What does the EU General Data Protection Regulation (GDPR) mean for sport's clubs and associations?

All Heads of Association and Coaches running clubs

YES, the GDPR applies to **YOU** and to anybody who processes data on your behalf (whether paid or not) If you collect any personal data in running your club in any form, paper records, index files or computer records (which you most certainly do, if you have any members, volunteers or helpers) then the GDPR will apply to you.

Key changes in the legislation

The new legislation is based on individual's rights and individual empowerment for the protection of their data, significantly higher standards of consent are required than before. The individual must provide clear, freely given, specific, informed and unambiguous consent for the organisation to process their personal data. The consent document should be laid out in clear simple terms; for us, in Chinese Martial Arts it means that your membership application form (which should be the document you use for data capture), will need to be modified before the Regulations become law on the 25th May 2018.

The definition of personal data has been significantly expanded. Please note that Parental / Guardian consent will now be required for the processing of personal data of children under age 16.

The appointment of Data Protection Officers (Mandatory for large organisations) will not be required by Clubs and Associations, as our core business activities are not data processing and are therefore exempt from this obligation.

Processes must be built on the principle of privacy by design, with the principles of protection of data built it from day one.

Responding to subject access requests

Subject access requests (requests for copies of personal data from individuals) will need to be responded to within one calendar month rather than the current 40 calendar day period. It is also no longer possible to charge £10 for dealing with the request. Data subjects can request a copy of personal data in a format usable by them.

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, and these are likely to be negotiated and drafted in favour of your processors.

Penalties under the GDPR

The Regulation mandates considerably tougher penalties than the DPA: organisations found in breach of the Regulation can expect administrative fines of up to 4% of annual global turnover or €20 million – whichever is greater. Fines of this scale could very easily lead to business insolvency. Data breaches are commonplace and increase in scale and severity every day. As Verizon's 2016 Data Breach Investigations Report reaffirms, "no locale, industry or organization is bulletproof when it comes to the compromise of data", so it is vital that all organisations are aware of their new obligations so that they can prepare accordingly.

Getting consent

Consent will be much harder to achieve. 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.

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 and you can't keep it indefinitely.

Breaches

You will only have 72 hours from being aware of a breach to report it to the ICO. Under the Data Protection Act there are no obligations to report breaches.

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 your affiliates 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.

Subject access requests

They are often contentious. Individuals only make requests if they have something to complain about. 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.

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? 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.

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 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. https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

References:

Many thanks to Muckle-llp.com for permission to use this document

https://www.muckle-llp.com/enews/gdpr-mean-grassroots-clubs/