




BROTHERS OF CHARITY SERVICES IRELAND

DATA BREACH PROCEDURES

Document reference number	2019NP36	Revision No.	1
Approved by	Brothers of Charity Services Ireland		
Signed	 Michael Hennessy, Chief Executive		
Approval date	29/6/2023	Next Revision Date	29/6/2026

Contents

Ethos	3
1.0 Introduction	3
2.0 Procedure Statement	3
3.0 Purpose	4
4.0 Scope.....	4
5.0 Glossary of Terms and Definitions	4
6.0 Data Security & Breach Requirements	6
7.0 Data Breach Procedures & Guidelines	7
7.1 Breach Monitoring & Reporting.....	7
7.2 Identification of an Incident.....	7
7.3 Breach Recording.....	8
8.0 Data Breach Risk Assessment	8
8.1 Human Error	8
8.2 System Error.....	9
8.3 Assessment of Risk and Investigation	9
9.0 Breach Notifications	10
9.1 Data Protection Commissioner Notification	10
9.2 Data Subject Notification	11
10.0 Record Keeping	11
11.0 Responsibilities.....	12
12.0 Review of Procedure.....	12
Appendix 1 Data Breach Incident Form	13

Ethos

'We are committed to working with people with an intellectual disability to claim their rightful place as valued citizens. Inclusion is a fundamental principle that underlies all aspects of our work. We believe in the intrinsic value of every person and we aim to further the dignity of all associated with our services. '

'We continue the Brothers of Charity Services' tradition of being open to the best contemporary influences. We want to be inspired by the most creative ideas and to ask how we give them concrete expression.'

The Brothers of Charity Services Ethos (2001), Going Forward Together.

1.0 Introduction

The Brothers of Charity Services Ireland endeavours to offer services/supports in local communities. This enables each person who is supported by our services to positively engage in the social and economic life of their local towns and villages and in doing so, develop a range of relationships that enhance their quality of life. Our responses are based on the recognition of each person (who is supported by our service) as an individual, an equal citizen with equal rights and an absolute respect of that status. We, therefore, support each person to live their lives based on their own personal visions and choices, to identify and select their personal goals in life and to develop their personal plan to achieve those goals.

One of those rights is the right to Privacy and Confidentiality for both those we support and those we employ. For the purpose of the Data Protection Act and the General Data Protection Regulations (GDPR) the Brothers of Charity Services Ireland is the Data Controller of personal and sensitive data of all those to whom we provide Services and all those who work within the Services.

2.0 Procedure Statement

- 2.1 The Brothers of Charity Services Ireland (BOCSI) is committed to our obligations under the regulatory system and in accordance with the General Data Protection Regulations (GDPR). We maintain a robust and structured program for compliance and monitoring. We carry out risk assessments (see BOCSI Risk Management Policy & Procedure) to ensure that our compliance processes, functions, and procedures are fit for purpose. BOCSI recognises that data breaches can occur and this procedure states our intent and objectives for dealing with such incidents.
- 2.2 Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures, and processes to help protect data subjects and their information from any risks associated with processing data. The protection and security of the data we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the Data Protection Laws.

- 2.3 These procedures are for the protection of BOCSI, its staff, the people who are supported by our Services, and third parties, and are of the utmost importance for legal regulatory compliance.

3.0 Purpose

- 3.1 The purpose of this procedure is to outline BOCSI's objectives and procedures regarding data breaches involving personal or sensitive information. In line with our obligations under the GDPR we have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This procedure details our processes for reporting, communicating, and investigating such breaches and incidents.

4.0 Scope

- 4.1 This procedure is to be used by all staff within BOCSI (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, students, work experience placements, and agents engaged with BOCSI in Ireland or overseas) who are responsible for managing and reporting data breaches. The BOCSI Data Protection Handbook - A Practical Guide for BOCSI staff to Data Protection and GDPR, the Subject Access Policy & Procedure and the Confidentiality Policy & Procedure, give further guidance to staff. Adherence to this procedure is mandatory and noncompliance could lead to disciplinary action.

