SeeBeyondBorders Ireland

POLICY

DATA PROTECTION, CYBERSECURITY AND DATA BREACH POLICY

Approval and Review Schedule

Policy
Data Protection, Cybersecurity and Data Breach Policy *This policy was developed from 2 standalone policies on Data Protection and Data Breach. The revised policy covers data protection, cybersecurity and data breach.

Contents

INTRODUCTION AND PREAMBLE

Data protection and security is a matter of trust. This policy is our commitment to treat personal information of Trustees, Employees and Stakeholders with the utmost care and confidentiality. The aim of this policy is to ensure that SBBI collect, store and handle personal data fairly, transparently and with the greatest respect to individual rights.

For the purposes of this document and to ensure a cohesive and consistent approach to its implementation, this policy has been developed in 3 parts:

1. Data Protection
2. Cybersecurity
3. Data Breach

SCOPE

The policy covers both personal and special categories of personal data held in relation to data subjects by SeeBeyondBorders, Ireland. The policy applies equally to personal data held in manual and automated form. All personal and special categories of personal data will be treated with equal care by SeeBeyondBorders, Ireland. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy applies to Trustees, Employees, Volunteers, and any individuals and stakeholders engaged with the charity, who receive, handle or processes personal data in the course of their interactions with SBBI. It is our aim that all parties are aware of the need to maintain secured systems and fully understand their individual responsibilities as outlined in this policy.

Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

1.DATA PROTECTION

1.1 PURPOSE

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of SeeBeyondBorders Ireland. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, including the Data Protection Act (1988), the Data Protection (Amendment) Act (2003), the Data Protection Act (2018) and the General Data Protection Regulation (2018).

The aforementioned legislation describes how organisations — including SeeBeyondBorders Ireland— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must be:

1. obtained and processed fairly
2. kept for one or more specified and lawful purpose(s)
3. processed in ways compatible with the purposes for which it was given initially
4. kept safe and secure
5. kept accurate and up-to-date
6. adequate, relevant and not excessive
7. retained no longer than is necessary for the specified purpose(s)
8. copied and given to any individual on his/her request

1.2 RATIONALE

SeeBeyondBorders, Ireland must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by SeeBeyondBorders Ireland in relation to its employees, trustees, service providers, donors, supporters and others (e.g. event participants) in the course of its activities. SeeBeyondBorders Ireland makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

1.3 STATEMENT OF COMMITMENT

SeeBeyondBorders Ireland recognise that data protection and cybersecurity is paramount in today's digital landscape. The General Data Protection Regulation (GDPR) and Data Protection Acts 1988-2018 apply to the processing of personal data. SBBI is committed to complying with its legal obligations in this regard. SBBI collect and process personal data relating to Employees, Trustees and Stakeholders in the course of our business in a variety of circumstances.

SBBI maintain a list of third party data processors; which include professional services such as insurance companies / brokers, auditors along with service providers such as IT support, payroll companies, software providers, etc. Any company that processes personal data on behalf of SBBI have relevant contracts in place to ensure the protection of personal data.

By adhering to this policy, SBBI is protecting our data from potential security risks and vulnerabilities.

1.4 SEEBEYONDBORDERS IRELAND AS A DATA CONTROLLER

In the course of its daily organisational activities, SBBI acquires, processes and stores personal data in relation to:

- SBBI Trustees
- Employees of SBBI
- Volunteers of SBBI
- Consultants/Service providers engaged by SBBI
- Participants at SBBI meetings/events/conferences
- Recipients of SBBI newsletters/communications
- Donors of SBBI

In accordance with Data Protection legislation, this data must be acquired and managed fairly. SeeBeyondBorders, Ireland is committed to ensuring that its employees, volunteers and trustees have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, employees/volunteers/trustees must ensure that the Data Protection Officer is informed, in order that appropriate corrective action can be taken.

In general terms, the employee should consult with the Data Protection Officer to seek clarification.

Data Protection			
Deirdre Heverin	Data Protection Officer (DPO)	Operations & Education Lead	+353 87 4877 996 deirdre.heverin@seebeyondborders.org
Catherine Byrne	Deputy Data Protection Officer	Chair	+353 86 048 4040 catherine.byrne@seebeyondborders.org

1.5 PROCEDURE

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, SBBI will adhere to best practice regarding the applicable Data Protection legislation.

Third Party Processors

In the course of its role as a Data Controller, SBBI engages a number of Data Processors to process

Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation. These Data Processors include auditors, fundraising platforms, payroll processors and online payment system providers.

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to SBBI's Data Protection policy.

In its capacity as Data Controller, SBBI ensures that all data shall:

1. ***Be obtained and processed fairly and lawfully.***

For data to be obtained fairly, the data subject will, at the time the data is being collected, be made aware of:

- The identity of the Data Controller (SBBI)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing is fair.

SBBI will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, SBBI will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data will be carried out only as part of SBBI's lawful activities, and SBBI will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to SBBI and operating on its behalf.

