GDPR:
Our best suggestions

Introduction
Data protection has hit the radar of sports organisations following high profile data leaks and cyber-attacks. The EU has reacted to these by drawing up the General Data Protection Regulation (GDPR), which is already in force and Active Sussex are in a period of implementation - with the deadline for compliance set at 25 May 2018.

It may sound like a while off, but there are some key changes that will affect sports clubs/organisations and need addressing. With Brexit anticipated for April 2019, current indications are that the GDPR will be applicable in the UK initially. Post-Brexit, the UK will have the option of developing its own law that is deemed adequate by EU Regulators (but which are expected to follow GDPR principles).

What are the key things to consider?
All sports clubs/organisations need to ensure with regard to personal data that:

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

Control of information
The GDPR applies to any data controllers or processors, so if you collect any personal data in running your club/organisation (which you definitely will do if you have any members) - then the GDPR will apply to you! Your organisations key decision makers should be aware of the changes which will be brought in by the GDPR. Data protection should be a boardroom issue and board level training made a priority. Identify who monitors data protection compliance, as you may need to appoint a Data Protection Officer.

Key changes for your organisation

1. More communication
You’ll need to tell people about how and what you do with their data at the point you collect it. Think about what information you collect and if 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. If you collect a name and contact details of an individual, so that they can become a member of your club/organisation, you cannot simply use that information to contact them for say marketing purposes.

2. Information Commissioners Office (ICO) notifications
You no longer have to notify the ICO as a data controller – you may already not need to under the current not-for profit legislation.

3. Responding to subject access requests
Subject access requests (appeals 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. They are often contentious and individuals usually make requests if they have something to complain about. Make sure you keep a log of how and when you respond – on a CRM if you have one.
4. **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.

5. **Fines increase significantly**

Currently the highest fine the ICO can levy is £500,000. Under the GDPR they will be able to issue fines up to 20 million euros or 4% of your global annual turnover (whichever is the higher) for serious breaches. The fine could be 10 million euros or 2% of your global annual turnover (whichever is the higher) for less serious breaches. Whilst smaller organisations will be fined for breaches, these will be proportionate. On the spot audits are possible, so make sure you are compliant!

6. **Getting consent**

Due to the need to ‘opt in’, consent will be much harder to achieve than in days gone by. 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. It is worth noting that regarding communications, separate consent is needed for the following:

- Sending details about promotions/offers from sponsors
- Sending out a newsletter
- Sending information about selling sports kit, merchandise or fundraising

7. **Data retention**

Retention policies need to be crystal 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 (e.g. after an event) as you can’t keep it indefinitely. With the increased attention on better data protection, potential members will look at your data policies and practices with more scrutiny. Don’t risk your club/organisations reputation with shoddy, outdated data governance. Your competitors, too, will be quick to take advantage of your failure to employ best practices, so update and keep your members’ trust.

8. **Privacy by design**

If you are planning on putting in place a new system or electronic portal, then you need to consider whether the service provider you choose has adequate security to protect personal data. Your club/organisation should assess the information that it holds, where it has come from and with whom it is shared. You could use a detailed questionnaire to ascertain what of the information gathered can then be used in a report to inform strategy and next steps. Study your data processing activities, identify your legal basis for carrying it out and document it.

9. **Breaches**

You will only have 72 hours from being aware of a breach to report it to the ICO. Under the Data Protection Act 1998, there were no obligations to report breaches. You need to make sure that electronic documents are encrypted and password protected and that they are backed up on a regular basis. You also need to ensure that your volunteers can identify when a breach has happened and that they know what they should do and who they should talk to. Failure to report a breach could result in a double fine – for the failure to report the breach and for the breach itself.

10. **Special Protection for Children**

There are additional restrictions placed on children’s personal data. If you collect it, then you need to make sure that your privacy policy is written in plain and simple English. If you offer an online service to children, you may need to obtain consent from their parent/guardian to process the information.

11. **Privacy or data capture statements**

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

12. **Sports clubs/organisations are not immune from cyber-attacks and data leaks**

Sport has become big business. Even smaller clubs/organisations handle substantial amounts of personal data – e.g. their members’ names, their bank accounts or credit cards when members pay subs, buy uniforms, or conduct other transactions.

GDPR offers a good opportunity to review internal policies, procedures, contracts & filing systems and limit the amount of paperwork you have to manage. Personal data collected manually and stored in files as a hard copy still has to be managed in accordance with the data protection regulations. Transportation of data in any format (including paper) should be seen as a threat to information security.

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 should ask for assurances over the security of the system.

*** Active Sussex’s TOP 10 Summary Checklist ***

Don’t risk huge fines and loss of reputation that could devastate your club/organisation. Use this checklist to make sure you are ready for GDPR compliance:

- Scan and shred as many hard copies as you possibly can
- Make sure that sensitive documents are filed immediately after printing
- Create anonymous print file names
- Avoid duplication of sensitive documents
- Encrypt data where possible
- Document changes to documents, as well as who changes them
- Update data often to keep it current and avoid errors
- Create stricter user permissions and protocol settings
- Review and update your club/organisations handling of children’s data
- Read the ICO guidance – take a look at the [12 steps to take now](#) and the [Getting ready for the GDPR](#) self-assessment tools