Data Protection Breach Procedure Policy

Purpose of procedure

The purpose of this document is to provide a structured procedure for responding to incidents that result in the loss of personal data for which Tricel is the data controller. It is designed to be used alongside the Information Security Incident Response Procedure, which outlines the comprehensive approach to managing incidents affecting Lowara Distribution Ireland's information security. This document ensures compliance with the EU General Data Protection Regulation 2016 (GDPR), which mandates that any data breach likely to pose a risk to the rights and freedoms of data subjects must be reported to the relevant supervisory authority within 72 hours of detection.

IFS Template Reference: 1553318 Revision: 1

Name of Policy	Data Protection Data Subject Request Procedure
Lowara Site	50 Broomhill Close, Tallaght, Dublin 24, D24 APP8, Ireland
Applicable Policies	Data Protection Policy Data Protection Impact Assessment Procedure Data Subject Request Procedure
Last Updated	23/06/2025

Lowara Distribution Ireland Data Protection Breach Procedure Policy

Tricel (Baldonnell) Ltd, trading as Lowara Distribution Ireland (hereinafter referred to as "Lowara Distribution Ireland" or "the Company"), is a company registered in Ireland under registration number IE497442, with its registered office at 50 Broomhill Close, Tallaght, Dublin 24, D24 APP8, Ireland.

This procedure offers guidance on assessing the risk associated with a data breach, determining whether notification to the supervisory authority or affected data subjects is required, and executing the notification process in a timely and effective manner. It emphasises the importance of using common sense and professional judgment in handling incidents, as the precise impact of a breach can vary.

The document serves as a framework to help Lowara Distribution Ireland fulfil its GDPR obligations by detailing the steps for notifying the supervisory authority and data subjects, documenting the breach, and taking appropriate remedial actions. The procedure aims to protect the rights and freedoms of data subjects while ensuring that Lowara Distribution Ireland responds to data breaches promptly and effectively.

1. SCOPE

This document applies to all incidents involving the unauthorised access, loss, or compromise of personal data for which Lowara Distribution Ireland acts as the data controller. It encompasses the procedures for assessing, documenting, and responding to such data breaches in compliance with the EU General Data Protection Regulation 2016 (GDPR).

The scope of this document includes:

Identification and Assessment: Guidance on identifying and assessing the severity and impact of personal data breaches, including the evaluation of potential risks to the rights and freedoms of data subjects.

Notification Procedures: Detailed instructions on the criteria and processes for notifying the supervisory authority and affected data subjects, including timelines and the information that must be communicated.

Roles and Responsibilities: Specification of the roles and responsibilities of key stakeholders involved in managing data breaches, including top management, information security, technology, legal, and data protection officers.

Documentation and Record Keeping: Requirements for documenting the breach, risk assessment findings, notification decisions, and actions taken to mitigate the breach and prevent future occurrences.

Interplay with Existing Procedures: Integration with Lowara Distribution Ireland 's existing Information Security Incident Response Procedure, ensuring a comprehensive approach to incident management.

This document is intended for use by all employees, contractors, and partners of Lowara Distribution Ireland who are involved in handling personal data or managing data breaches. It provides a framework for ensuring that Lowara Distribution Ireland meets its legal obligations under the GDPR while safeguarding the personal data of its customers and stakeholders.

2. OUT OF SCOPE

The following areas are considered out of scope for this document:

Non-Personal Data Incidents: This document does not cover incidents involving

data that is not classified as personal data under the GDPR, such as corporate or proprietary information, unless such incidents also involve personal data.

Data Breaches Outside Lowara Distribution Ireland 's Control: Incidents involving personal data breaches that occur within third-party systems or organizations where Lowara Distribution Ireland is not the data controller are not addressed by this procedure. Such incidents are managed according to the third party's data protection policies and agreements with Lowara Distribution Ireland .

Detailed Technical Response Procedures: The document does not include specific technical procedures or instructions for containing, investigating, or remediating the technical aspects of a data breach. These are covered in Lowara Distribution Ireland 's Information Security Incident Response Procedure and other technical protocols.

Employee Misconduct and Disciplinary Actions: This procedure does not address the handling of employee misconduct or disciplinary actions related to data breaches. Such matters are managed in accordance with Lowara Distribution Ireland 's human resources policies and procedures.

Comprehensive Information Security Management: The document does not encompass the broader aspects of Lowara Distribution Ireland 's information security management, risk assessment, or data protection strategies beyond the scope of responding to personal data breaches.

Incidents Involving Non-EU Jurisdictions: While the procedure is designed to comply with the GDPR, it does not cover specific legal requirements for data breach notifications in jurisdictions outside the EU unless they involve personal data governed by the GDPR.

This document is focused on providing guidance specifically for managing personal data breaches within the context of GDPR compliance and should be used in conjunction with other relevant policies and procedures to address areas beyond its defined scope.

3. ROLES & RESPONSIBILITIES

The document outlines the procedures and responsibilities for handling a personal

data breach at Lowara Distribution Ireland , in compliance with the EU GDPR. Key points include:

- Incident Response
- Notification Requirements
- Risk Assessment
- Supervisory Authority Notification
- Data Subject Notification
- Documentation and Follow-up

The document ensures Lowara Distribution Ireland 's adherence to GDPR requirements in case of a personal data breach.

4. POLICY

Identification and Initial Assessment of the Data Breach

The objective of this step is to promptly identify a potential personal data breach and perform an initial assessment to determine its nature, scope, and potential impact. This assessment helps in deciding the appropriate course of action and prioritizing the response.

