SIGBI DATA PROTECTION PROTOCOLS

2018

For the purpose of this document, references to Soroptimist International Great Britain and Ireland (SIGBI) Limited and Soroptimist International may be written as "SIGBI" and "SI" only.

Contents

Pages

The General Data Protection Regulation ("GDPR")

Overview

Growing digital technology means the world is a different place to what it was when the Data Protection Act 1998 ("DPA") came into force. Record keeping has shifted from paper to electronics, the methods for manipulating personal information have become more powerful and identity theft has become a significant problem. People want greater choice and control over how their personal data is used.

The EU General Data Protection Regulation ("GDPR") extends the data rights of individuals, making transparency a right and increases the obligations on organisations to have clear policies and procedures in place to protect personal data and to adopt appropriate technical and organisational measures. Although the GDPR has been described as a game changer for data protection and privacy law, requiring substantial forward planning for every organisation, if organisations are already complying with the Data Protection Act, they may need to simply make tweaks to their current procedures.

SIGBI Limited is already registered with the Information Commissioner's Office and has such has complied with Data Protection to date. SIGBI HQ is diligent in not disclosing members' personal details without their prior consent.

The GDPR will come into force on 25 May 2018. The new Data Protection Bill repeals the Data Protection Act 1998 and incorporates the GDPR into UK law.

How does the GDPR apply to SIGBI LIMITED?

Every organisation in the EU will need to comply with GDPR and that means SIGBI Limited will need to review the impact of the Regulation on its operations and determine what changes have to be made to ensure compliance. There are no significant charity exemptions in the GDPR.

SIGBI LIMITED comes within the definition of *data controller* in the legislation, as a 'body, which determines the purposes and means of the *processing* of *personal data'*.

Processing means 'obtaining, recording, or holding information or data or carrying out any operation on the information or data". *Personal data* is 'information relating to a living individual who can be identified from that data (*data subject*).

Steps to take now

These are the steps SIGBI has taken:

1. Awareness – ensured the key people (staff and directors) in SIGBI Limited are aware that the law is changing to the GDPR. Compliance with GDPR has been placed on the Risk Register.

2. Audit – We have carried out an audit of the personal data currently held across the organisation. We have documented our answers to the following questions –
   - What personal data do you hold and where did it come from?
   - How is it stored (electronic/paper?) and where does it reside physically? (e.g. if you use a Cloud solution, where is the Cloud supplier based?)
   - What is the lawful basis for processing that data? (see below)
   - What have you told the data subjects about the processing you carry out?
   - What do you do with it and what are you planning to do with it?
   - Who do you share that data with? (see below)
   - How secure is that data?
   - How long is data held for and what is the reason for that time period?

   The GDPR mandates '*data protection by design'*. This means giving consideration to privacy and data protection compliance in the early stages of any new project (e.g. building a new IT system/developing policies that have privacy implications) rather than as an after-thought or ignoring these issues altogether.

The ICO says "We would like to see more organisations integrating core privacy considerations into existing project management and risk management methodologies and policies".

Privacy Impact Assessments (PIAs), referred to as Data Protection Impact Assessments in the GDPR, are an important way of showing a *'data protection by design approach'.* They are a tool for identifying and reducing the data protection/privacy risks of projects.

3. Privacy information. We have reviewed current privacy notices and put a plan in place to make any changes required by GDPR. We plan to explain (to Members/employees/others) the different ways information will be used, what we will not do with the data, how we will ensure its security, how Members/employees may access their data and how to make a complaint.

4. Individual rights – SIGBI has considered all of the rights (see below) and how we would ensure these can be met. For example, how we would deal with a subject access request.

5. Data breaches – we have put in place procedures to detect, report and investigate a personal data breach.

6. Person Responsible – SIGBI will designate someone to take responsibility for data protection compliance and assess where the role sits within SIGBI Limited's structure and governance arrangements.

NB. It is best not to use the term 'data protection officer' as this carries with it statutory responsibilities and there is no legal requirement for SIGBI Limited to have a data protection officer.

GDPR in detail

The GDPR outlines 6 principles that should be applied to any collection or processing of personal data. Fundamentally, if SIGBI Limited can demonstrate that we are meeting these requirements, we will be in a good position to meet GDPR compliance requirements. Note that the GDPR places greater emphasis on the documentation that data controllers must keep in order to demonstrate compliance with all of the principles.

