Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Data Breach Response Plan.

Date: 01-04-2024.

Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Purpose

This document outlines the procedures to be followed in the event of a data breach, ensuring a swift and effective response to protect all stakeholders.

Scope

This plan applies to all data systems, employees, contractors, and partners associated with Brytend B.V.

Definitions

Data Breach: Unauthorized access, disclosure, alteration, or destruction of data.

SaaS: Software as a Service.

Roles and Responsibilities

Incident Response Team (IRT)(: A designated group responsible for executing the response plan.

Data Protection Officer (DPO): Ensures compliance with data protection laws and regulations.

IT Security Team: Manages and secures IT infrastructure.

Legal Counsel: Advises on legal obligations and communications.

Communications team: Manages internal and external communications.

Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Preparation

- Regularly update and patch systems.
- Conduct employee training on data security.
- Establish a communication protocol for breach notification.

Identification and Notification

- Implement monitoring tools to detect breaches.
- Define criteria for what constitutes a breach.
- Notify the IRT and DPO immediately upon breach detection.

Containment and Eradication

- Isolate affected systems to prevent further unauthorized access.
- Remove malicious software or unauthorized access points.
- Document actions taken for later analysis.

Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Recovery

- Restore systems from clean backups.
- Test systems to ensure the breach has been fully resolved.
- Monitor systems for any signs of recurrence.

Post-Incident Analysis

- Conduct a thorough investigation to determine the breach's cause.
- Assess the effectiveness of the response.
- Update policies and procedures based on lessons learned.

Compliance and Documentation

- Comply with all legal reporting requirements.
- Document all actions taken in response to the breach.
- Review and update the response plan regularly.

Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

Communication

- Inform affected partners and clients without undue delay.
- Provide clear and concise information about the breach and its impact.
- Offer support and solutions to mitigate potential harm.

Training and Testing

- Regularly train staff on the response plan.
- Conduct simulated breach exercises to test the plan's effectiveness.

Review and Update

- Review the plan annually or after significant changes to operations or IT infrastructure.
- Update the plan to reflect new threats, technologies, and best practices.