Personal Data Breach Policy & Procedures

Policy Area	Personal Data Breach Policy & Procedures
Policy no.	Policy no. 28
Policy version	Version number 1
Policy operational date	22.01.2024
Policy review date	22.01.2026

Introduction

torc.CFRC collect personal data relating to employee's/ board members/ training participants/ community members/volunteers/third party contractors/suppliers of goods and services which can include: name, home address, home telephone number, private email address, job title, date of birth, passport data, PPS number, bank details, emergency contact, staff number etc.

torc.CFRC also collects special category data relating to staff /board members which can include ethnic origin, health records and trade union membership.

torc.CFRC process personal data for the following purposes:

- To carry out research and statistical analysis.
- To register an interest in and communicate about our services, training, and volunteering opportunities.
- To respond to queries and/or information requests.
- To process job or volunteer applications.
- To process staff payroll.
- To respond to Subject Access Request(s).
- To respond to feedback or compliant(s).
- To comply with governance and statutory obligations.
- To select, contract and reimburse suppliers of goods and services.
- To update health and safety contact details of next of kin for staff members.

GDPR Obligations on Data Controllers & Data Processors

torc.CFRC is the Data Controller of most of the data which we process while managing the above activities. In a few instances we outsource data processing to third parties e.g., staff payroll, web hosting, financial management, HR services – these third parties are data processors, but torc.CFRC remains the Data Controller with primary responsibility for the data.

The General Data Protection Regulation (GDPR) 2018 requires organisations, both data controllers and processors, to have appropriate mechanisms in place to guarantee that all personal data is adequately protected. More specifically, Article 32 of the GDPR requires organisations to implement appropriate technical and organisational l measures to ensure a level of security appropriate to the risk. They must also ensure that any employees do not access or process any data unless they are required to do so.

The obligation to report data breaches

Under the GDPR and the Data Protection Act 2018, torc.CFRC as a data controller must notify the Data Protection Commission (DPC) of a personal data breach without delay where that breach is likely to result in a risk to the rights and freedoms of the

data subject. Notification should be made at the latest, within 72 hours of the controller becoming aware of the breach. Data processors must notify the respective controllers if the processor becomes aware of a breach. The controller should then notify the data subject without delay.

A controller must also notify a data subject without delay in clear and plain language if the data breach is likely to result in a high risk to the rights and freedoms of the data subject. An example of a high-risk situation would be where a person's bank or passport details are stolen.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The term 'personal data' means any information concerning or relating to an identified or identifiable individual. Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) as well as deliberate acts (such as phishing attacks to gain access to customer data). A personal data breach occurs in incidents where personal data are lost, destroyed, corrupted, or illegitimately disclosed. This includes situations such as where someone accesses personal data or passes them on without proper authorisation, or where personal data are rendered unavailable through encryption by ransomware, or accidental loss or destruction.

What should a notification to the DPC contain?

A notification of a personal data breach by a controller to the DPC (which can be done through the breach notification form on the DPC's website) must at least:

a) Describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
b) Communicate the name and contact details of the main contact point where more information can be obtained.
c) Describe the likely consequences of the personal data breach.
d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Data Breach Incident – External Notification Form

The purpose of this Form is to report a Breach Incident involving Personal Data, as required under GDPR 2018.
torc.CFRC is committed to protecting the confidentiality and integrity of the personal information under its control and will ensure that such incidents are appropriately investigated and reported, and that the risk of a recurrence is minimised.

Contact Information

Data Controller/Organisation:	torc.CFRC
Data Protection Officer (where relevant):	Derek O'Leary
Contact details:	Derek.O'Leary@ballyspillanecfrc.ie

High Level Description of Incident

Brief Description of Incident:		
Date of Incident:		
Location of Incident (if known):		
Date and time when Controller was made aware (if different):	**Date:**	**Time:**

Personal Data Impacted by Incident

Description of Personal Data / Sensitive Personal Data impacted:	
Categories of Data Subjects impacted:	
Volume of records involved:	
Number of Data Subjects impacted:	

Detailed Description of the Incident

(Description of the sequence of events
leading up to the breach incident - please include associated e-mail correspondence)

Actions taken (to date) to address the Incident
(Description of the measures which have been taken since becoming aware of the Incident)

Current Status (At time of reporting)
(What is the current status of the Personal Data impacted by the breach incident?)

Actions being taken to minimise impact on Data Subjects

Action	Description	Owner	Status (planned, under way, complete)

Actions being taken to prevent a recurrence of the incident

Action	Description	Owner	Status (planned, under way, complete)

Review

This policy will be reviewed every three years or sooner if required.

Revision No.	Approval Date	Document Reference and Changes Made	Name