Taking each in turn illustrates how GDPR will apply to SIGBI Limited:

1. PERSONAL DATA MUST BE PROCESSED LAWFULLY, FAIRLY AND TRANSPARENTLY

Registration with the ICO

To process data ***lawfully,*** under the Data Protection Act 1998 (DPA), all *data controllers* are currently required to register with the Information Commissioner's Office (ICO) in order to be included within the ICO's public register of data controllers (available on the ICO website), unless an exemption applies. Currently the registration has to be maintained on an annual basis and there is an annual fee. This fee structure is likely to change when the new GDPR comes into force and the requirement to register is likely to go but may be replaced with an alternative regime under the ICO. SIGBI Limited is already registered with the ICO.

Conditions for processing

In order for processing to be **lawful** under the GDPR, we need to identify a lawful basis before we can process *personal data*, referred to in the GDPR as *'conditions for processing'.* The legal basis identified has an effect on individuals' rights (see below), e.g. relying on consent to process data means the individual will generally have stronger rights, e.g. to have data deleted.

You don't need consent for every use of personal data, but if you don't have consent, you need to know what other legal justification you have that allows you to use the data. It is important that you determine your lawful basis for processing data and document this.

The *conditions for processing* that may be relevant to SIGBI Limited's processing of personal data are:

(i) Consent of the data subject

CONSENT UNDER THE GDPR

- The GDPR sets a high standard for consent. SIGBI needs to ensure it has *clear and unambiguous consent.*
- Consent should be in a separate form/document to other terms and conditions of business and the consent document should be laid out in simple terms.
- Pre-ticked opt-in boxes are specifically banned.
- Consent must be given to each separate processing activity (e.g. if you wish to carry out 6 different actions, the data subject must consent to all of them).
- You must keep clear records to demonstrate consent (who consented, when, what they were told at the time, how they have consented and whether they have withdrawn consent).
- The data subject should be informed of their right to withdraw consent and it should be easy for them to do this.
- Children under 16 are no longer able to give consent.
- You must name your organisation and any third parties who will be relying on the consent (e.g. outsourced payroll or outsourced shredder company that disposes of confidential waste etc).
- There should be no imbalance of power in the relationship between the individual and the organisation (so it is better to rely on an alternative *lawful condition for processing* for employment matters – see below).
- The GDPR makes clear that organisations can rely on existing consents given and there will be no need to seek fresh consent **but** the consent requests must already meet the GDPR standard and be properly documented.
- If your existing consents do not meet the GDPR high standards or are poorly documented you will need to (a) seek fresh GDPR compliant consent, or (b) identify a different *lawful condition for processing* or (c) stop the processing.

(ii) The processing is necessary for the performance of a contract (for staff details – the contract of employment).

(iii) The processing is necessary for the purposes of legitimate interests pursued by SIGBI Limited (including commercial benefit) unless this is outweighed by harm to the individual's rights and interests.

Most of SIGBI Limited's processing of personal data relating to members falls under this condition of processing, it being required by SIGBI Limited to enable it to carry out its functions as a membership organisation.

The *conditions of processing special categories of data* (e.g. religious beliefs, racial or ethnic origin or alleged criminal activity and criminal record) include:

(i) Explicit consent of the data subject.

(ii) For the purposes of carrying out obligations under employment law.

(iii) The processing is carried out by a not-for-profit body with a religious aim provided the processing relates only to members (or those who have regular contact with it in connection with those purposes) and provided there are no disclosures to a third party without consent).

(iv) Processing is necessary for the establishment, exercise or defence of legal claims.

Fair and transparent processing

Even if an organisation has a legal basis other than consent for sharing data, it still needs to tell people what it is doing with their data in order for the processing to be **fair and transparent** (unless there is an exemption from this in data protection legislation).

When collecting personal data organisations currently have to give people certain information, such as their identity and how they intend to use their information. This is usually done through a ***Privacy Notice***. Under the GDPR there are some additional things we need to tell people including, our lawful basis for processing the data, our data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way we are handling their data. The information must be provided in concise, easy to understand and clear language.

This information will appear on the website and will be included in employment contracts.

2. PERSONAL DATA CAN ONLY BE COLLECTED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

(See below Right to Information).

3. PERSONAL DATA MUST BE ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY FOR PROCESSING

This requires data minimisation – collecting only what is necessary for the particular job and retaining a minimum amount of data.

