GDPR Guidance for BWSW Affiliates

Published April 2018

The **General Data Protection Regulation** (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union. The GDPR aims primarily to give control back to citizens and residents over their personal data - the GDPR comes into force on **25th May 2018** and it replaces the current 1995 Data Protection Directive.

FAQs – so what does GDPR mean for our affiliates?

What does GDPR mean for grassroots clubs?

GDPR is an important change in government legislation regarding data protection. It effectively brings in new requirements and increases the penalties for breaches. Any organisation that is required by law to comply with GDPR must do so by the 25th May 2018 at the latest.

Important - there are some key changes that will affect grassroots clubs that need to be addressed by the deadline date.

Does this apply to our club?

The GDPR applies to any "data controllers" or "data processors". Basically, if you collect any personal data in running your club (which you will do if you have any members or collect data on regular participants) then the GDPR will apply to you.

We are just a small voluntary members club – are we affected by the changes?

If you collect and store any personal data you will have to manage the data in accordance with strong data protection principles. The GDPR applies to all organisations whether commercial or voluntary irrespective of their size.

What are the key things to consider for grassroots clubs?

All clubs need to ensure that with regard to personal data that:

- they process it securely
- it is updated regularly and accurately
- it is limited to what the club needs
- it is used only for the purpose for which it is collected and
- used for marketing purposes only if the individual has given the club consent to do so

My club organises competitions, do we need to add anything to our entry form?

Yes, if data regarding a competitor or league member's results will be passed to another organisation to publish (either online or in print), the individual entering the event needs to be aware of this. So, if your club organises any events, to comply with the Data Protection Act, organisers should include appropriate wording on entry forms for example:

"By entering this event you agree that we may publish your Personal Information as part of the results of the Event and may pass such information to the governing body or any affiliated organisation for the purpose of insurance, leagues or for publishing results either for the event itself or combined with or compared to other events. Results may include (but not be limited to) name, any club affiliation, region, scores, date of birth and age category."

Our club is compliant with the current UK Data Protection Act so what is particularly new about GDPR?

More communication – your club will need to clearly inform people about how and what you do with their data at the point you collect it e.g. via a club renewal form.

For example, the following sample statement could be used for the administration of the sport at your club at the point you collect data. The activities where the data may be used and the organisations with which the data can be shared are clearly identified. Any statement should be included within your club privacy policy.

In becoming a member of [CLUB NAME], [CLUB NAME] will collect certain information about you which will include your name, date of birth, gender, email address, postal address, telephone number(s), names of any other affiliated clubs that you are a member of and details of any coaching, boat driving, competition data or officiating qualifications you hold.

The uses of any data should be made explicitly clear for example it is likely to include the following activities:

- ***Membership and club / centre management***

  Processing of membership applications / renewals and payments.

  Share data with committee members / staff members to provide information about club activities, membership renewals or invitation to social events or ability to assist with coaching and officiating at competitions.

  Publishing of any competition results.

  Website / online portal management.

  In order to complete any accreditation process where for example the qualifications and roles of staff members require the identification of those individuals via the sharing of data with the governing body.

- ***National Governing Body Member Registration***

  Registering your personal details with British Water Ski & Wakeboard for the provision of membership services e.g. personal accident insurance, membership card issue and mailing of magazines and access to discounts and other member benefits.

  For the registration / issue of qualifications, event entry, competition licences and the publishing of any competition results in any leagues and ladders.

- ***Training and Competition Entry***

  Share data with club coaches or officials to administer training sessions.

  Share data with club team managers to enter events.

  Share data with facility providers to manage access to the facility.

  Share data with leagues, other associations and other competition providers for entry in events.

- ***Marketing and communications (where separate consent is provided)***

  Sending information about promotions, offers and member benefits.

  Sending club newsletters.

  Sending information about selling club kit, merchandise or fundraising activities.

All clubs should have a privacy statement that outlines to an individual who is providing you with their data, details of exactly how it will be used. If someone isn't clear and you do not manage data in accordance with the policy, you are **increasing the risk** of breaching data protection laws.