5.0 Glossary of Terms and Definitions

- **"Biometric data"** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as fingerprinting or facial images.
- **"Binding Corporate Rules"** means personal data protection policies which are adhered to by BOCSI for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- **"Consent"** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **"Cross Border Processing"** means processing of personal data which takes place in more than one EU Member State; or which substantially affects or is likely to affect data subjects in more than one EU Member State
- **"Data controller"** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- **"Data processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **"Data protection laws"** means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws with which BOCSI complies.
- **"Data subject"** means an individual who is the subject of personal data
- **"GDPR"** means the General Data Protection Regulation (EU) (2016/679)
- **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- **"Personal data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **"Privacy Engine"** is the BOCSI's Data Protection and GDPR compliance software for data protection practitioners.
- **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Profiling"** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **"Pseudonymisation"** means the enhancement of privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms.
- **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- **"Supervisory Authority"** means the 'Data Protection Commissioner's Office.

- **"Third Party"** means a natural or legal person, public authority, agency or body other than the data subject under our direct authority
- **"Data Protection Representative (DPR)"** means the BOCSI person identified in each of the BOCSI Regions as the person supporting and driving the implementation of the BOCSI's Data Protection Policy and associated procedures in that Region. The DPR receives and processes Subject Access Requests and manages Data Protection Breaches for their Region. The DPR is a member of the National Data Protection Team appointed by the Chief Executive.
- **"Data Protection Officer" (DPO)** means the person appointed by the Chief Executive to be the BOCSI Data Protection Officer as set out under GDPR, and notified to the Data Protection Commissioner's Office. The DPO chairs the National Data Protection Team appointed by the Chief Executive.

6.0 Data Security & Breach Requirements

- 6.1 BOCSI defines a data breach as any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure' of, or access to, personal or sensitive data.
- 6.2 Alongside our 'Privacy by Design' approach to protecting data, BOCSI also has a legal, regulatory and business obligation to ensure that personal and sensitive information is protected whilst being processed by the organisation. Our technical and organisational measures are detailed in our ICT Security Policies & Procedures.
- 6.3 BOCSI carries out audits to ensure that all personal data processed is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments, where appropriate, that assess the scope and impact of any potential data breach both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, which may include (but not limited to):
 - Pseudonymisation/anonymisation and encryption of personal data.
 - Restricted access, need to know basis.
 - Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
 - Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident.
 - Audit procedures and stress testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations.
 - Frequent and ongoing data protection information and training programs for all employees.

- Regular knowledge testing to ensure a high level of competency, knowledge, and understanding of the data protection regulations and the measures we have in place to protect personal information.
- Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared, or is due for disposal, it is rechecked and authorised by a relevant senior manager.

7.0 Data Breach Procedures & Guidelines

BOCSI has robust objectives and controls in place for preventing data breaches and for managing them in the event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented Breach Incident Procedure aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

7.1 Breach Monitoring & Reporting

- 7.1.1 BOCSI Data Protection Officer (DPO) is responsible for the review and investigation of any data breach involving personal information regardless of the severity, impact or containment. All data breaches must be reported to the Data Protection Representative (DPR) in the relevant region who in turn will report the breach to the DPO.
- 7.1.2 All data breaches will be investigated, even in instances where notifications and reporting are not required (e.g. an incident where data is lost and retrieved quickly without being accessed by anyone else). A full record of all data breaches is retained to ensure that any pattern can be analysed and actioned. Where a system or process failure has given rise to a data breach revision to any such process is recorded and reviewed.

7.2 Identification of an Incident

- 7.2.1 As soon as a data breach has been identified:
 - a. If possible contain the breach immediately.
 - b. Report the breach to both your direct Line Manager and the Data Protection Representative (DPR) immediately so that breach procedures can be initiated and followed without delay.
 - c. Once the DPR is satisfied that a breach has occurred they should report the breach to the Data Protection Officer and complete the Data Breach incident Form (Appendix 1).
 - d. The DPO will establish if the breach is reportable, and if so, will report to the Data Protection Commissioner within 72 hours of the breach being identified.
- 7.2.2 Reporting incidents in full and with immediate effect is essential to ensure BOCSI remains compliant with Data Protection regulations.
- 7.2.3 As soon as an incident has been reported measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken. The aim of any such measures should be to stop any further risk/breach to the

organisation, the people we support, families, employees, volunteers, retired employees, contractors, third-parties, and system or data, prior to investigation and reporting. The measures taken must be noted on the Breach Incident Form in all cases.