4. PERSONAL DATA MUST BE ACCURATE AND KEPT UP TO DATE

SIGBI Limited must have a method for ensuring details (such as addresses) are kept up-to-date. We should request evidence (e.g. in the case of a staff member, a marriage certificate for change of name) before changing details on our systems to prevent fraud.

5. PERSONAL DATA MUST BE KEPT IN A FORM SUCH THAT THE DATA SUBJECT CAN BE IDENTIFIED ONLY AS LONG AS IS NECESSARY FOR PROCESSING

It is important to consider what retention policy is suitable for the personal data we process. We need to consider commissioning software that allows information to be deleted in line with retention periods. We will consider how electronically stored personal data will be securely deleted, as well as hardcopies.

SIGBI Ltd, as part of its Data Protection Policy, has a data retention policy that specifies retention periods for different categories of information. For employee data, some data can only be kept for 12 months (eg. sick notes).

6. PERSONAL DATA MUST BE PROCESSED IN A MANNER THAT ENSURES ITS SECURITY

Internal Safeguards

The GDPR specifies protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate *technical or organisational* measures.

Any measures taken to secure data should be taken on the basis of a thorough risk assessment identifying any threats or vulnerabilities in the organisation. It is important to have an ***Information Security Policy*** and to carry out regular testing, assessing and reviewing of the effectiveness of measures taken.

Examples of *technical measures* are: anti-virus software on computers, back-up, firewalls, password protection, encryption, steps taken to stop cybercrime, hacking and other security compromises, robust IT systems etc.

Examples of *organisational measures* are: policies and procedures, business continuity plans, training for staff and volunteers, home working policy, telephone and email policy, laptop policy and procedure, social media policy, all coupled with staff discipline if there is a breach. SIGBI already has such policies and procedures in place.

Outsourcing

It is also important to ensure service level agreements/outsourcing arrangements are reviewed in line with the requirements of the GDPR. As a data controller, SIGBI Limited will be equally liable for any breaches that occur as a result of a supplier's failure to preserve data protection.

This means having robust information security practices in place for supplier contracts where the responsibilities and liabilities between the controller and processor are stipulated. It is important to audit processors (e.g. shredding company/cleaners) to ensure they can guarantee processing will be in line with the GDPR.

INDIVIDUAL RIGHTS

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act. The GDPR provides the following rights for individuals:

1. THE RIGHT TO BE INFORMED

The right to be informed encompasses our obligation to provide 'fair processing information', usually through a privacy notice.

The GDPR sets out the information we should supply and when individuals should be informed. The information we provide is determined by whether or not we obtained the personal data directly from individuals. The information must be concise, transparent, intelligible and easily accessible. It should be written in clear and precise language and be free of charge.

2. THE RIGHT OF ACCESS (SUBJECT ACCESS REQUESTS)

Individuals will have a right to obtain confirmation that their data is being processed and access to their data under the GDPR. These are similar to existing subject access requests under the DPA but there is less time to comply (without delay and within 30 days). In addition no charge can be made for complying with the request.

3. THE RIGHT TO RECTIFICATION

Individuals are entitled to have any inaccurate or incomplete personal data rectified and if you have disclosed the personal data to any third parties, you must also inform them of the rectification where possible. You must respond to a request for rectification within one month.

4. THE RIGHT TO ERASURE/ RIGHT TO BE FORGOTTEN

This is to enable individuals to request the deletion of personal data where there is no compelling reason for its continued processing but is only available in limited circumstances and is not an absolute right. There are extra requirements for the erasure of children's personal data.

5. THE RIGHT TO RESTRICT PROCESSING

When individuals exercise this right, you are allowed to store personal data but not to further process it.

6. THE RIGHT TO DATA PORTABILITY

This is unlikely to ever apply to SIGBI Limited. It is designed to enable easy transfer of data for consumers.

7. THE RIGHT TO OBJECT

Individuals have a right to object to processing based on legitimate interests. SIGBI Ltd must stop processing in these circumstances unless we can demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the individual or the processing is in relation to legal claims.

It is important to inform individuals of their right to object "at the point of first communication" and in our ***privacy notice.***

8. RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

This is unlikely to ever apply to SIGBI Limited. It is designed to be a safeguard against potentially damaging decisions being taken without human intervention.

