

DATA BREACH RESPONSE AND NOTIFICATION POLICY

DORNAN
A Turner Company

LCD
COMPLIANCE YOU CAN TRUST

CONTENTS

1. PURPOSE 2
2. SCOPE 2
3. DEFINITIONS 2
4. RESPONSIBILITIES 2
5. BREACH IDENTIFICATION AND REPORTING 3
6. INVESTIGATION AND RISK ASSESSMENT 3
7. NOTIFICATION PROCEDURES 3
8. DOCUMENTATION AND RECORD-KEEPING 4
9. PREVENTIVE MEASURES 4
10. POLICY REVIEW AND MAINTENANCE 4
11. CONTACT INFORMATION: 4

DATA BREACH RESPONSE AND NOTIFICATION POLICY

1. PURPOSE

The purpose of this Data Breach Response and Notification Policy (the "Policy") is to establish the procedures and responsibilities for identifying, reporting, and responding to data breaches to ensure compliance with the General Data Protection Regulation (GDPR) and other applicable laws.

2. SCOPE

This Policy applies to all employees, sub-contractors, and third-party service providers who handle/process personal data on behalf of Dornan.

3. DEFINITIONS

Personal Data: Any information relating to an identified or identifiable natural person.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Officer (DPO): The designated individual responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

4. RESPONSIBILITIES

- Employees and Business Partners: Report any suspected data breaches immediately to the DPO.
- DPO: Lead the breach investigation, assess the risk, notify relevant authorities and affected individuals, and document the incident.
- IT Department: Assist in breach containment and recovery efforts and implement technical measures to prevent future breaches.

5. BREACH IDENTIFICATION AND REPORTING

Immediate Reporting: Any individual who suspects a data breach must report it immediately to the DPO using the SysAid via the Legal, Compliance, & Data Protection page on Dornet Submit Request - SysAid Help Desk Software

Initial Assessment: The DPO will conduct an initial assessment to determine if a data breach has occurred.

6. INVESTIGATION AND RISK ASSESSMENT

Containment and Recovery: The IT Department, in collaboration with the DPO, will take immediate steps to contain the breach and recover any lost data.

Risk Assessment: The DPO will assess the potential impact of the breach on data subjects, considering factors such as but not limited to the type of data, its sensitivity, and the number of affected individuals.

7. NOTIFICATION PROCEDURES

Supervisory Authority Notification: If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO will notify the relevant supervisory authority within 72 hours of becoming aware of the breach.

Notification Content: Description of the breach, categories and approximate number of data subjects and records concerned, likely consequences, and measures taken or proposed to address the breach.

Affected Individuals Notification: If the breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify affected individuals without undue delay.

Notification Content: Nature of the breach, contact details of the DPO, likely consequences, and measures taken or proposed to address the breach and mitigate its adverse effects.

8. DOCUMENTATION AND RECORD-KEEPING

- **Incident Log**: All data breaches, regardless of their impact, must be documented in the Privacy Risk Register.
- **Report Contents**: Date of the breach, nature and cause of the breach affected data, response actions, notifications made, and preventive measures taken.

9. PREVENTIVE MEASURES

- **Training**: Regular data protection training for all employees.
- **Security Measures**: Implementation of technical and organisational measures to protect personal data against breaches.
- **Policy Review**: Regular review and update of this Policy to ensure its effectiveness and compliance with regulatory requirements.

10. POLICY REVIEW AND MAINTENANCE

This Policy will be reviewed annually or after any significant data breach incident to ensure its effectiveness and compliance with GDPR and other applicable laws

This Policy ensures that Dornan is prepared to respond promptly and effectively to data breaches, minimising potential harm and maintaining compliance with GDPR requirements.

11. CONTACT INFORMATION:

Legal, Compliance, &, Data Protection Department
DPO
Unit 6,
East Gate Avenue,
Eastgate
Little Island,
Cork
T45 YW71
Dpo@dornangroup.com