Practitioners' Checklist
Data Breach

This checklist is intended as a practical tool to help brand owners and practitioners prepare for, respond to, communicate during, and mitigate the impact of a personal data breach. Applicable legal, regulatory, contractual, and notification requirements should be assessed for each relevant jurisdiction and incident.

Prevention

Governance and Internal Responsibility

- Designate internal personnel responsible for data protection and incident response.
- Clearly define and document roles and responsibilities for data protection and incident response.
- Limit the collection of personal data to what is necessary for legitimate purposes.

Awareness and Employee Training

- Provide regular data protection and information security training to personnel.
- Educate personnel on the risks and consequences of data breaches.
- Implement ongoing awareness initiatives to reinforce good data handling practices.
- Maintain records of training and awareness activities.

Security Measures and Frameworks

- Adopt and maintain appropriate information security measures.
- Adopt and follow an appropriate information security and data privacy framework.
- Regularly review and update security controls.
- Ensure software, operating systems, and applications are updated and patched in a timely manner.

Monitoring and Detection

- Implement mechanisms to detect, identify, and classify potential security incidents and data breaches.
- Monitor internal and external sources that may indicate a potential breach.
- Establish procedures for investigating alerts and suspicious activity.
- Provide employees with clear channels for reporting suspected security incidents or privacy concerns.
- Encourage employees to report suspicious activity, including:
  - Suspicious emails
  - Unauthorized access attempts
  - Unusual system activity

Third-Party Vendors and Contractual Safeguards

- Identify vendors that collect, process, store, or access personal data.
- Require vendors to maintain appropriate security measures and comply with applicable privacy laws.
- Include data protection obligations in relevant contracts.
- Require vendors to support the organization in the event of a security incident or data breach.
- Conduct periodic vendor assessments or audits.
- Assess data protection controls before engaging new vendors or service providers.

Internal Breach Protocols and Procedures

- Maintain a written data breach response protocol.
- Define procedures for escalating, investigating, and managing security incidents and data breaches.

- Establish a multidisciplinary incident response or crisis management team.
- Clearly define and document team members' roles and responsibilities in the response protocol.
- Identify legal, regulatory, contractual, and insurance notification requirements.
- Define response timelines to ensure prompt action and compliance.
- Ensure key stakeholders can be contacted quickly during a security incident.

Risk and Impact Assessments

- Conduct periodic risk assessments relating to personal data processing.
- Conduct data protection impact assessments where appropriate.
- Identify key risks and implement mitigation measures.
- Regularly test and update plans for preventing, responding to, and mitigating identified risks.

Communication Preparedness

- Develop a communication plan for potential data breach scenarios.
- Train communication and public relations personnel on crisis response procedures.
- Prepare template communications for:
  - Regulators
  - Affected individuals
  - The public
- Establish approval procedures for external communications.
- Define in advance the roles responsible for managing internal and external communications during a data breach.

Legal Compliance

- Monitor applicable privacy and data protection laws.
- Review and update privacy policies and internal procedures as legal requirements evolve.
- Ensure compliance obligations are documented and regularly reviewed.

Response

Activate the Data Breach Protocol and Coordinate the Response

- Activate the established incident response protocol and response team.
- Coordinate all relevant internal teams under the direction of executive management.
- Inform relevant internal teams of the incident as soon as possible and share the available verified information needed to coordinate the response.
- Involve the legal, data protection, or equivalent privacy function from the outset.

Stop and Contain the Breach

- Take immediate action to contain, minimize, and stop the breach as soon as it is discovered.
- Verify that unauthorized access has been terminated and that the immediate threat has been contained.
- Implement appropriate technical containment measures, such as:
  - Isolating compromised systems or accounts
  - Blocking unauthorized access
- Identify and engage the appropriate internal or external support for containment, as needed.

Engage External Support and Preserve Evidence

- Assess whether external digital forensic or cybersecurity experts should be engaged.
- Preserve relevant evidence before remediation, where appropriate.

Analyze and Investigate the Breach

- Gather the facts about the breach, including its cause and consequences, as soon as possible.
- Establish the key facts of the security incident, including:
  - The date and time the incident began
  - The date and time of discovery and resolution
  - The circumstances in which the incident was discovered
  - The nature of the incident
  - The geographical impact
  - The actions taken to stop, contain, and mitigate the breach
- Establish the scope of the data breach, including:
  - The number of data subjects involved
  - The categories of data subjects involved
  - The types of personal data affected
- Assess whether vulnerable individuals may be affected, such as:
  - Children
  - People with disabilities
  - The elderly
  - Patients
  - Other vulnerable individuals
- Assess whether sensitive or highly confidential personal data are affected, such as:
  - Political opinions
  - Religious beliefs
  - Biometric data
  - Health data
  - Bank details
  - Identity documents
  - Geolocation data
  - Data relating to legal actions
- If the incident was discovered late, gather evidence explaining the delay.

Log and Document the Breach

- Document the analysis and investigation of the incident, including the measures taken to contain and mitigate the breach.
- Retain the documentation relating to the breach and the response.

