The General Data Protection Regulation (GDPR) 25th May 2018

Does this apply to our club?
If you collect any personal data in running your club (which you most likely will do) then the GDPR will apply to you. The GDPR applies to any data controllers or data processors.

Data controller, means any person who decides the reason for collecting personal data and how it will be used.

Data processor, means any person who processes the data on behalf of the data controller.

What are the key changes for SAA clubs?
More communication
We will need to tell people about how and what you do with their data at the point you collect it. The SAA will be doing this on behalf of clubs but if you also use your members data in any way you will need to tell them how you are going to use it i.e. sharing with other club members.

Responding to requests about personal data (subject access requests)
Requests for copies of personal data from individuals must be responded to within one calendar month rather than the current 40 calendar day period.

Obligations
There will be a direct obligation which may mean that if you use any third parties to process data, for example hosting your website, then you must have a written contract in place, and these are likely to be negotiated and drafted in favour of your processors.

Getting consent for processing data
You should review how you are asking for and recording consent. Consent also has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity. The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

Data retention (the length of time you store personal data)
Retention policies need to be clear. You can't keep data for longer than is necessary for the purpose for which it was collected. Personal data should only be stored to maintain a relationship with your existing members and associated individuals. You also need to inform people how long you will keep their personal data and you can't keep it indefinitely.

Privacy by design
If you are planning on putting in place a new system or electronic portal that will store members' details, then you need to consider whether the service provider you choose has adequate security to protect personal data.

Persona 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. This means that a breach is more than just losing personal data. You will only have 72 hours from being aware of a breach to report it to the ICO. Under the existing Data Protection Act there are no obligations to report breaches. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, under the new regulations you must notify those concerned directly.

Data transfer
One of the principles of the Data Protection Act 1998 (and the GDPR), is that you can only process data for the purpose for which it is collected. This means that if you collect a name and contact details of an individual, so that they can become a member of your club, you can't simply use that information to allow any third parties or sponsors to contact them for marketing purposes. You also need to tell people when they join your club if you are going to transfer their data, for example to an umbrella organisation. The SAA do not transfer members' data.

Subject access requests
Individuals have the right to access their personal data. The right of access allows individuals to be aware of and verify the lawfulness of the processing. You must provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request is unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information. Make sure you keep a log of how and when you respond and that you apply the exemptions from disclosure carefully.

Privacy or data capture statements
When individuals provide you with their details, make sure you are clear and transparent about why you have it and what you will do with their information. This means you need to make sure that you have the right data capture statements to present to individuals when they give you their personal details.

Children
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. In short, if your organisation collects information about children – in the UK this will probably be defined as anyone under 13 – then you will need a parent or guardian's consent in order to process their personal data lawfully. Remember that consent has to be verifiable and that when collecting children's data, your privacy notice must be written in language that children will understand.

Data breaches
You need to make sure that personal data is held securely, i.e. that electronic documents are encrypted and password protected and that they are backed up on a regular basis. You also need to make sure that your volunteers can identify when a breach has happened and that they know what they should do and who they should talk to.

Top tips to start your journey to GDPR readiness

1. **Process** – understand the journey that personal data takes through your club. What information do you collect and do you need that information? What do you tell people when you collect it? On what legal basis have you collected it (i.e. membership of your club) ? Where and how do you store that data? What do you do with it? When is it deleted? This will allow you to identify any areas of risk. Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

2. **Awareness** – make sure that your volunteers are aware of the GDPR and data protection issues and that they know who to talk to if they receive a request for information (subject access request) or if there is a breach.

3. **Policy** – make sure the policies and procedures you have in place help your volunteers deal with data protection issues.

4. **Communication** – make sure you tell individuals at the point of collection what you will do with their data and when you will delete it.

5. **ICO guidance** – take a look at the 12 steps to take now and the Getting ready for the GDPR self-assessment tools.

Further advice
The SAA will ensure that any data we hold on your behalf, or on behalf of your club, is dealt with securely. We will also ensure that any third parties, like our website providers, are also following the GDPR regulations.

If you have any questions about the GDPR, please contact Irene Sartorius at admin@saa.org.uk