Other changes that will be introduced by the introduction of GDPR include:

Responding to subject access requests
Subject access requests (requests for copies of personal data from individual club members) will need to be responded to within one calendar month rather than the current 40 day period. It is also no longer possible to charge £10 for dealing with the request. Subject access requests are often contentious - individuals usually make requests if they have something to complain about. Make sure you keep a log of how and when you respond to any request.

Obligations
There will be direct obligations on data processors as well as on data controllers. This 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.

Fines increase significantly under GDPR
Obviously, these fines are designed to ensure larger commercial organisations comply, but penalties exist **for all sizes** of organisation.

Obtaining consent
Consent will be a more onerous task. If you rely on consent from individuals to use their personal data in certain ways, for example to send marketing emails, then there are additional requirements to comply with. For example, if you currently have one opt in box for 'marketing information by email, post and SMS' under the new regulations 'email, post, SMS' would have to be separated out for individual consent for each method of communication. The individual providing their data therefore has greater control over the methods by which they are contacted.

Data retention
Retention policies need to be clear - you can't keep data for longer than is necessary for the purpose for which it was collected. You also need to inform people how long you will keep their personal data for and you cannot keep it indefinitely. For example, a member may not have renewed for 4 years - how likely is it that they will return? If the answer, is 'unlikely' then their core data should be deleted, or their record anonymised after that time.

Privacy and IT systems
If you are planning on putting in place a new IT system or electronic portal, then you need to consider whether the service provider you choose has adequate security to protect personal data.

Data Breaches
You will only have 72 hours from being aware of a breach to report it to the Information Commissioners Office (ICO). Under the current Data Protection Act there are no obligations to report breaches. For example, if a membership secretary holds the membership data on their laptop and it is not encrypted and is stolen the data is now at risk and a breach would have to be reported. 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 / staff members can identify when a breach has happened and that they know what they should do and who they should talk to.

Children
There are additional protections for children's personal data. If you collect children's personal data, then you need to make sure that your privacy policy is written in plain simple English and if you offer an online service to children, you may need to obtain consent from the parent or guardian to process the personal data.

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 other bodies (e.g. a commercial sponsor) 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.

Does GDPR only apply to data that is held digitally, e.g. on a computer, or does it cover paper records?

This may be a good opportunity to review filing systems and to limit the amount of paperwork you have to manage. Personal data collected manually and stored in files as hard copy still has to be managed in accordance with the data protection regulations.

My club keeps its membership records "in the Cloud" (e.g. via shared files on DropBox or Google Drive, or via a bespoke or commercially available membership system): what should I do about that data?

Data security is key and when storing anything online you need to ensure that you protect yourself by ensuring you keep passwords safe and ensure that files that contain personal data are encrypted. The likes of Dropbox, OneDrive and Google Drive have built in security measures for the protection of files whilst in storage or in the process of being shared. When using third party software you need to ask for assurances over the security of the system.

Tips to start your journey to GDPR readiness

Here are a few suggestions to help you get started:

- **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? 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.

- **Awareness** – make sure that your volunteers / staff members are aware of the GDPR and data protection issues and that they know who to talk to if they receive a subject access request or if there is a data breach.

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

- **Communication** – make sure you tell individuals at the point of collection what you will do with their data and when you will delete it. Ensure any joining / renewal information is clear and provide a privacy policy as standard.

- **ICO guidance** – the ICO also now offer a helpline. Representatives of small organisations should dial 0303 123 1113 and select option 4.

- **BWSW advice** - if you have any questions about GDPR then please email info@bwsf.co.uk.

The guidance provided here is aimed at assisting British Water Ski Federation Ltd affiliated organisations with identifying the key areas that they should be addressing as a result of the additional requirements arising from the upcoming introduction of GDPR. Our affiliates may already have considered (and where appropriate have taken specialist advice) regarding the impact of existing UK Data Protection legislation insofar as that may impact their activities. It is similarly recommended that clubs and associations take appropriate advice if they have concerns or are still in doubt regarding specific issues having read this FAQs document. There are some suggestions within this document as to where that advice may be sought, but those should not be viewed as exclusive.

Document History

April 2018	Version 1.0	CEO