2. ***Be obtained only for one or more specified, legitimate purpose.***

SBBI will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which SBBI holds their data, and SBBI will be able to clearly state that purpose(s).

3. ***Not be further processed in a manner incompatible with the specified purpose(s).***

Any use of the data by SBBI will be compatible with the purposes for which the data was acquired.

4. ***Be kept safe and secure.***

SBBI will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by SBBI in its capacity as Data Controller. Access to and management of Employee and service provider records is limited to those Employees/Trustees with appropriate authorisation and password access.

5. ***Be kept accurate, complete and up-to-date where necessary.***

SBBI will ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy and conduct an annual review to ensure that relevant data is kept accurate and up-to-date. Training will be provided to Trustees and Employees where appropriate, to ensure they stay abreast of changing legislation and processes pertaining to data protection and security.

2. CYBERSECURITY

2.1 PURPOSE

The purpose of this policy is to ensure a safe and secure environment for Trustees, Employees, Volunteers and Stakeholders, while protecting our assets and information. All information systems operated by SBBI are secure and comply with the requirements of the Data Protection Act and the Computer Misuse Act.

This policy is a set of guidelines and rules to safeguard the information assets of SeeBeyondBorders Ireland from cyber threats and unauthorised access. This policy outlines the legal requirements and responsibilities of SBBI in maintaining cybersecurity measures and defines the protocols to be followed in the event of a security incident related to our data.

2.2 POLICY

SBBI strives to meet all relevant Data Protection, privacy, and security requirements, whether originating from legal, regulatory, or contractual obligations.

This cybersecurity policy is essential to ensure the protection of our information security, maintain regulatory compliance, and mitigate the security risks associated with cyber threats. By establishing clear guidelines and expectations, SBBI can minimize the likelihood of security breaches and protect our reputation and integrity.

This policy includes guidelines for the following key areas:

- Confidential or sensitive data (Data Protection)
- Security of personal and company devices
- Security of emails and other digital communications
- Password management and secure data transfer
- Reporting violations and disciplinary actions

2.4 STATEMENT OF COMMITMENT

SeeBeyondBorders Ireland recognise that data protection and cybersecurity is paramount in today's digital landscape. The General Data Protection Regulation (GDPR) and Data Protection Acts 1988-2018 apply to the processing of personal data. SBBI is committed to complying with its legal obligations in this regard. SBBI collect and process personal data relating to Employees, Trustees and Stakeholders in the course of our business in a variety of circumstances.

SBBI maintain a list of third party data processors; which include professional services such as insurance companies / brokers, auditors along with service providers such as IT support, payroll companies, software providers, etc. Any company that processes personal data on behalf of SBBI have relevant contracts in place to ensure the protection of personal data.

By adhering to this policy, SBBI is protecting our data from potential security risks and vulnerabilities.

2.5 PROCEDURE

Handling Confidential Data

Confidential data refers to any sensitive information that, if disclosed or compromised, could harm the organisation or its stakeholders. Examples include:

- Customer Information: Personal identifiable information (PII) such as names, addresses, contact details.

- Financial Records: Financial statements, transaction records, banking information, and payroll data.
- Intellectual Property: Patents, trademarks, copyrights, and proprietary research and development

SBBI Guidelines for Handling Confidential Information:

- SBBI protect data using passwords.
- Only authorised personnel can access confidential data.
- Employees are discouraged from storing data on personal devices or unsecured platforms.
- Employees are encouraged to stay informed by participating in training sessions to understand security threats like phishing emails or scams.
- Breaches of data/security are reported in a timely fashion to Data Protection Officer. If deemed notifiable to the Data Protection Commission, the incident should be reported within 72 hours.
- SBBI comply with data protection laws like GDPR.

Securing Personal and Company Devices

SBBI Employees are required to stay abreast of data security measures including, but not limited to:

- *Software Updates*: Regularly updating operating systems, applications, and antivirus software to patch vulnerabilities and defend against cyber attacks or threats.
- *Using Strong Passwords*: Setting strong, unique passwords for all accounts and devices.
- *Enabling Device Encryption*: Using encryption features on devices to safeguard data in case of theft or unauthorized access. Encrypt hard drives or utilize built-in encryption tools (e.g.) codes for in-camera meeting minutes.
- *Being aware of Phishing Emails*: Exercise caution when opening emails from unknown senders or clicking on suspicious links. Report phishing attempts immediately.
- *Installing Antivirus Software*: Install antivirus software on company devices to detect and remove malware, ransomware, and other malicious software.
- *Using Secure Wi-Fi Connections*: Connecting to secure Wi-Fi networks and avoid using public or unsecured networks whenever possible.
- *Implementing Two-Factor Authentication* (2FA): Enabling 2FA on accounts (banking) and devices to add an extra layer of security beyond passwords. This helps prevent unauthorised access even if passwords are compromised.

