Spraoi Chill Mhantáin

Data Breach Policy

Version	1.0
Date	May 2018
Owner	Spraoi Chill Mhantáin, Ciara@naionra.org, www.naionra.org, 087 9261318

Table of contents

1. Introduction

Spraoi Chill Mhantáin strives to comply with applicable laws and regulations related to Personal Data protection in Ireland. This procedure outlines the duties, the responsibilities and the notification process when responding to, and mitigating against, a personal data breach in Spraoi Chill Mhantáin.

Data breaches can occur regardless of the technical or physical measures that are implemented. Human error can also lead to a breach. This procedure outlines the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to the Data Protection Commissioner and individuals as required under GDPR.

2. Who is this policy for?

All employees either permanent or temporary, all contractors, all volunteers and students, regardless of their length of employment/placement in the service are required to read and understand this document, so they are fully aligned with the policy of Spraoi Chill Mhantáin. This document will also be made available to parents or guardians on request.

3. Definitions

In the Personal Data Protection Policy, Spraoi Chill Mhantáin has listed a number of key definitions of terms that are used in this policy and these are specifically drawn from Article 4 of GDPR.

4. Responsibilities in relation to Data Breaches

- The Owner/Manager will ensure that Spraoi Chill Mhantáin is prepared to implement a valid procedure in the event of a data breach.
- The Owner/Manager will provide an immediate, effective, and skilful response to any suspected/alleged or actual personal data breach affecting Spraoi Chill Mhantáin.
- If required, the Owner/Manager may also involve external parties (e.g. IT vendor) in this response.
- The Owner/Manager must be prepared to respond to a suspected/alleged or actual personal data breach 24/7, year-round.

5. Data Breach Response Procedure

All data breaches should be reported to the Owner/Manager as soon as possible. Once a personal data breach is reported to or detected by the Owner/Manager, the Data Breach Response Procedure is initiated

Step 1: Identify and confirm that a breach has occurred. The Owner/Manager is responsible for determining if the breach should be considered a breach affecting personal data.

Step 2: Take immediate action to stop the breach if it is ongoing or to reduce the affected data.

Step 3: Ensure proper and impartial investigation is initiated, conducted, documented, and concluded. The Data Breach Register will be used to record this information. The Owner/Manager is responsible for documenting all decisions and actions in relation to the breach. This may be reviewed by the Irish Data

Protection Commissioners Office and therefore will be written as precisely and thoroughly as possible to ensure traceability and accountability.

Step 4: Identify remediation requirements and document the remediation.

Step 5: Notify the Irish Data Protection Commissioners office if required. Not all personal data breaches need to be notified to the supervisory authority. The notification obligations under the GDPR are only triggered when there is a breach of personal data which is likely to result in a risk to the rights and freedoms of individuals. The Owner/Manager will establish whether the personal data breach should be reported to the Supervisory Authority.

In order to determine the risk to the rights and freedoms of the data subject(s) affected and therefore whether the breach should be reported to the Supervisory Authority, the Owner/Manager will consider the following:

1. The type of breach
2. The nature, sensitivity and volume of the personal data in question
3. The ease of identification of individuals from the data
4. The severity of consequences for individuals
5. The special characteristics of the individual (s) – e.g. a breach affecting vulnerable individuals may place them at a great risk of harm
6. The number of affected individuals

- If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification will be required. However, the data breach will be recorded in the Data Breach Register.
- If the Owner/Manager determines that the breach should be reported to the Supervisory Authority, then the Supervisory Authority will be notified without delay but no later than in 72 hours after the Owner/Manager has been made aware of the breach. Any possible reasons for delay beyond 72 hours will be communicated to the Supervisory Authority.

Step 6: Coordinate internal and external communications. The Owner/Manager will assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, as a result of the Data Protection Impact Assessment.

- If the personal data breach is likely to result in a risk to the rights and freedoms of the affected data subjects, the Owner/Manager owner will notify the affected data subjects without delay. The Notification to the data subjects must be written in clear and plain language and the Data Breach Notification Form – Data Subject will be used for this process.
- If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the Owner/Manager will take the necessary measures to ensure that the affected data subjects are notified using appropriate, publicly available channels.

Note: If an encrypted mobile phone/laptop is lost, a breach has occurred however as it is encrypted, no personal data is at risk of being exposed, therefore there is no requirement to report to the authorities or to parents.

6. If a data processor (i.e. third party) is responsible for a breach

Spraoi Chill Mhantáin, as the data controller, will ensure that an agreement (Supplier Data Processing Agreement) is in place between all third-party processors (i.e. payroll provider etc.) to ensure personal data is protected. If a personal data breach or suspected breach occurs within the third party, the third party will report this to Spraoi Chill Mhantáin without undue delay.

The Third Party should send Notification to the owner / manager that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

The Owner/Manager will record the data breach in the Data Breach Register. The Owner/Manager will then inform the data subjects affected of the breach.

7. Accountability

Any individual who breaches this Procedure may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

8. Validity and document management

This document is valid from _____(date).

The owner of this document is the Owner / Manager, who must check and, if necessary, update the document at least once a year.

This policy was adopted by Spraoi Chill Mhantáin on Date: _____

Signed by: _____ On behalf of Management
Position in Setting (Manager or Chairperson of Board of Management)

This policy will be reviewed by _____on _____