GDPR FREQUENTLY ASKED QUESTIONS

It is hoped that the following Questions and Answers will help your Club get ready for the new GDPR.

Q. What is the General Data Protection Regulation and when does it come into force?

A. On 25 May 2018, the EU General Data Protection Regulation (GDPR) comes into force. Accountability and transparency are driving forces to the GDPR. The rules of transparency and fairness have not changed from earlier legislation, but organisations are now obliged to account for what they do, why and how they do it.

Data Protection law is not that complex, it is based on a set of common sense principles and presents six conditions for processing data. Anyone who wants to process personal data must meet one of the six conditions. Sensitive data relating, for example, to health or sexuality must meet an additional set of conditions.

Q. Does my Club have to register with the Information Commissioner's Office in the UK?

A. No. The Data Protection Act provides exemption from registration with the ICO for some 'not for profit' organisations. Clubs are categorised as being established for not-for-profit making purposes and are exempt from registration.

A SIGBI Club may make a profit for its own purposes, which are usually charitable or social, but the profit should not be used to enrich its Members. Any money that is raised should be used for the Club's own activities.

Clubs should process data purely for the purposes for which it was established, notably:

- Establishing or maintaining membership.
- Supporting a not-for-profit body or association.
- Providing or administering activities for either the Members or those who have regular contact with the Club.

However, even though Clubs are able to claim an exemption they must still comply with the data protection legislation. Clubs are still obliged to respond in 30 days to a written request to provide the information.

Q. What does a Club need to do to prepare for GDPR?

A. The first thing to do is make all Members within your Club aware that the law is changing in regards to data protection. This can be undertaken at a Club meeting by setting aside a small amount of time to discuss data protection and how the new GDPR will impact on your Club. The Information Commissioner's Office has lots of information to assist you on its website: https://ico.org.uk/

Q. What is personal data?

A. Personal data is defined as information about a living individual from which they can be identified.

Q. What is sensitive personal data?

A. GDPR defines sensitive data as "special categories" which includes racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission by the data subject of any office or any proceedings for any offence that are currently ongoing.

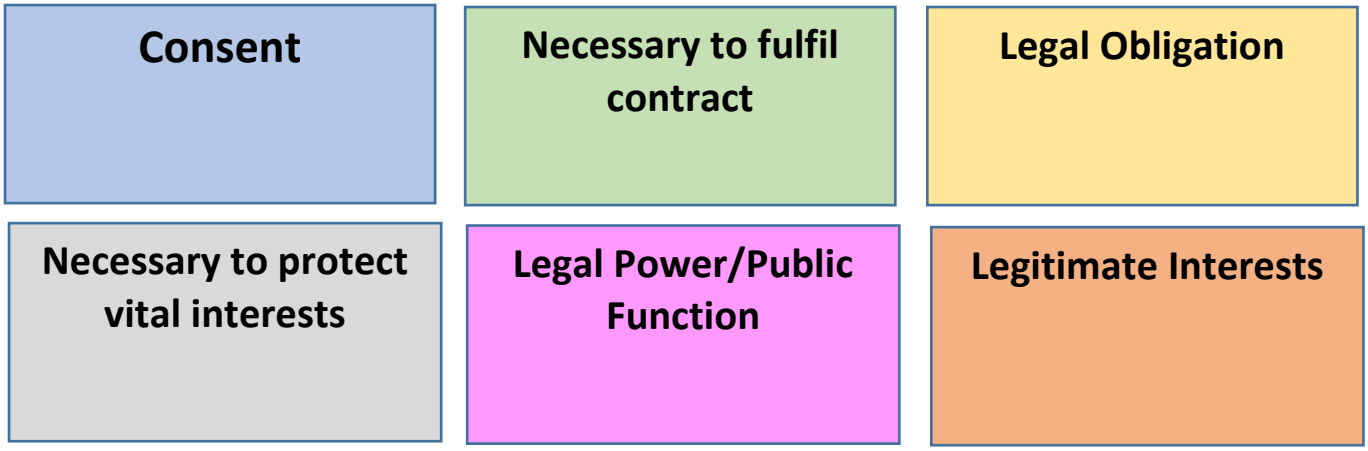
Q. What is a data audit and should my Club carry one out?

A. The purpose of a data audit is for the Club to be able to demonstrate that it has considered what personal data it holds and what is done with that data. An example of a Data Audit is attached as Appendix 1.

Q. Under what conditions is a Club allowed to process its Members' data?

A. There are six conditions to justify the processing of personal data found in Schedule 2 of the Data Protection Act and Article 6 of the General Data Protection Regulation.

The Club must satisfy one of the six conditions. If it cannot meet one of the six conditions listed below you cannot process personal data of Members.



Q. What is consent?

A. Consent is defined within the EU Directive as ***"any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed".***

Q. What does freely given mean?

A. In relationship to Club Membership, freely given means the Member must be given a free choice in the first place, and they must be able to change their minds at any time (the option to opt out).

Q. What does specific mean?

A. The processing of data to which the Member is agreeing to must be clear:

- What marketing are they going to receive?
- Who will it be from?
- Will it be shared with third parties?

