Bader Malan Limited Security Breach Notification Process

Bader Malan Limited
Neville House, 17 Richmond Close, Bookham Nr. Leatherhead
Surrey KT22 9NX
Email: Info@badermalan.co.uk
Company Registration Number 4329913

1. Purpose

The purpose of this process is to ensure that Bader Malan Ltd responds promptly and effectively to any information security breaches, minimizing harm to individuals and the organization. This process outlines the steps for detecting, reporting, managing, and notifying relevant parties of a data breach in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Definition of an Information Security Breach

An **information security breach** is any incident that leads to the unauthorized access, disclosure, alteration, loss, or destruction of personal data or other sensitive information. Examples include, but are not limited to:

- Hacking or cyber attacks
- Loss or theft of data or equipment
- Unintentional disclosure of information
- Human error (e.g., sending an email to the wrong recipient)
- Insider threats (e.g., misuse of access privileges)

3. Roles and Responsibilities

- **Employees:** All employees are responsible for reporting any suspected or actual data breaches immediately.
- **Information Security Officer (ISO):** The ISO is responsible for coordinating the breach response, including containment, investigation, and notification.
- **Data Protection Officer (DPO):** The DPO ensures compliance with legal obligations and assists in evaluating the risk and necessity of notifying the Information Commissioner's Office (ICO) and affected individuals.
- **IT Team:** The IT team assists in identifying, containing, and mitigating the breach and preventing future occurrences.

4. Breach Detection and Reporting

- **Immediate Reporting:** All employees must immediately report any suspected or actual information security breaches to their line manager and the Information Security Officer (ISO).
- **Initial Assessment:** The ISO will conduct a preliminary assessment to determine the nature, cause, and potential impact of the breach. If personal data is involved, the ISO will inform the Data Protection Officer (DPO).

5. Breach Management and Containment

Upon confirmation of a breach, the following steps will be taken:

1. **Containment:** Take immediate steps to contain the breach (e.g., disconnect affected systems from the network, change access credentials, or apply patches).

2. **Mitigation:** Identify and mitigate risks associated with the breach to prevent further damage (e.g., recover lost data, fix vulnerabilities).
3. **Investigation:** Conduct a thorough investigation to determine the cause, extent, and impact of the breach. Document all findings and actions taken.
4. **Recovery:** Develop and implement a recovery plan to restore normal operations as soon as possible.

6. Risk Assessment

Evaluate the potential impact of the breach on affected individuals, considering:

- The type and sensitivity of the data involved
- The potential harm to individuals (e.g., financial loss, identity theft, reputational damage)
- The volume of data affected
- Whether the data was encrypted or otherwise protected

7. Notification Requirements

If the breach is likely to result in a risk to the rights and freedoms of individuals, the following notifications must be made:

1. **Notification to the Information Commissioner's Office (ICO):**
    - **Timing:** Notify the ICO within 72 hours of becoming aware of the breach, where feasible.
    - **Content:** The notification must include:
        - A description of the nature of the breach, including categories and approximate number of affected individuals and data records.
        - Contact details of the DPO or other relevant contact.
        - A description of the likely consequences of the breach.
        - A description of the measures taken or proposed to address the breach and mitigate its effects.
2. **Notification to Affected Individuals:**
    - If the breach is likely to result in a high risk to the rights and freedoms of individuals, notify the affected individuals without undue delay.
    - **Content:** The notification should include:
        - A description of the nature of the breach.
        - The likely consequences of the breach.
        - Contact details for the DPO or relevant contact.
        - The measures taken or proposed to address the breach and mitigate its effects.
    - If direct notification is not possible, consider alternative methods such as public communication.

8. Internal Reporting and Documentation

- **Internal Reporting:** All breaches, regardless of their impact, must be documented in the company's Breach Register. The register should include details of the breach, its impact, and the actions taken.
- **Post-Incident Review:** Conduct a post-incident review to identify lessons learned and improve security measures and breach response procedures.

9. Training and Awareness

- **Employee Training:** All employees must receive regular training on information security and the importance of reporting breaches promptly.
- **Awareness Campaigns:** Periodically conduct awareness campaigns to reinforce the importance of information security and breach reporting.

10. Monitoring and Review

This process will be reviewed annually or sooner if required by changes in legislation or circumstances to ensure it remains effective and compliant with legal requirements.

11. Contact Information

For any questions or concerns regarding this process, please contact:

- **Information Security Officer (ISO):** Louise Nelligan at louise@badermalan.co.uk
- **Data Protection Officer (DPO):** Mike Nelligan at Mike@badermalan.co.uk

---

Approval and Implementation
This policy is approved by the Board of Directors and is effective as of 14th August 2024.

Louise Nelligan
Director