4.1 Actions

4.1.1 Detection and Reporting:

Action: Encourage all employees, contractors, and partners to report any suspected or confirmed data breaches immediately to the Information Security Team or Data Protection Officer (DPO).

Inputs: Incident reports from staff, automated alerts from security systems, logs, or notifications from external sources (e.g., partners or vendors).

Output: An initial incident report that contains basic information about the breach, such as the date and time of discovery, nature of the breach, and affected systems or data.

4.1.2 Initial Analysis:

Action: The Information Security Team conducts a preliminary analysis of the incident to confirm whether it involves a personal data breach.

Inputs: Information from the initial incident report, access logs, security alerts, and other relevant data sources.

Output: A preliminary determination of whether a personal data breach has occurred and the potential severity of the breach.

4.1.3 Incident Classification:

Action: Classify the breach based on its nature (e.g., accidental, malicious, or system failure) and potential impact (e.g., low, medium, or high risk).

Inputs: Details from the initial analysis, including data types affected and initial risk assessment.

Output: An incident classification report that categorizes the breach and provides an initial risk level assessment.

4.1.4 Notification of Key Stakeholders:

Action: Notify key stakeholders, including top management, the DPO, and relevant department heads, of the potential breach and its initial classification.

Inputs: Incident classification report.

Output: A notification sent to stakeholders, outlining the initial findings and proposed next steps.

4.1.5 Documentation:

Action: Document all findings, decisions, and actions taken during the initial assessment.

Inputs: All information gathered during detection and initial analysis.

Output: A comprehensive incident log entry that captures the incident's initial identification and assessment details.

Inputs

4.2 Inputs

4.2.1 Incident Reports

Information from employees, contractors, and partners who suspect or identify a data breach.

4.2.2 Security Alerts:

Automated alerts and notifications from security systems that may indicate a breach.

4.2.3 Access Logs:

Logs from IT systems that can provide evidence of unauthorized access or anomalies.

4.2.4 External Notifications:

Information received from third parties or vendors regarding a potential breach.

4.3 Outputs

4.3.1 Initial Incident Report:

A report summarizing the initial discovery and details of the potential breach.

4.3.2 Incident Classification Report:

A detailed report categorizing the breach and assessing its initial risk level.

4.3.3 Stakeholder Notifications:

Communications sent to relevant stakeholders informing them of the breach and initial findings.

4.3.4 Incident Log Entry:

Documentation of all actions and findings during the initial assessment stage, stored for future reference and compliance purposes.

4.4 Considerations

4.4.1 Timeliness:

Ensure that the identification and initial assessment are conducted promptly to minimize potential impacts and comply with GDPR timelines.

4.4.2 Confidentiality:

Handle all reports and findings with strict confidentiality to protect sensitive information and maintain trust.

4.4.3 Collaboration:

Engage relevant teams, such as IT, legal, and data protection, to provide a comprehensive initial assessment and prepare for further investigation.

This step sets the foundation for a structured response to the data breach, ensuring that all relevant parties are informed and that the organization can quickly move forward with the next steps in managing the breach.

5. MONITORING AND REVIEW

The document outlines a thorough process for monitoring and reviewing incidents involving personal data breaches. Here are the key points:

5.1 Risk Assessment and Notification:

- The risk assessment process evaluates factors such as data encryption, pseudonymization, data types, volume, and the number of affected individuals.
- The decision to notify the supervisory authority or data subjects depends on the assessed risk to the rights and freedoms of natural persons.
- Notifications must be made without undue delay and within 72 hours when feasible.

5.2 Supervisory Authority Notification:

- The GDPR requires prompt notification to the supervisory authority if the breach likely poses a risk.
- The notification must include details such as the nature of the breach, data categories, and measures taken to address the breach.

5.3 Data Subject Notification:

- High-risk breaches necessitate informing affected data subjects.
- Communication should be clear, detailing the breach, consequences, and mitigation measures.

5.4 Documentation and Review:

- All risk assessments, decisions, notifications, and subsequent actions must be documented.
- Feedback from the supervisory authority and new information discovered during the investigation may alter the initial conclusions.
- The documented process ensures compliance with GDPR and helps in the ongoing review of the breach response procedures.

The process emphasizes thorough documentation and adaptive response to evolving information during the breach investigation

6. SUPPORTING DOCUMENTATION

- Data Protection Policy
- Data Protection Impact Assessment Procedure
- Data Subject Request Procedure

7. ACKNOWLEDGMENT AND COMPLIANCE

To acknowledge and comply with the policy outlined in the "Breach Procedure Document," follow these steps:

7.1 Acknowledgement of Policy

7.1.1 Formal Acceptance:

Staff must sign a document confirming they have read and understood the policy.

7.1.2 Training and Awareness:

Conduct regular training sessions on breach notification procedures.

7.1.3 Policy Distribution:

Share the policy document with all relevant employees via email, intranet, or printed copies.

7.1.4 Record Keeping:

Maintain records of staff acknowledgments to ensure compliance.

7.2 Compliance with the Policy

7.2.1 Incident Reporting:

- Immediate Reporting: Implement a process for prompt reporting of data breaches.
- Incident Response Team: Create a team with representatives from management, business, IT, and legal departments.

7.2.2 Risk Assessment:

- Evaluate the breach's risk to determine the need for notification.

7.2.3 Notification:

- Supervisory Authority: Notify within 72 hours if required, providing detailed information about the breach.
- Data Subjects: Notify affected individuals without undue delay if the breach poses a high risk.

7.3 Regular Reviews

7.3.1 Policy Reviews:

- Periodically review and update the policy to ensure ongoing compliance with GDPR and other regulations.

7.3.2 Audits:

- Conduct regular audits to ensure the procedures are being followed correctly.