

GDPR Breach Notification Checklist

Preparing for a Breach

- Understand “Personal Data Breach”**
Involves the destruction, loss, alteration, or unauthorized disclosure of/access to personal data.
- Locate and Document Data**
Identify where personal data is stored and document controls to prevent unauthorized access.
- Implement Preventive and Monitoring Controls**
 - Ensure security hygiene, conduct tests, and monitor networks.
 - Set up breach alerts for the 72-hour reporting requirement.
- Perform Incident Response Tests**
Test the incident response plan so employees know their roles.

Responding to a Breach

- Identify the Extent of the Breach**
Determine the type, disclosed information, and affected data subjects.
- Report to Appropriate Entities**
Processors report to the EU company; controllers report to the regulatory body.
Notify data subjects if the breach poses a high risk, unless safeguards (e.g., encryption) are in place.
- Report Correct Information**
 - Report to the authority within 72 hours, including:
 - Breach details
 - Data protection officer's contact
 - Likely consequences
 - Mitigation measures

