guidance.** Every SA publishes its own. Your lead SA's guidance takes precedence over generic interpretation.

Want the Full Triage?

The free GDPR Breach Response Triage at *gdprbreach.sylvanassurance.com* asks nine questions about your current breach. It returns:

- A notifiable-or-document verdict (notify both / notify SA only / borderline / document only).
- A deadline countdown from your awareness time.
- The Article 33(3) required contents tailored to your situation.
- A starter notification draft your DPO can hand to counsel.
- A do-not-touch list.

It runs entirely in your browser. Your answers are never transmitted.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience translated into plain-language guidance for small business owners.

It provides **general guidance and recommended practices**. It is **not** legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common risk. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the GDPR Breach Response.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-gdpr-breach-response

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/gdpr-compliance