Data breach response plan template

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

1. Purpose, scope and breach team

This plan applies when personal or regulated data may have been accessed, disclosed, lost or altered without authority, at [Organization name] or at a supplier that holds our data.

- Breach team: incident lead [name]; privacy lead [name]; legal counsel [name]; communications lead [name]; technical lead [name]; executive sponsor [name]; each with a named deputy.
- The team has authority to [take systems offline, suspend accounts, engage outside experts] without further approval.

2. Discover, report and contain

Anyone who suspects a breach reports it at once. The incident lead records the time of discovery.

1. Record the date and time the breach was first known, and who knew.
2. Stop the exposure: revoke access, take down the page or share, recover the device or message where possible.
3. Preserve logs and evidence. Do not wipe systems yet.
4. Open the log and the decision record.

3. Assess the breach

Answer these questions, in writing, as soon as the facts allow. Update the answers as the investigation develops.

- What data: types of data and, for each, the number of people and records.
- Whose data: customers, employees, patients, students, children; which countries and states.
- How: cause and whether the breach is still happening.
- Was the data protected, for example by strong encryption, so that it is unintelligible to unauthorized people?
- Who has it: an unknown actor, a known recipient, a supplier, a misdirected email.
- What harm could follow: fraud, identity theft, physical or reputational harm, discrimination.

4. Decide who must be told

The privacy lead and counsel complete this table within [24 hours] of discovery and revisit it daily.

Recipient	Test for notifying	Deadline	Decision, time and owner
Supervisory authority or regulator	[rule and test from section 10 of the plan]	[deadline]	
Affected individuals	[rule and test]	[deadline]	
Customers whose data we process	[contract clause]	[deadline]	
Insurer	[policy clause]	[deadline]	

Recipient	Test for notifying	Deadline	Decision, time and owner
Law enforcement	[when advised by counsel]	n/a	
Payment brands, banks, other contractual parties	[contract clause]	[deadline]	

Examples of tests, each from the source named on this site: GDPR Article 33 (72 hours to the authority unless the breach is unlikely to result in a risk), Article 34 (communicate to individuals when likely to result in a high risk), HIPAA 164.404 (60 days to individuals), FTC Safeguards Rule 314.4(j) (30 days to the FTC for 500 or more consumers).

5. Write the notice

Use plain language. Include the same minimum content for every audience, then add what the audience needs.

- What happened, with dates, and when it was discovered.
- The categories and approximate number of people and records involved.
- The likely consequences.
- What we have done and are doing, including steps to limit harm.
- What recipients should do to protect themselves.
- How to ask questions: name or role, phone, email, website or postal address.

GDPR Article 33(3) lists the elements on what happened, the categories and numbers, the likely consequences, the measures taken and the contact point. The element on what recipients should do to protect themselves comes from 45 CFR 164.404(c)(1)(C); GDPR reaches it only through the mitigation measures in Article 33(3)(d) and Article 34(2).

6. Support affected people

Decide what help to offer and who delivers it.

- Dedicated phone line or mailbox: [details], staffed [hours].
- Offers such as credit monitoring or identity protection where the data supports a need: [offer, provider, duration].
- A frequently asked questions page, updated daily until closure.

7. Document and review

Document every breach, even one that is not reported to anyone.

- Record the facts, the effects and the remedial action, in a form that lets a regulator check compliance (GDPR Article 33(5)).
- Hold a review within [10 business days] of closure: cause, controls that failed, what to change, owners and dates.
- Update the plan, the notice templates and the training.