DATA BREACHES

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to *personal data.*

The Regulation mandates informing both the ICO and the *data subject* themselves in certain circumstances. A process must be in n place to make these notifications in event of a breach. Data breach reports must be made within 72 hours of the *data controller* becoming aware of the breach. The notification must be in a specific format and should include a description of the measures taken to address the breach and mitigate its possible side effects.

SIGBI Data Protection Policy

Data Protection legislation means the Data Protection Act 1998, the Privacy and Electronic Communications Regulation (EC Directive) Regulation 2013 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the information Commissioner's Office.

The Data Protection Legislation ("the Legislation") is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of SIGBI Limited ("we") will collect, store and process personal data about our members, people who use our services and attend our activities, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in us. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held by the SIGBI Executive Officer, SIGBI HQ, 2nd Floor, Beckwith House, 1 Wellington Road North, Stockport, SK4 1AF, Tel: 0161 480 7686, Email: hq@sigbi.org

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

Processing Personal Data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Employees and others who process data on our behalf should assume that whatever they do with personal data will be considered to constitute processing. Individuals should only process data:

- If they have consent to do so; or;
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll;
- If neither of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly and lawfully;
- be obtained for specified lawful purposes and used only for those purposes;
- be adequate, relevant and not excessive for those purposes;

- be accurate and kept up to date;
- not be kept for any longer than required for those purposes;
- be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected);
- be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction;
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

Monitoring the use of Personal Data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All employees must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the Executive Officer in January every year. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling Personal Data and Data Security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Manual records relating to members or staff will be kept secure in locked cabinets. Access to such records will be restricted. Computer files will be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop should be password protected.

The Rights of Individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the SIGBI Executive Officer in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

Sensitive Data

SIGBI will not normally request sensitive data, but in the event that such data is obtained, we will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

SIGBI Data Retention Policy

Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

2. Data and records which are active will be stored in the most appropriate place for their purpose commensurate with security requirements.

3. Data and records which are no longer active, due to their age or subject, will be stored in the most appropriate place for their purpose.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

5. Any data file or record which contains personal data of any form can be considered as confidential in nature.

6. Data and records will not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose ***"shall not be kept for longer than is necessary for that purpose".***

7. Any data that is to be disposed will be securely disposed of, for example by shredding.

8. Special care will be given to disposing of data stored in electronic media.

Guidelines for Retention of Personal Data (this is not an exhaustive list)

If you have any queries regarding retaining/disposing of data please contact the SIGBI Executive Officer

Types of Data	Suggested Retention Period
Personal Files including: Training Records Grievance/Disciplinary Hearing Notes	• 6 years from end of employment
Applications Forms/Interview Notes	• Maximum of one year from the data of the interviews for those not subsequently employed. • If employed, retain in personnel file.
Information relating to children	• Check for accuracy once a year. • Record that child was a member of the group – permanent. • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member.
Member Information	• Check for accuracy once a year (Annual Return). • Record that adult was a member – permanent. • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member.
Income Tax and NI Returns, including correspondence with tax office.	• At least 6 years after the end of the financial year to which the records relate.
Statutory Maternity Pay Records and Calculations	• As above. • (Statutory Maternity Pay (General) Regulations 1986.
Statutory Sick Pay Records and Calculations	• As above. • Statutory Sick Pay (General) Regulations 1982.
Wages and Salary Records	• 6 years from the tax year in which generated.
Accident Books and Records/Reports of accidents.	• For Adults – 3 years after the date of the last entry. • For Children – 3 years after the child attains 18 years (RIDDOR 1985).
Health Records	• 6 months from date of leaving employment. • (Management of Health & Safety at Work Regulations).
Health Records where reason for termination of employment is connected with health, including stress related illness.	• 3 years from date of leaving employment. • (Limitation period for personal injury claims).
Student Records, including academic achievements and conduct.	• At least 6 years from the date the student leaves in case of litigation for negligence.

SIGBI Data Breach Policy

Introduction

SIGBI Limited ("we", "us") hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

Purpose

This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the organisation.

Scope

The policy relates to all personal data held by us, regardless of format. It applies to anyone who handles this personal data, including those working on our behalf. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident

Any person using personal data on our behalf is responsible for reporting data breach incidents immediately to the SIGBI Executive Officer, or in her absence to the SIGBI Membership Officer.

