General Data Protection Regulation (GDPR) Update for Clubs – February 2018

Data protection laws are changing.

A new "General Data Protection Regulation" (commonly known as GDPR) will come into force on 25 May 2018, replacing the previous Data Protection Act 1998. This gives individuals more rights in relation to their personal data, whilst increasing the onus on organisations to keep personal data secure and only to use it for the purposes it is intended for.

This update is provided to Clubs by way of high level guidance only, and is not intended to be, nor should it be relied upon in substitution for, tailored legal advice.

Will this apply to your Club?

GDPR will apply to any 'data controllers' or 'data processors'. Essentially, this means that if you collect personal data in running your Club (which you definitely do if you have any members) then GDPR will apply to your Club. Personal data is data which relates to a living person. The most common types of personal data are things like:

1. Names
2. Addresses
3. Telephone numbers
4. Emails
5. Photos
6. Personal medical information
7. Criminal records
8. Bank details

How to prepare for GDPR?

Ahead of 25 May, there are several things you should start thinking about in order to assess your compliance with the new law:

1. Look at how you collect personal data from and about your members – are online or paper forms used? Is information saved in spreadsheets or other electronic documents? Do you inform members that you will be storing and using their personal data? Is the personal data stored on a laptop? Are passwords used to protect documents? Are there locks on any filing cabinets you might use?

2. Consider how you are using or sharing your members' personal data. Is it used for anything other than the running of your Club? For example, do you share it with third parties such as sponsors, or send messages or promotions on their behalf? If you are part of a multi-sports club, do you share personal data with other parts of that club? If so, have you obtained permission from your members to use their personal data for those purposes?
3. It is good practice to keep a record of what types of personal data are being collected, where they are stored, who has access to them and what they are used for.

These steps will give you a clearer picture of what personal data you, as a Club, collect and hold, and what you do with that personal data.

What are the key changes for your Club?

It's important to note that potential non-compliance fines under GDPR are much higher than under present data protection legislation, so it's in everyone's interests to familiarise themselves with the new law and make sure they handle personal data correctly and with care. More specifically:

1. You need to give people more information about what you do with personal data (and how you do it) at the point of collection. This could be achieved by having a policy document (written in clear, plain-English) for your club which clearly sets this out.
2. If you are sending marketing emails to your members, or sharing their personal data so that third parties can contact them, you should obtain explicit consent from each member that they are happy to receive these communications. Personal data can only be processed for the purpose for which it was collected. Simply being a member of your Club does not allow you to contact that member for marketing purposes without their express permission.
3. Certain types of personal data are particularly sensitive and must be handled carefully. This will include information relating to children, any member's medical information, and information about race, sexuality and religious beliefs. It is important that such data is stored securely and is only accessed by those people who strictly require to use it for the purposes of running the Club. You should consider whether it is strictly necessary to hold all of this sensitive information, as it should only be collected for a specific and legitimate purpose.
4. If you use third parties to process any of your data (for example, if a third party hosts your Club website) then make sure you have a written contract in place which includes a clause on data protection obligations and compliance.

5. Personal data should only be kept for as long as is necessary for the purpose for which it is collected. You should have a system in place for filtering out historic, unused data and deleting it. Your policy document should also explain to your members how long you will keep their personal data for. Destruction of hard copies of personal data should be done as securely as possible – preferable using a shredder.
6. GDPR puts an onus on organisations to report 'data breaches' to the Information Commissioner's Office within 72 hours of that breach taking place. A breach could be something obvious like a printed document containing members' names and addresses being left on a train, or a laptop where lots of personal data is stored being stolen. However, breaches can be less obvious, such as member data being seen by someone who does not have a right or need to see it. Given the tight time periods in place for reporting the breach, and the fines attached for failing to do so, you should familiarise yourself with what might constitute a breach, and consider a Club wide strategy for dealing with and reporting data breaches if they occur.

Next steps

1. Think about the personal data you are holding and how you can ensure you are complying with GDPR.
2. Ensure that GDPR is discussed by your Club's Board of Directors or Committee and that someone is responsible for considering the issues relating to your Club's compliance with GDPR.
3. Further helpful guidance about GDPR can be found via the Information Commissioner's Office website, which can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
4. The Welsh Sports Association has created a useful online resource for sporting organisations to assist them with their GDPR compliance, including some templates which can be used to create data protection policies. This can be found at http://wsa.wales/our-services/gdpr/ where you can enter the username - WRU001 and password - WSAWRU2017.