Q. What does informed indication mean?

A. The Member needs to fully understand how her data is going to be used. If she does not, the consent is not valid. Language used should be easily understandable, clear and unambiguous.

You do not need consent for every use of personal data, but if you do not have consent you need to know what other justification you have that allows you to use that data.

Q. How do I as a Club Member give consent for my data to be used?

A. In future, there will be a 'box' on the 'New Member Form' asking the Member to give consent to her data being used for membership and marketing purposes. Consent will be for the duration of her membership or until such time as she opts-out.

Existing Members will be issued with a Privacy Notice, together with an accompanying letter from SIGBI HQ, informing them how their data will be used for membership and marketing purposes.

Q. What is a Privacy Notice?

A A Privacy Notice informs the Member how and why her data will be used in relationship to her membership. SIGBI's Privacy Notice may be found on its website https://sigbi.org/

As a Club you will need to consider the best way to inform your Members of the intention to use their data for membership purposes. If you hold email addresses for all Members it's likely that communicating with them by email will be sufficient.

A Privacy Notice should contain clear references to the following:

- Data sharing with other organisations – regardless of whether the data is sold or exchanged for free. If you do not intend to share data – the Privacy Notice should state this.

- Any research or profiling you may wish to undertake, regarding age, interests etc. – the Privacy Notice should state this.

You should make the Club's Privacy Notice easily accessible for anyone to view, for example by placing it on your Club's website.

It is not an explicit requirement under the GDPR to get proof that Members have received/acknowledged the Privacy Notice. You just need to ensure they have been provided with it in an accessible way.

Q. If a Club Member gives her consent for her data to be used, how long does that consent last?

A. The ICO's consent guidance says "***There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate".***

On the New Member's Form it will state that consent will be for the duration of her membership or until such time as the Member wishes to opt-out.

Q. As a member, what sort of marketing activities will my data be used for?

A. The ICO considers that any activities which promotes the organisation's aims and ideals are deemed to be "marketing". For example, you may receive an invitation to attend the annual SIGBI Conference, which would be deemed marketing.

Q. What does 'opt-out' mean?

A. Members must be given the option of "opting out" of allowing their data to be used for marketing purposes, or for sharing with a third party. A list of Members who have chosen to opt out must be kept.

Q. One of the six conditions justifying the processing of personal data is "necessary to fulfil contract", what does this mean?

A. This means that the data controller (Club) needs to process personal data in order to comply with a legal contract, for example recording information in order to pay a sole trader/supplier.

Q. What does "legal obligation" mean?

A. The question the Club needs to ask is ***"does the Club need to process personal data to comply with the law?"*** Given a Member's involvement in Club activities, it is unlikely their data will be required to comply with the law. The exception could be to comply with health and safety regulations when participating in events, eg a Member undertaking a risk assessment may be required to give their details to a third party.

Q. Would sharing Members' data be "necessary to protect vital interests"?

A. The GDPR suggests that this only applies to a life or death situation, so highly unlikely to be applicable for Members.

Q. Under what terms does the condition "legal power/public function" apply?

A. This provision only applies to public bodies.

Q. Does the condition of "legitimate interests" apply to Clubs?

A. Legitimate Interests is defined as ***"The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted by reason of prejudice to the rights and freedoms of legitimate interests of the data subject".***

In simple terms, the Data Controller (Club) collects the personal details of a Club Member for its own recording purposes for the legitimate purposes of running a Club. The Club then forwards this information to a third party (SIGBI Limited) for the legitimate purposes of running the Federation.

Q. What is a Data Subject?

A. The individual whose data you are holding. A Member must understand why you hold their personal data and how it will be used.

Q. What is a Data Controller?

A. The Club is the Data Controller, as it is the Club which determines the purposes of gathering and using the data of Members.

Q. Is SIGBI responsible for a Club's Data Protection?

A. No. Every Club is responsible for its own Data Protection. SIGBI Limited cannot be held responsible for a Club's failure to comply with GDPR.

Q. Who in the Club should be responsible for Data Protection?

A. Each Club should designate someone to take responsibility for data protection compliance. It is best not to use the term 'Data Protection Officer' as this carries with it onerous responsibilities and there is no legal requirement for Clubs to have a data protection officer.

Q. What are the principles of Data Protection?

A. There are six principles of Data Protection.

The First Principle states personal data must be processed lawfully, fairly and transparently. For Clubs the purpose of collecting personal data is in order to run the Club, for example to

- induct new Members
- prepare the Club's Annual Return.
- create a Club Directory
- organise an event
- fundraise

For Club records you should write down your purposes for collecting data, such as:

1. SI ????? wants to maintain a list of Members, so that we can contact them when necessary.
2. SI ????? wants to claim Gift Aid on a person's donations.
3. SI ????? wants to keep Members' information up to date.
4. SI ????? wants to submit its annual return to SIGBI.

The above are examples only, and your Club needs to make a note of all the purposes for which it holds personal data of Members.

"Fair" is described as "free from discrimination, dishonesty etc." or "in conformity with rules and standards". Put yourself in the shoes of the Data Subject and ask "How would I feel if this was my data?" As an ethical organisation we are used to being fair and considered.

