GDPR Briefing - SCA Affiliated Clubs - April 2018

The General Data Protection Regulation (the GDPR) comes into force in the UK on 25th May 2018. Although this is EU legislation, the GDPR will be transposed into UK law and will replace current data protection law including the Data Protection Act 1998. It applies to all organisations regardless of size and status - therefore it applies to the SCA and to Affiliated Clubs.

Many of the principles that underpin the GDPR are the same as those on which the Data Protection Act was based. However the GDPR contains several notable differences and has an increased emphasis on the rights of individuals about how their data is provided to organisations and how it is used. There are also much larger fines for non compliance. Some of the main changes include:

Privacy Notices
Individuals have greater rights about being informed about how their data will be used (processed) by organisations. New Privacy Notices have been drafted for the SCA based on the GDPR and a template privacy notice has been drafted for clubs to use as a basis for their club privacy notices. When personal data is collected, the grounds for collecting it need to be made clear to the individual.

Grounds for Processing Personal Data
There are 6 grounds under which personal data may be processed:

1. **Contractual** Grounds - where data is necessary in order to carry out a contract. This could be where someone joins as a member or enters an event and it is necessary to collect and process data in order to administer the membership or run the event
2. **Legal Requirement** - this could be to do with Safeguarding or other legal necessity
3. **Vital Interests** - this could be collecting relevant medical data to look after the health and wellbeing of participants at an event
4. **Public Interes**t - where processing of data is considered to be in the public interest
5. **Legitimate Interes**t - where an organisation can demonstrate the need to process data e.g. event results
6. **Consent -** where consent is required for e.g. collecting data, consent must be given explicitly by the individual. There cannot be any pre-ticked boxes that we might have seen in the past.

Data Retention
The SCA has devised a Data Retention Policy setting out how long different types of data will be kept. Clubs should review the length of time they keep club member data and ideally explain to their members what will be kept and for how long. Some data needs to be kept for legal/other reasons whereas other types of data will be deleted to a set timetable to ensure that data is not kept longer than necessary.

Data Security
It is even more incumbent on us all to protect the data that we have access to - whether on an electronic device or on paper. This includes restricting access to devices and even specific files and thinking carefully before we transfer personal data to any other person or organisation.

Relationship between Data Controllers and Data Processors
If a club collects data the club is normally defined as being the “Controller” of that data. This includes club officials acting on behalf of the club e.g. committee members. If data is transferred to another organisation that organisation becomes a “Processor” of the club’s data. If you are going to transfer data to a third party you need to be able to trust the third party to keep the data safe and not to share it with other organisations without first gaining permission from the Controller of the data. When a club official enters details of their club members (who are not individual SCA members) into Go Membership then the Club is the Controller of that data and the SCA is a Processor of the data.

Contracts with Data Processors of Club Data
There needs to be a written agreement in place between a Controller of data and any other organisations that Process that data. For club members (who are not individual SCA members) the club is the Controller of the data and the SCA is the Processor of the data. Therefore an agreement will be put in place between each affiliated club and the SCA to cover this data processing.

Legal Requirements - Data Breaches
Each organisation is under obligation to maintain a register of all data breaches, no matter how trivial. For serious data breaches, where the breach is likely to result in a ‘risk to the rights and freedoms of individuals’, the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach and the data subject informed. Many clubs already have Data Protection Officers. It is recommended that all have a Data Protection Officer one of whose responsibilities will be to log any data breaches and if necessary inform the ICO. Please also inform the SCA Data Protection Officer immediately by emailing: sca.dpo@canoescotland.org

Additional Rights of Individuals
These include Subject Access Requests (where an individual requests data stored about them) and the right to be forgotten (where an individual requests to have their data erased by an organisation).