7.3 Breach Recording

- 7.3.1 A Breach Incident Form (Appendix 1) is completed by the person involved in the breach with the support of the line manager and/or the DPR for all data breaches regardless of severity.
- 7.3.2 Completed Breach Incident Forms are logged and filed in the Breach Incident Folder of the Privacy Engine (IT System) by the relevant DPR. Hard copy of completed forms are forwarded to the DPO, who is required to keep hard copies on file and available for the Data Protection Commissioner on demand. These Forms are reviewed against existing records to ascertain patterns by the DPR and audited by the DPO.
- 7.3.3 In cases of a major data breach the DPR supported by the DPO is responsible for carrying out an investigation, appointing the relevant staff to contain the breach, ensuring the recording of the incident on the Breach Incident Form and making any relevant and legal notifications.
- 7.3.4 An investigation must be conducted and recorded on the Breach Incident Form with the outcome being communicated to all staff involved in the breach and to the relevant Director of Service and the DPO.
- 7.3.5 If applicable, the Data Protection Commissioner (DPC) and the data subject(s) are notified by the DPO in accordance with the GDPR requirements (refer to Section 6 of this procedure). The DPO makes the decision to notify data subjects and/or the DPC. The Data Protection Commissioner protocols are to be followed and their 'Security Breach Notification Form' should be completed and submitted by the DPO. Any individual whose data or personal information has been compromised must be notified, if there is a possibility of harm arising from the breach, and they should be kept informed of the date, type of data breached, actions taken to retrieve the data, actions taken by BOCSI to ensure that a similar breach does not occur and any other outcomes and actions. The notification must include the individual's right to complain to the Data Protection Commissioner.

8.0 Data Breach Risk Assessment

8.1 Human Error

- 8.1.1 Where the data breach is the result of human error an investigation into the root cause will be conducted and the employee(s) will be interviewed.
- 8.1.2 A review of the procedure(s) associated with the breach and a risk assessment will be conducted in accordance with BOCSI's Risk Management Policy & Procedures. Any identified gaps that are found to have caused/contributed to the breach will be revised and risk assessed to mitigate any future occurrence of the same root cause.

8.1.3 Resultant employee outcomes of such an investigation can include, if there has been numerous breaches by the same person or if it has been determined that the breach was malicious, but are not limited to: -

- Re-training in specific/all compliance areas.
- Re-assessment of compliance knowledge and understanding.
- Suspension from compliance related tasks.
- Formal warning (in-line with BOCSI's disciplinary procedures).
- Dismissal.

8.2 System Error

8.2.1 Where the data breach is the result of a system error/failure, the Chief Information Officer (CIO) will be notified by the DPO. The CIO will assess the risk and investigate the root cause of the breach. A gap analysis will be completed on the system/s involved and a full review and report will be forwarded to the DPO to attach to the Breach Incident Form.

8.2.2 Any identified gaps that are found to have caused/contributed to a breach will be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause by ICT. Full details of the breach should be determined and mitigating action, such as the following, should be taken to limit the impact of the incident.

- Attempt to recover any lost equipment or personal information.
- Shut down an IT system.
- Remove an employee from their tasks.
- Use of back-ups to restore lost, damaged or stolen information.
- Make the building secure.
- Change of entry codes or passwords.

8.3 Assessment of Risk and Investigation

8.3.1 The DPR and the DPO will ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

8.3.2 The DPR/DPO will discuss: -

- The type of information involved.
- It's sensitivity or personal content.
- What protections are in place (e.g. password protect)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident.

8.3.3 The DPR/DPO will keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

9.0 Breach Notifications

BOCSI recognises its obligation and duty to report data breaches in certain instances.

All staff will be made aware of BOCSI's responsibilities. The BOCSI has internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay to the DPR and through them to the DPO.

9.1 Data Protection Commissioner Notification

- 9.1.1 Where a breach is likely to result in a risk to the rights and freedoms of individuals the Data Protection Commissioner will be notified of any breach by the BOCSI Data Protection Officer.
- 9.1.2 Where applicable the Data Protection Commissioner will be notified of the breach no later than 72 hours after the DPO becomes aware of the breach. The Data Protection Commissioner will be kept informed throughout any breach investigation and will be provided with a full report, including outcomes and mitigating actions, as soon as possible and always within any specified timeframes.
- 9.1.3 If for any reason it is not possible to notify the Data Protection Commissioner of the breach within 72 hours the notification will be made as soon as is feasible and will outline the reasons for the delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons BOCSI reserves the right not to inform the Data Protection Commissioner in accordance with Article 33 of the GDPR.
- 9.1.4 The notification to the Data Protection Commissioner will contain
 - Date and time of breach.
 - A description of the nature of the personal data breach.
 - The categories and approximate number of data subjects affected.
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information).
 - A description of the likely consequences of the personal data breach.
 - A description of the measures taken, or proposed to be taken, to address the personal data breach (including measures to mitigate its possible adverse effects).
 - A notification that the Data Subjects have been notified.
- 9.1.5 Breach Incident Procedures must always be followed and an investigation carried out, regardless of our notification obligations and outcomes, with Reports being retained and made available to the Data Protection Commissioner on request.