The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery

The Executive Officer will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment

An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The SIGBI Executive Officer will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences.

Notification

The SIGBI Executive Officer will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website:
www.ico.org.uk/media/1536/breach_reporting.pdf

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks. The SIGBI Executive Officer will keep a record of all actions taken in respect of the breach.

Evaluation and response

Once the incident is contained, the SIGBI Executive Officer will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

Data Breach Report

Date and Time of Discovery of Breach	
Name of Person Discovering Breach	
Nature of Personal Data Involved	
How Many Individuals' Data is affected	
Assessment Carried Out By	
What actions were taken?	
Further Investigation/Advice required?	
Resolution	

Signed by: **Date:**

SIGBI Data Protection Complaints Process

SIGBI Limited ("we") take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the SIGBI Executive Executive without delay. She can be contacted as follows:

Phone number 0161 480 7686

Email address hq@sigbi.org

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Any complaint received by us must be referred to the SIGBI Executive Officer who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.

2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.

3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.

4. At the conclusion of the investigation the SIGBI Executive Officer will reflect on the circumstances and recommend any improvements to systems or procedures.

SIGBI Information Security Policy

The Data Protection Act says that:
"Appropriate technical and organisational methods shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This is the seventh data protection principle. In practice, it means SIGBI must have appropriate security in place to prevent the personal data we hold being accidentally or deliberately compromised.

SIGBI Limited will:

1. Organise IT security to fit the nature of the personal data we hold.
2. Ensure we have the right physical and technical security in place, backed up by robust policies and procedures.
3. Train staff to ensure adherence to GDPR.
4. Respond to any breach of security swiftly and effectively.

The Act also states we should have security that is appropriate to the nature of the information in question; and the harm that might result from its improper use, or from its accidental loss or destruction. However, it does not define "appropriate".

Our data is currently held off site on remote servers. Data is protected by encryption software, anti-virus software, firewalls and daily back-ups. Staff access data via the use of unique passwords which are changed on a regular basis.

Staff are trained not to diverge personal data over the telephone or via electronic means, unless consent has been given to do so.

SIGBI's Business Continuity Plan and Risk Register are included as part of its security processes and procedures.

SIGBI Data Protection Compliance Questionnaire

Please tick appropriate box

	Yes	No	N/A
Has the data subject been informed of processing?			
Has the data subject been informed of third parties to whom their data may be provided			
Has the data subject given their consent to the processing			
If the data subject has not given consent (or consent is not a sufficient ground for processing) is processing justified by data controller's legitimate interest			
If the data is sensitive data has the data subject given explicit consent			
Has the data subject been informed of the purpose(s) for processing			
Is there a clear ground for processing each item of data			
Is the information gathered no more than is necessary for the purpose(s)			
Are steps taken to ensure data is accurate			
Is there a system of rolling reviews to keep data up to date			
Is there a data retention policy			
Is there a justification for retaining the data for the period in question			
Has the data subject been informed of their right of access			
Is the level of security applied to the data appropriate to the risks represented by the nature of the data to be protected (give consideration to possibility of theft, malicious damage or corruption including computer viruses, unlawful access, accidental disclosure, loss and destruction)			
Are staff who deal with personal data aware of purposes for which it has been collected			
Are staff who process data aware of parties to whom they can legitimately disclose it			
Where consultants and contractors have access to the data is there a written statement in place governing their obligations regarding security and use of data			
Are appropriate measures in place for the secure disposal and/or destruction of personal data no longer required			
Where applicable has consent of the data subject been obtained to transfer personal data to countries outside the EEA			

Soroptimist International Great Britain and Ireland (SIGBI) Limited Privacy Notice

How SIGBI Limited ("we") use your information.

Your privacy is important to us. We are committed to safeguarding the privacy of your information.

Why are we collecting your data?

We collect your personal data to fulfil our role as a membership organisation, to monitor and assess the quality of our services, to fulfil our purposes and to comply with the law regarding data sharing. In legal terms this is called 'legitimate interests'. When it is required, we may also ask you for your consent to process your data. We do not share your information with others except as described in this notice.

The categories of information that we may collect, hold and share include:

- Personal information (such as name, date of birth, address, telephone number and email address).
- Characteristics (such as gender, ethnicity, language, nationality, country of birth).

Storing your data

We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. We will contact you annually to check that the information we are holding is accurate and that you agree to us holding it.

