GDPR DATA BREACH RESPONSE TEMPLATE

a

PRIVALEX

guide

FIRST THINGS FIRST...

A data breach is every company's nightmare. Under the GDPR, you must:

- ✓ Detect and assess breaches quickly.
- ✓ Notify the supervisory authority within 72 hours if the breach poses a risk to individuals.
- ✓ Communicate with affected users if the risk is high.

This template gives you a ready-to-use structure for documenting, and managing breaches.

INCIDENT IDENTIFICATION & INITIAL REPORT

Template Log Entry:

- **Date/Time Detected:** *Insert date and time*
- **Reported By:** *Name/Department*
- **How Identified:** *Monitoring system, employee report, client notification, etc.*
- **Description of Incident:** *Brief explanation of what happened*
- **Systems/Data Involved:** *e.g., CRM, email, payment database*

CONTAINMENT & MITIGATION

Checklist:

- ☐ Isolate affected systems.
- ☐ Disable compromised accounts/access points.
- ☐ Preserve evidence (logs, screenshots, alerts).
- ☐ Engage IT/security to confirm scope.

Note: ***Describe immediate measures taken to stop or reduce the impact.***

BREACH ASSESSMENT

Questions to Answer:

What type of personal data is involved?

How many data subjects are affected?

Is there sensitive data?

Is the data encrypted or otherwise protected?

What are the potential consequences for individuals?

(identity theft, financial loss, reputational harm)

Risk Rating *(check one):*

☐ LOW
The incident is unlikely to cause harm to individuals. Data was limited, well protected (e.g. encrypted), or quickly contained, with no real impact expected on data subjects.

☐ MEDIUM
The incident could cause some inconvenience or limited harm to individuals. Data is personal but not highly sensitive, or mitigating measures reduce the likelihood of serious impact.

☐ HIGH
The incident is likely to cause significant harm to individuals, such as identity theft, financial loss, or serious reputational damage. Sensitive data is involved or the data is exposed without effective protection.

NOTIFICATION DECISION (72-HOUR RULE)

1.

Notify Supervisory Authority?

☐ Yes ☐ No

Required if the breach is likely to result in a risk to the rights and freedoms of individuals. Must be notified within 72 hours of becoming aware of the breach.

2.

Notify Data Subjects?

☐ Yes ☐ No

Required if the breach is affecting the individuals and their data privacy rights directly. Notification must be made without undue delay and in clear, plain language.

Risk is:

LOW
No notification necessary

MEDIUM
Authority notification only

HIGH
Authority + individuals notification

REGULATORY NOTIFICATION TEMPLATE

TO SUPERVISORY AUTHORITY

- ✓ Nature of the breach
- ✓ Categories and approximate number of data subjects affected
- ✓ Categories and approximate number of personal data records concerned
- ✓ Likely consequences of the breach
- ✓ Measures taken or proposed to address/mitigate breach
- ✓ Contact details of DPO or responsible person

TO DATA SUBJECTS

Subject: *Important Notice About Your Personal Data*

Message: *We recently identified a security incident that may have affected your personal data. The information involved was *describe categories*.*

*We have taken immediate steps to contain the issue and prevent recurrence, including *describe measures*.*

*What you can do: *e.g., reset your password, monitor accounts*.*

*If you have questions, you can contact our Data Protection Officer at *email/DPO contact*.*

We sincerely apologize for the inconvenience and take our responsibility to protect your data seriously.

POST-INCIDENT REVIEW

Template Fields:

- **Root Cause Analysis:** *Explain*
- **Lessons Learned:** *List key takeaways*
- **Corrective Actions:** *Update policies, training, or technical controls*
- **Responsible Owner:** *Assigned person/team*
- **Deadline for Actions:** *Insert date*

QUICK REFERENCE CHECKLIST

- [ ] Detect and document the breach
- [ ] Contain and mitigate damage
- [ ] Assess risk to individuals
- [ ] Notify authority within 72h (if required)
- [ ] Notify individuals without undue delay (if high risk)
- [ ] Document everything (even if no notification is required)
- [ ] Conduct a post-incident review

WHAT'S NEXT?

Most companies lose precious time in a breach because they don't know who does what. Having a clear template avoids panic and shows regulators you take compliance seriously.

Don't wait until a breach happens. Contact us to get a customized breach response pla aligned with your sector and risks.

GET IN TOUCH

PRIVALEX