- 9.1.6 Where BOCSI acts in the capacity of a Processor we will ensure that the Data Controller is notified of the breach without undue delay. In instances where we act in the capacity of a Controller using an external processor, a written agreement must be in place to state that the Processor is obligated to notify BOCSI without delay after becoming aware of a data breach.

9.2 Data Subject Notification

- 9.2.1 When a data breach is likely to result in a high risk to the rights and freedoms of natural persons the BOCSI DPO will determine that a communication, in a written, clear, and legible format be sent out to the data subjects without undue delay, indicating a data breach has occurred setting out the exact data breached and the plan in place to rectify the breach. The DPO will determine who the most appropriate person to issue this communication is.
- 9.2.2 The notification to the Data Subject will include
- A full apology.
 - The nature of the data breach.
 - The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information or making a complaint).
 - A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects).
 - Information on their right to make a complaint and direction on how to lodge the complaint with the Data Protection Commissioner's Office.
- 9.2.3 BOCSI reserves the right not to inform the data subject of any data breach in situations where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc.) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.
- 9.2.4 If informing the data subject of the breach involves disproportionate effort BOCSI reserves the right to issue a public communication whereby the data subject(s) are informed in an equally effective manner.

10.0 Record Keeping

- 10.1 All records and notes taken during the identification, assessment, and investigation of a data breach must be approved by the DPR and the DPO and must be retained for a period of 6 years from the date of the breach incident.
- 10.2 Data Breach Incident Forms will be reviewed by the DPR and the DPO to identify patterns of breach reoccurrences and review actions taken to prevent further breach incidents from occurring.

11.0 Responsibilities

- 11.1 BOCSI will support staff to learn, understand, and implement all procedures within this document. It is the responsibility of all staff to adhere to the guidelines surrounding Data Protection and GDPR.
- 11.2 The Data Protection Officer and the Data Protection Representatives are responsible for compliance audits and monitoring and the subsequent reviews and follow up actions.

12.0 Review of Procedure

- 12.1 This procedure will be reviewed at least every three years or more frequently if required by any changes in legislation or in the structure.

Appendix 1 Data Breach Incident Form

DATA PROTECTION REPRESENTATIVE (DPR) DETAILS:			
NAME:		REGION:	
DATE:		TIME:	
TEL:		EMAIL:	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH: (Human Error or Systems Failure)			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		NO. OF RECORDS INVOLVED:	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
NAME OF STAFF INVOLVED IN BREACH:			
PROCEDURE(S) INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE BOCSI DATA PROTECTION OFFICER NOTIFIED?			YES/NO
WAS THE DATA PROTECTION COMMISSIONER'S OFFICE NOTIFIED?			YES/NO
IF YES, WAS THIS WITHIN 72 HOURS?			YES/NO/NA
<i>If no to the above, provide reason(s) for delay</i>			
INFORMATION PROVIDED WITH THE NOTIFICATION?			YES NO
<i>A description of the nature of the personal data breach</i>			

<i>The categories and approximate number of data subjects affected</i>		
<i>The categories and approximate number of personal data records concerned</i>		
<i>The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)</i>		
<i>A description of the likely consequences of the personal data breach</i>		
<i>A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)</i>		
<i>Has the Data Subject been notified?</i>		
Has the Data Subject been notified about their right to complain?		
Has the BOCSI Data Protection Officer been copied on this Form?		
<i>Has the Office of the Data Protection Commissioner been notified?</i>		
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: (if applicable)		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
DID THE MITIGATING ACTIONS TAKEN PREVENT THE BREACH FROM OCCURRING AGAIN? (Describe)		
WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	YES/NO	
<i>If yes to the above, describe measures</i>		
DPR Signature: _____ Date: _____ DPR Name: _____ Authorised by: _____ (DoS) DPO Signature _____ DPO Name _____		