Data protection for your club

Find out more about the General Data Protection Regulation (GDPR), what it means for your club and what actions you need to take to comply with the law.

What is GDPR?

From 25 May 2018 the UK's existing data protection laws were replaced by the General Data Protection Regulation (GDPR). This gives EU citizens more control over how their personal data is used, especially online. All organisations who collect, store, share or use individuals' personal data, need to comply with the GDPR or face penalties, including hefty fines. This includes clubs. The key principles to bear in mind are:

- Data must be processed and stored securely
- Data should be updated regularly and accurately
- Data must be limited to what the club needs for the purpose for which it is collected
- Data must be used only for the purpose for which it is collected and
- Before using personal data, organisations must give people clear information about how it will be used in a privacy notice.

What do clubs need to do?

Clubs are 'controllers' of personal data for their members (eg. name, address, email address, telephone number, date of birth, etc). Clubs may also store personal data for people who have agreed to receive email communications.

GDPR requires that controllers set out a valid lawful basis for holding and processing personal data. While obtaining explicit consent or 'opting-in' is one of the six options available to do this, it is not required where processing personal data is necessary to provide a service that someone has signed up for, like membership of a club.

Clubs have a 'contractual', 'legal' and 'legitimate' basis for holding and processing members' personal data - we do not need to seek their additional approval. Instead, the law requires that these reasons are explained clearly to members, that we show we take their privacy seriously and offer options to manage communication preferences, where practical.

Step 1 - review your club's personal data needs & handling

You need to understand and record what personal data your club holds and the journey it takes through the club. It is a good idea to review this regularly and record these details.

Your club needs to be confident that all those people or organisations who have access to your members' personal data are aware of data protection regulations and handle that data securely. This may impact how your club Membership Secretary or Treasurer store membership forms or other records. You may wish to select a member of your committee to coordinate this.

Data security is key and when storing anything on a computer you need to ensure that you protect yourself by keeping passwords safe, ensuring that files are stored securely and encrypting files that

contain personal data. Many online systems including membership systems have built in security measures for the protection of files whilst in storage or in the process of being shared, but it is your responsibility to ensure that these are adequately secure.

All documents containing personal information shared by email between us should be password-protected before sending.

- Template data audit and recording table for clubs
- How to password-protect documents like spreadsheets that contain personal data

Step 2 - create a privacy notice

GDPR aims to ensure that individuals are more clearly informed by organisations that hold their personal data about how and why it is used, how long it is kept for, who it is shared with and what their rights are as data subjects. A privacy notice is the tool organisations use to set out this information.

Your club needs an up to date privacy notice.

Step 3 - share privacy notices with your members

It is important that all your club's existing members receive details of any updates to the club's privacy notice. This can be done by email and you should keep a record of how and when you share the privacy notice with your members. You do not need to ask for explicit consent or confirmation that the privacy notice has been seen or accepted.

Step 4 - update your membership (or other) forms

Your club must ensure that it only collects personal information that it really needs, and must share its privacy notice with new members (or other individuals) at the point of collecting their personal data, so they can make an informed decision to sign-up.

GDPR requires additional protection for the personal data of young people under 16 years old. If you collect children’s personal data, then you need to make sure that you obtain explicit consent from the parent or guardian to process the personal data.

Step 5 - get assurances from any third-party suppliers

There are obligations on data 'processors' as well as 'controllers' of personal data too. This may mean that if you use any third parties to process data, for example hosting your website, distributing emails, then you must have a written contract in place with those third parties that they will only use the data provide for the purpose of providing the agreed service to you.

Step 6 - be prepared for breaches or subject access requests

By following steps 1 and 5 here, clubs will minimise the risk that personal data in their control is lost or stolen. However, in the event of a 'breach' which puts personal data at risk, GDPR obliges controllers to report it to the Information Commissioner's Office (ICO) within 72 hours of being

aware of it. Make sure all members of the club with access to personal data are aware of this. We suggest that clubs designate a committee member to take responsibility for reporting any breach.

Another requirement of GDPR is that 'subject access requests' (requests for copies of personal data from individual club members) need to be responded to within one calendar month. To comply with this you must provide a copy of the personal data you hold for this person (after confirming their identity) in a commonly used format e.g. word document, .csv or excel file. We suggest that you keep a log of any requests of how and when you respond.