FREE GUIDE

The GDPR Breach Battle-Card — Your First 72 Hours

Five plain-English moves for the first three days of a personal-data breach, while the clock is running.

When personal data is lost, exposed, or locked, the General Data Protection Regulation (GDPR) can put you on a 72-hour clock. This card is the first three days in plain English — what to do first, what not to touch, and the two notification decisions that matter. It's general guidance, not legal advice.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Move 1 — Start the clock and write down when you knew

What it is

Recording the moment you became "aware" that a personal-data breach likely happened.

Why it's first

The 72-hour notification clock under Article 33 of the General Data Protection Regulation (GDPR) starts when you become aware — not when you finish investigating. The time you write down here anchors every deadline that follows, so capture it precisely.

Do this

Note the date and time you became aware, and who reported it. Open a simple running log now — every action, with timestamps. You'll need this record whether or not you end up notifying anyone.

Move 2 — Contain it without destroying the evidence

What it is

Stopping the bleeding — while preserving what you'll need to understand what happened.

Why it matters

The instinct to "wipe it and move on" can destroy the logs and artefacts you need to assess risk and report accurately. Contain, but don't scrub.

Do this

Cut off the exposure (revoke access, isolate the system, reset credentials) but don't delete logs or reimage machines yet. Capture the do-not-touch items: the relevant logs, the affected data, and a snapshot of the system as found.

Move 3 — Decide whether it's a personal-data breach, and how risky

What it is

A quick, documented assessment of what data was involved and how much harm it could cause.

Why it matters

Your two notification decisions both turn on risk. Not every security incident is a notifiable personal-data breach — but you must assess and record the call, not assume.

Do this

Write down what data was affected, whose, how much, and the likely harm (identity theft, financial loss, distress). This risk judgement decides Moves 4 and 5.

Move 4 — Notify the supervisory authority if required (Article 33)

What it is

Reporting the breach to your supervisory authority — the data-protection regulator for your country — usually within 72 hours.

Why it matters

Unless the breach is unlikely to result in a risk to people's rights and freedoms, Article 33 requires notifying your supervisory authority — and being late without a good reason is itself a problem.

Do this

If there's a risk, notify your supervisory authority within 72 hours of awareness. If you don't have every detail yet, notify on time with what you know and follow up — a phased notification is allowed. If you decide not to notify, record why.

Move 5 — Tell the affected people if the risk is high (Article 34)

What it is

Communicating the breach directly to the individuals whose data was involved.

Why it matters

When a breach is likely to result in a high risk to people, Article 34 requires telling them, in plain language, without undue delay — so they can protect themselves.

Do this

If the risk to individuals is high, tell them clearly: what happened, what data, what you're doing, and what they can do (reset passwords, watch statements). Keep the message plain and free of jargon.

Where to go from here

The free GDPR Breach assessment helps you gauge your readiness in a few minutes, and it runs entirely in your browser, so we never see your answers: sylvanassurance.com/free/gdpr-breach/

When you're ready for the full breach playbook — decision trees, notification templates, and the operational detail — the GDPR Breach Response toolkit lays it out: sylvanassurance.com/gdpr-breach-response

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-gdpr-breach-response