Assess and Carry Out Regulatory Notification

- Determine whether the relevant regulatory authority must be notified of the breach.
- Verify the applicable notification requirements, thresholds, and deadlines, including any sector-specific or local requirements, in each relevant jurisdiction.
- Prepare the notification with the required information, including, as applicable:
  - The origin and consequences of the breach
  - The security measures in place before the breach

- The security measures implemented after the breach

Assess and Carry Out Notification to Affected Data Subjects

- Determine whether the affected individuals must be notified of the breach.
- Verify the applicable notification requirements, thresholds, and deadlines in each relevant jurisdiction.
- Determine the appropriate means of notification in accordance with the applicable requirements.
- Draft the notification in clear and understandable terms, including, as applicable:
  - The origin and likely consequences of the breach
  - Relevant contact information

Assess Disclosure to Other Authorities and Third Parties

- Identify any applicable obligation to notify cybersecurity authorities.
- Determine whether the incident should or must be reported to the appropriate law enforcement authorities.
- Identify third parties that may need to be informed of the breach.
- Review contractual notification obligations, including, as applicable, those arising from:
  - Insurance policies
  - Agreements with service providers or other business partners

Address Insurance Considerations

- Identify any insurance policies that may apply to the breach.
- Review applicable insurance requirements before engaging external providers or incurring response costs.
- Notify applicable insurers in accordance with the relevant policy requirements and deadlines.

Manage Breaches Originating with Third-Party Vendors

- Determine whether the breach originated with a vendor, processor, or other service provider and, where applicable, coordinate the response with that third party.
- Activate applicable contractual notification and cooperation obligations with the third-party vendor.

Communication

Internal Communication

- Immediately activate the established internal communication and approval process.
- Confirm the designated spokesperson for the incident.
- Ensure that relevant internal teams receive timely, verified, and consistent information throughout the incident.

External Communication

- Route external inquiries to the designated spokesperson or point of contact.
- Follow the established approval process for external communications.
- Identify the relevant external stakeholders to be addressed, depending on the nature and impact of the breach.
- Communicate the breach promptly to relevant external stakeholders, where appropriate, and consider whether communication should occur before the breach becomes public through third parties.
- Ensure consistent external messaging through the designated spokesperson or authorized communication channels.

- Communicate the steps being taken to address the breach and prevent similar incidents.
- Coordinate the timing and content of external communications with any applicable legal or regulatory notifications.

Consistency and Accuracy of Messaging

- Provide clear, accurate, balanced, and transparent information based on verified facts and available records.
- Ensure consistency between internal and external communications and any applicable regulatory notifications.

Manage Inquiries and Ongoing Communications

- Establish appropriate channels for inquiries from affected individuals, media, and other relevant stakeholders.
- Prepare FAQs and other response materials to ensure clear and consistent responses to inquiries.
- Brief staff handling inquiries on approved responses and escalation procedures.
- Monitor media and social media coverage and address significant inaccuracies where appropriate.
- Review and update communications as new verified information about the breach becomes available.
- Coordinate the organization’s public and media response if the breach becomes public.
- Maintain a record of inquiries and complaints received and the responses provided.

Mitigation

Remediation Measures

- Address the root cause of the breach identified during the incident investigation.
- Replace compromised or potentially compromised credentials, keys, and certificates.
- Rebuild or restore compromised systems from trusted and verified sources, where appropriate.
- Identify and address related vulnerabilities across relevant systems and networks.
- Review and strengthen access controls, including, where appropriate:
  - Least-privilege access
  - Multi-factor authentication
  - Removal of unauthorized accounts or access mechanisms
- Verify that backups are not compromised before using them for recovery.
- Conduct appropriate vulnerability assessments and security testing, such as:
  - Vulnerability scans
  - Penetration testing
- Consider appropriate remedial or support measures for affected individuals, depending on the nature and impact of the breach, such as:
  - Credit monitoring
  - Identity protection services
  - Other appropriate assistance

Lessons Learned

- Prepare a post-incident review report documenting the incident, the response and remediation measures taken, and the lessons learned, and share relevant findings with appropriate internal teams.
- Conduct a post-incident review with the relevant internal stakeholders within an appropriate time frame after closure of the incident.

- Identify what worked well, what did not, and why, during the detection, response, and remediation of the breach.
- Identify gaps or weaknesses in systems, processes, tools, procedures, and staff training revealed by the incident.
- Assess whether detection and response times met the organization’s established incident response targets or procedures.
- Assess and document the financial, operational, and reputational impact of the breach, including relevant breach-related costs.

Actions to Reduce the Risk of Future Incidents

- Update incident response and recovery procedures based on lessons learned from the incident.
- Update the organization’s risk assessments and, where applicable, its risk register based on the incident findings.
- Address systemic weaknesses identified through the post-incident review by updating and implementing appropriate policies, procedures, technical measures, and organizational controls.
- Continue monitoring systems and networks for risks related to the incident and the remediation measures implemented.
- Update security monitoring and awareness training based on risks and weaknesses identified through the incident.
- Regularly test the incident response plan through tabletop exercises or other appropriate exercises.
- Review and update third-party risk management procedures based on lessons learned from the incident.
- Review whether existing insurance coverage remains appropriate in light of the incident.
- Periodically review and update the incident response checklist and related procedures.