CLUBS

Briefing paper on the key changes under the GDPR for clubs

What is the GDPR?

The General Data Protection Regulation (EU) 2016/679 (the GDPR) will directly apply in EU Member States from 25 May 2018 and will govern how organisations use personal data and increase the protection of individual's privacy. There will also be a new UK Act to replace the Data Protection Act 1998.

Does it apply to clubs?

Clubs will be "controllers" of personal data (for example, name, address, date of birth) that they collect, store, use, share and delete (this is known as "processing" of personal data). Clubs will process personal data of their members, parents, volunteers, committee members, etc. The GDPR will apply to clubs, regardless of size.

The GDPR will even apply to clubs which are not incorporated (for example, as a company) as they will still process personal data, whether or not this is shared with anyone outside the club.

How do clubs prepare?

As controllers, clubs need to prepare for the GDPR. It may seem like a lot of work at first but using the **sport**scotland templates will help clubs and aim to reduce the burden of the GDPR for clubs when it comes into force.

Data protection principles

The GDPR includes six data protection principles that clubs need to be aware of whenever they are using personal data (for example, signing up a new member, sending an email to a volunteer, etc.).

In order to comply with these principles, clubs need to:

1. ensure they identify a lawful basis to process the personal data (from the list set out in the GDPR) and provide a privacy notice to the individual, which tells individuals how the club uses their proposal data (one of the templates provided);

2. only collect, use and keep personal data for specific purposes – i.e. only use a member's personal data for membership purposes;

3. only collect, use and keep personal data that clubs actually need;

4. keep personal data up-to-date where possible;

5. only keep personal data for as long as clubs need it – i.e. when a member leaves a club, clubs should review all the member's personal data held to see whether they still need it after a specific period of time (for example, three years); and

6. protect personal data and keep it secure.

Paper or electronic records?

The GDPR is mainly concerned with electronic personal data. However, if a club uses a paper filing system that allows information to be picked from specific criteria then the GDPR will apply to this paper filing system.

Most clubs will use email and any personal data included in emails will be caught by the GDPR.

Lawful basis for processing

There is a specific list of "lawful bases" for processing personal data in the GDPR and clubs will need to identify which one applies before collecting and/or using personal data.

Once clubs have identified their lawful basis, they must explain this to individuals in privacy notices.

What is the lawful basis for members' personal data?

When processing members' personal data (for example, membership admission, membership fee payments, AGMs, etc.) clubs will have a "contractual" lawful basis.

This is because the club needs to use members' personal data to comply with the terms of their membership and the club should only use such personal data for this purpose.

A club may also be legally required to process members' peronal data for specific purposes, for example, health and safety. This lawful basis is known as the "legal obligation" lawful basis, as it applies when a controller needs to use personal data to comply with a legal obligation.

What is the lawful basis for employees' personal data?

Again, clubs will have a "contractual" lawful basis as employees will have a contract of employment and clubs should only use employees' personal data to comply with their obligations under that contract of employment.

Clubs will also need to process employees' personal data for legal reasons under the "legal obligation" lawful basis. For example, clubs will need to report details of employees' income to HMRC for tax reporting purposes.

What are "legitimate interests"?

Another lawful basis is where the club (or a third party) has legitimate interests for processing personal data. However, the catch with this lawful basis is that any such legitimate interests cannot be outweighed by the interests of the relevant individual.

This might apply where clubs issue newsletters to members / other individuals or communications promoting upcoming events / competitions, which is seen as 'direct marketing'. Clubs should always make sure that individuals can stop receiving such newsletters or communications by contacting the club.

What about asking for consent?

Asking individuals if they consent to the club using their personal data is a lawful basis under the GDPR. However, there are specific requirements for asking for consent, which means it will be more difficult going forward and clubs should use one of the other lawful bases if more appropriate.

If clubs do want to ask individuals for consent then they must use a consent statement that:

- is a clear affirmative action: opt-in rather than opt-out and no pre-ticked boxes;
- is separate from other terms and conditions and not a precondition of signing up to a service;
- provides granular options for different processing operations; and
- is easy to withdraw.

