Regulatory Breach Incident Submission Document

Document Reference:

RB-2024-001
Date of Submission:

2024-06-15
Submitted By:

Jane Doe, Compliance Officer
Department:

Compliance & Risk Management

1. Incident Details

Date and Time of Incident:

2024-06-12, 14:30
Location:

Head Office, 4th Floor
Regulation(s) Breached:

Data Protection Act 2018
GDPR - Article 32
Type of Breach:

Unauthorized Data Disclosure

Description of Incident:

On June 12, 2024, it was discovered that confidential client information was inadvertently emailed to an unauthorized third party due to a manual error. The data included names, email addresses, and account numbers of 24 clients. The incident was identified during a routine compliance audit.

2. Impact Assessment

Immediate Impact:

- Breach of client confidentiality
- Potential reputational damage
- Possible regulatory fines

Number of Individuals Affected:

24 clients
Actions Already Taken:

- Affected individuals have been notified.
- Error was reported to the Compliance department immediately.
- Investigation initiated to review similar vulnerabilities.

3. Root Cause Analysis

Summary:

The breach was caused by human error during manual processing of client communications. Insufficient verification steps in the email dispatch process contributed to the incident.

4. Corrective and Preventive Actions (CAPA)

- Implement mandatory dual verification for all client data communications.
- Immediate retraining of staff involved in data handling.
- Periodic audit of data transmission workflows.
- Enhancement of data monitoring systems scheduled for Q3 2024.

5. Regulatory Notification

Date Notified:

2024-06-13
Regulator Notified:

Office of the Information Commissioner
Reference Number (If Provided):

ICO-2024-00632
Additional Notes:

All mandatory notifications have been made within required timeframes in accordance with applicable law.

Important Notes

- This document is confidential and must be handled accordingly.
- Accurate and prompt reporting of regulatory breaches is a legal requirement.
- All incidents must be investigated thoroughly, and remediation actions documented.
- Retain all related evidence and correspondence per the organizationâ€™s policy.
- Non-compliance can result in significant financial and reputational penalties.