Who do we share your information with?

We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data

Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information contact the Executive Officer at SIGBI HQ – hq@sigbi.org

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

Your rights

Under the Data Protection Act 1998, you have rights as an individual which you can exercise in relation to the information we hold about you.

You can read more about these rights on the ICO website – see link below:
https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

Individuals applying for a grant under the Diamond Education Grant programme

When individuals apply for a grant under the Diamond Education Grant programme, they submit their information in an application form, provide details of their proposal and an outline of what the grant will be used for. Those who are awarded grants are asked to provide progress reports and/or a final report. Any personal information that is provided in the application will only be used for the administration and management of any grants that are awarded.

Job applicants, current and former SIGBI Limited employees

SIGBI Limited is the data controller for information provided during the process of recruiting staff and the retention of staff. All of the information provided during the process will only be used for the purpose of processing an application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information provided during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information provided will be held securely by SIGBI Ltd whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

We do not collect more information than we need to fulfil our stated purpose and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you do not.

We will ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. The recruitment panel will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information. If you do not provide it, it will not affect your application. This information will not be made available to anyone outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring panel shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.

Conditional offer

If we make a conditional offer of employment we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend our office with original documents, from which we will take copies.
- Proof of your qualifications – you will be asked to attend our office with original documents, from which we will take copies.
- You will be asked to complete a criminal records declaration to declare any unspent convictions.

We will contact your referees, using the details you provide in your application, directly to obtain references.

Final Offer

If we make a final offer, we will also ask you for the following:

- Bank details – to process salary payments.
- Emergency contact details – so we know who to contact in case you have an emergency at work.
- Application to the SIGBI Limited Pension Scheme – after qualifying period.

Employee Information

If you are successful, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment, plus 6 years following the end of your employment. This includes your criminal records declaration, fitness to work, records of any security checks and references.

If you are unsuccessful at any stage of the process, the information you have provided until that point will be retained for 6 months from the closure of the campaign.

Information generated throughout the assessment process, for example interview notes, is retained by us for 6 months following the closure of the campaign.

Equal opportunities information is retained for 6 months following the closure of the campaign whether you are successful or not.

Membership Communications

We would like to share your information with other Soroptimists both from SIGBI and the other three Federations and related companies, in furtherance of your membership.

If you do not want your information being shared in this way please contact the Executive Officer at SIGBI HQ – hq@sigbi.org

Promotional Communications

We would like to send you information about Soroptimist International Great Britain and Ireland (SIGBI) Limited, Soroptimist Trading Limited, Soroptimist International and other related organisations with whom we work, by post, email, telephone and SMS.

If you do not want to be contacted in any of the ways listed, please contact the Executive Officer at SIGBI HQ – hq@sigbi.org

Marketing

We would like to send you information about companies or special offers in the future. If you have consented to receive marketing, you may opt out at any time. You have a right at any time to stop us from contacting you for marketing purposes or giving your information to other parties.

If you no longer wish to be contacted for marketing purposes please contact the Executive Officer at SIGBI HQ – hq@sigbi.org

Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.

For further information visit www.aboutcookies.org or www.allaboutcookies.org

You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, in a few cases some of website features may not function as a result.

Websites

Our website contains links to other websites. This privacy policy only applies to this website. When you link to other websites you should read their own privacy policies.

When someone visits https://sigbi.org we use a third party service, Google Analytics, to collect standard internet log information and details of visitor behaviour partners. We do this to find out such things as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone and we do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

Security and Performance

SIGBI Limited uses a third party service, WordPress.com to publish blogs and materials on the SIGBI website and Conference websites. We use a standard Word Press service to collect anonymous information about users' activity on the website, for example the number of users viewing pages on the site and to monitor and report on the effectiveness of the site to help us improve it.

Changes to our privacy policy

We keep our privacy policy under regular review and will place any updates on this webpage. This privacy policy was last updated on 9 April 2018.

Contact Details:

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you, or if you would like to discuss anything in this privacy notice please contact the Executive Officer on hq@sigbi.org

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commission's Office at https://ico.org.uk/concerns/

If you need any further information please write to us at:

Soroptimist International Great Britain and Ireland (SIGBI) Limited
2nd Floor, Beckwith House,
1 Wellington Road North
Stockport
SK4 1AF
0161 480 7686
hq@sigbi.org
https://sigbi.org/