Q. What is the Second Principle of Data Protection?

A. Personal data can only be collected for specified, explicit and legitimate purposes in terms of membership of your Club.

Q. What is the Third Principle of Data Protection?

A. Personal data must be adequate, relevant and limited to what is necessary for processing as a Member of your Club.

Q. What is the Fourth Principle of Data Protection?

A. Personal data must be accurate and kept up to date. The Annual Return will be pivotal in ensuring the accuracy and up to date data of Members.

Q. What is the Fifth Principle of Data Protection?

A. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. In the case of a Member, this is the term of membership of a Club.

Q. What is the Sixth Principle of Data Protection?

A. Personal data must be processed in a manner that ensures its security. Clubs must ensure that Members' details are secure and not at risk of being breached.

Q. If the Club receives a request of names and details from another Club, Region, National Association or Network, are we able to share this data?

A. Yes, providing you have the consent of Members. For example, if a Region wishes to create a Directory of Club Presidents and Secretaries, Clubs may provide this data, provided it has the consent of Members in those positions.

Q. What will happen to my data when I leave the Club?

A. A record of your details will be kept for three years after you have ceased to be a member. After that time secure destruction of personal data (other than name and fact of membership) will take place.

Q. What if I want all my details removing as soon as I leave?

A. You have a right to request erasure and to be forgotten. This enables individuals to request the deletion of personal data where there is no compelling reason for its continued processing; however, it is only available in limited circumstances and is not an absolute right.

You should contact your Club with your request. The Club should consider whether it is legally obliged to keep some information (for example attendance at an event) for a period of time. If in doubt the Club should take advice.

Q. On leaving the Club I am happy for the Club to maintain my personal details but I do not want my details sharing elsewhere. How can I ensure this happens?

A. Members have a right to restrict processing of their data. If you exercise this right, the Club is allowed to store personal data but not to share it.

Q. What are my rights as an individual Member?

A. 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 comprehensive guidance on the rights for individuals.

For example you have the right to be informed of the purpose for which your data is being processed. This encompasses the Club's obligation to provide 'fair processing information', usually through a privacy notice.

The GDPR sets out the information you should supply and when individuals should be informed.

Q. How can I be sure my data is being processed correctly?

A. As an individual you will be able to access your data via a Subject Access Request. This is similar to the existing subject access requests under the DPA but there is less time to comply (without delay and within 30 days). The Club cannot charge for complying with the request.

Q. What if the Club is holding incorrect data on my Membership record?

A. As a Member you are entitled to have any inaccurate or incomplete personal data rectified. If the Club has disclosed the personal data to any third parties, the Club must also inform them of the rectification where possible. Requests for rectification must be completed within one month from the data of the request being received.

Q. What if I want to join a Club but do not want to have my personal details stored by the Club.

A. The Club needs to process your personal details for the legitimate purpose of running a Club. If you do not want your personal details to be processed you would not be able to join the Club.

Q. What happens if my data is lost, stolen or disclosed outside of the Club?

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

In this situation and in some particularly serious breaches which involves large numbers of data subjects or the risk of serious harm to the data subjects, the Data Controller (Club) would be required to notify the data subjects and the ICO. The Club will need to have a process in place to make these notifications in event of a breach.

Data breach reports, if required, must be made within 72 hours of the Data Controller (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.

Q. What should the Club do in such circumstances?

A. The Club should carry out an investigation without delay and where possible within 24 hours of the breach being discovered. The Club 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.

The Club 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:

See the ICO website for breach reporting.

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 Club will keep a record of all actions taken in respect of the breach.

Once the incident is contained, the Club 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.

Q. My Club has paper membership records going back years. What should we do with them?

A. Your Club needs to create guidelines for the retention of personal data and secure disposal of the same. SIGBI's Retention Policy recommends that membership data is held for a maximum of 3 years after the member has left. On the third year anniversary of the member leaving her details are then securely destroyed. What is retained is a record of membership of the Club – but there are no personal details attached to that record other than her name.

Q. My Club retains membership information on a computer. Is this allowed?

A. Yes, providing you have consent from those involved. You should also have the necessary security precautions in place to ensure the data held is secure. Your computer should have the necessary virus, firewall, back up and password protection notices in place to protect the data you hold. You should take particular care to install any updates on a regular basis.

Data can only be held for the purpose for which it is collected and it is essential that data no longer required for its original purpose is securely disposed of.

Q. Will my Club still be able to produce a Club Membership Booklet detailing members, dates of meeting, speakers and venues etc?

A. Yes providing you have consent from those involved. Consent is the key issue regarding the sharing of data.

Q. Is my Club able to send details about our Members to Region, National Association, Network and Federation?

A. Yes providing all those involved have given consent for their data to be shared in this way. Remember your Privacy Notice is key to gaining consent.

This document aims to provide guidance for Clubs and the questions included are not an exhaustive list. As more questions are received, they will be added to this document. The Information Commissioner's Office (ICO) has lots of information to help you prepare and adhere to GDPR. It also provides an online and telephone help desk for your queries. Please see contact details below:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
https://ico.org.uk/