**[](http://sigbi.org/members/files/SI_Logo_GBI_landscape.jpg)**

**SI St Albans and District**

**GUIDE TO DATA PROTECTION**

***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.***

**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.

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 as well as incorporating some additional new provisions.

**How does the GDPR apply to the Club?**

Every organisation in the EU will need to comply with GDPR and that means SI St Albans and District will need to review the impact of the Regulation on its operations and determine what changes have to be made to ensure compliance.

SI St Albans and District 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 you should take immediately:

1. Awareness – ensure the key people (officers and members) are aware that the law is changing to the GDPR.
2. Audit - Carry out an audit of the personal data you currently hold across the organisation. You should document your 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? (For example, 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?

1. Privacy information – make sure you have a privacy notice on the Club website and that members who do not have online access have access to a hard copy. The Club needs to explain (to Members/others) the different ways information will be used, what we will not do with the data, how we will ensure its security, how individuals may access their data and how to make a complaint.
2. Individual rights – consider all of the rights (see below) and how the Club would ensure these can be met. For example, how the Club would deal with a subject access request.
3. Data breaches – put in place procedures to detect, report and investigate a personal data breach.
4. Person Responsible – designate someone to take responsibility for data protection compliance

NB. It is best not to use the term ‘data protection officer’ as this carries with it onerous legal responsibilities and there is no legal requirement for the Club 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.

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

**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 the Club’s processing of personal data are:

1. Consent of the data subject

**CONSENT UNDER THE GDPR**

|  |
| --- |
| * The GDPR sets a high standard for consent. The Club 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. * 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 processing. |

1. The processing is necessary for the performance of a contract.
2. The processing is necessary for the purposes of legitimate interests pursued by the Club (including commercial benefit) unless this is outweighed by harm to the individual’s rights and interests.

Most of the Club’s processing of personal data relating to members falls under this condition of processing, it being required to enable it to carry out its functions as a membership organisation.

**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.

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

(See below Right to Information).

1. **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 purpose and retaining a minimum amount of data.

1. **PERSONAL DATA MUST BE ACCURATE AND KEPT UP TO DATE**

The Club must have a method for ensuring details (such as addresses) are kept up-to-date. This will usually be done via annual membership renewal.

1. **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.

The Club as part of its Data Protection Policy, has a data retention policy that specifies retention periods for different categories of information.

1. **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.

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.

**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.

1. **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.

1. **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.

1. **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.

1. **THE RIGHT TO RESTRICT PROCESSING**

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

1. **THE RIGHT TO DATA PORTABILITY**

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

1. **THE RIGHT TO OBJECT**

Individuals have a right to object to processing based on legitimate interests. If the request is valid the Club 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.***

1. **RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING**

This is unlikely to ever apply to the Club. 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 where the breach may result in serious harm to the rights and freedoms of the data subject or the breach affects the personal data of a large number of data subjects. A process must be in place to make these notifications in event of a breach. Data breach reports must be made within 72 hours of the *data controller (the Club)* 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.