Email Security

SBBI Employees engage in remote working conditions, meaning that email communication and access to shared drives are essential within the organisation. Both modes are vulnerable to data leaks and security breaches. To minimise the risk of compromise, anyone provided with a SBB email address must:

- *Stay Vigilant Against Phishing Attempts:* Being cautious of emails requesting sensitive information. Where possible, SBBI Employees should verify the sender's email address and scrutinise unexpected requests for personal data or financial information.
- *Utilise Secure Email Protocols*: Employees are provided with a secure SBB email address. Links to shared drive are protected when sharing outside SBB. Employees are encouraged to enable spam to automatically identify and divert suspicious or malicious emails to the spam or junk folder.
- *Exercise caution when clicking on links or downloading attachments*: Employees are encouraged to hover over links to verify the URL's legitimacy, and only open attachments from trusted senders.

Password Management and Secure Data Transfer

It is imperative to set strong, unique passwords using a combination of letters, numbers and symbols. SBBI recommend Employees change passwords periodically (every three to six months) to maintain the security of data, especially in response to security incidents.

As SeeBeyondBorders operates internationally, it may be necessary in the course of our work to transfer data within SBB in countries which do not have comparable data protection laws to Ireland. The transfer of such data may be necessary to facilitate the overall administration of SBB. SBBI will keep detailed records of all data transfers. This helps maintain accountability and facilitates auditing and compliance efforts.

Reporting Violations and Disciplinary Actions

As an Employee, it's essential to promptly report any violations or suspected breaches of our data protection and cybersecurity policies to the Data Protection Officer.

SBBI as a Data Controller is legally required to notify the Office of the Data Protection Commissioner where a personal data breach is likely to result in a risk to data subjects' rights and freedoms. In addition, SBBI are legally required to notify affected individuals (Data Subjects) where a Personal Data

breach is likely to result in a high risk to their rights and freedoms. SBBI Data Protection Officer is required to notify the Data Protection Commissioner within 72 hours after having become aware of the Personal Data breach.

3. DATA BREACH

3.1 POLICY STATEMENT

SeeBeyond Borders Ireland is committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured programme for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur; hence this policy states our intent and objectives for dealing with such incidents.

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 personal information from any risks associated with processing data. The protection and security of the personal data that 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.

3.2 PURPOSE

The purpose of this policy is to provide a concise statement regarding SBBI's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all Employees/ Trustees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

3.3 DATA SECURITY AND BREACH REQUIREMENTS

SeeBeyondBorders Irelands definition of a personal data breach is 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 data.

Alongside our *'Privacy by Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by SBBI. Our technical and organisational measures are detailed in our Data Protection and Cybersecurity Policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments 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, including *(but not limited to*): -

1. Encryption of personal data
2. Restricted access
3. Frequent and ongoing data protection training programs for all employees/Trustees
4. Staff assessments and 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
5. Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; it is rechecked and authorised by the Data Protection Officer and Chairperson of SeeBeyond Borders Ireland.

Objectives

- To adhere to the GDPR and Irish Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information

- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees; including their information and identity
- To ensure that where applicable, the Data Protection Officer and Chair are involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of SBBI having become aware of the breach

3.4 DATA BREACH PROCEDURES AND GUIDELINES

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

Breach Monitoring and Reporting

The Charity has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records. If deemed notifiable to the Data Protection Commission, the incident should be reported within 72 hours.

Breach Incident Procedures

1. Identification of an Incident

As soon as a data breach has been identified, it is reported to the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of SBBI and is not about apportioning blame. These procedures are for the protection of SBBI, its Employees, Volunteers, Stakeholders and third parties and are of the utmost importance for legal regulatory compliance.

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; however, the aim of any such measures should be to stop any further risk/breach to the organisation, donors, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

2. Breach Recording

SBBI utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder *(electronic or hard-copy)* and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the Data Protection Officer is responsible for ensuring a full investigation is carried out, reporting on same to the Board, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all Employees involved in the breach, in addition to the CEO-International Organisation. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Data Protection Commission and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 6 of this policy*). The Data Protection Commission protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all

outcomes and actions. The Data Protection Officer should ensure that the Board of SeeBeyondBorders Ireland are notified of any breaches and action taken.

Breach Risk Assessment

1. Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the Employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with SBBI's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, 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 the Charity 's disciplinary procedures)*

2. System Error

Where the data breach is the result of a system error/failure, IT support are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

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

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- The use of back-ups to restore lost, damaged or stolen information
- Making the hardware secure

- If the incident involves any entry codes or passwords, then these codes must be changed immediately and Employees informed

3. Assessment of Risk and Investigation

The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

Key factors to look at include:

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

The Data Protection Officer should 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.

3.6 BREACH NOTIFICATIONS

Supervisory Authority Notification

Homepage | Data Protection Commission

The Data Protection Commission is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after SBBI becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the Data Protection Officer and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- 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)*

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where SBBI acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer
- 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)*

3.7 RECORD KEEPING

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of

6 years from the date of the incident. Incident forms are to be reviewed quarterly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

3.8 RESPONSIBILITIES

SBBI will ensure that all Employees are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.