Where clubs use social media pages, it is likely that social media websites will have updated privacy policies as the providers will consider that they are controllers. Clubs should hopefully not notice much of a difference. However, clubs are advised to check these privacy policies.

What about "special category personal data"?

Special category personal data, is a separate category of personal data under the GDPR and includes data revealing a person's racial or ethnic original; health; sex life or sexual orientation; or religious or philosophical beliefs.

Where clubs process special category personal data they must have a lawful basis and meet at least one condition for processing special category personal data. The template privacy notice wording include some examples of these conditions and we would recommend that clubs seek advice if they process other special category personal data and want to check the conditions.

There will also be separate conditions in the new UK Act for processing personal data relating to actual or alleged criminal offences, which are still to be finalised.

Privacy notices

A "privacy notice" is a statement by a controller explaining to individuals what they do with personal data. Clubs have access to template wording for privacy notices, including: general wording with examples for members and participants and wording for employees. There is also an example of a completed member privacy notice.

When do we need to give people privacy notices?

When collecting or receiving personal data from anyone, clubs must give a privacy notice to the individual whose personal data the club is processing. For example, the privacy notice should be included in applications for membership, membership renewal forms, booking forms, and employment / volunteer forms.

Clubs should also put their privacy notices on their website and can provide individuals with the link to the relevant page.

What needs to be included in a privacy notice?

The templates set out all of the headings that the GDPR states should be in a privacy notice. However, the text under the headings can be tailored by clubs. It is important for clubs to cover all of their data processing activities in privacy notices.

If clubs pass membership data or other personal data to SGBs, the SGB will become a controller of that personal data in most cases. The clubs' privacy notice must tell individuals that the SGB will receive their personal data and become a controller of it. This could also apply to other third parties.

If clubs publish any personal data on a website or within a clubhouse then this must be stated within the privacy notice.

Rights of data subjects

Individuals (known as "data subjects") have certain rights regarding their personal data under the GDPR. Clubs will need to consider requests from data subjects and provide a response within one month.

We would recommend that if a club receives a request from an individual and it is unsure how to respond, it should take advice. Clubs need to be aware of the one month timescale and make sure that they comply.

Data subjects can ask clubs to:

1. provide a copy of their personal data and information on how the club processes the data (basically what is included in a privacy notice – a "subject access request";

2. correct or complete any incorrect or incomplete personal data held by the club – the "right to rectification";

3. delete all personal data held by the club (only in some circumstances) – the "right to erasure";

4. stop or limit the processing of their personal data (only in some circumstances) – the "right to restrict processing"; and

5. provide all personal data in a particular format for their re-use (only in some circumstances) – the "right to data portability".

Data subjects can also object to a club processing their personal data, which is known as the "right to object". This right only applies in some circumstances – for example, members can object to receiving the club's newsletter and the club should stop sending the newsletter to the member immediately.

Data processing

If clubs use any third-party suppliers they should check if they are given or have access to any personal data held by clubs as such suppliers are defined as "processors" under the GDPR. Clubs may use suppliers to send mailshots, administer online systems, process payments, host websites, online surveys, etc.

Clubs should have such suppliers sign the template data processing agreement or enter into a contract or terms and conditions, which includes the template data processing clause.

Accountability principle

The GDPR requires controllers to be responsible for and be able to demonstrate compliance with the data protection principles – 'accountability'. This principle will apply to clubs, who will need to keep records of their processing activities – i.e. details of what they use personal data for.

There is an exemption for controllers with less than 250 employees and guidance is awaited regarding the scope of this exemption. For clubs, this will mean that they only have to keep records of data processing activities that: are not occasional; could result in a risk to the rights and freedoms of the individuals; or involves special category personal data or data relating to criminal convictions or offences.

It is likely that clubs will need to keep a record of what and how they process personal data for members, employees, volunteers, participants as they do this on a regular basis.

What information do clubs need to keep?

Clubs should keep a document recording (such as a spreadsheet or table) the following:

- the purposes of processing – for membership, competitions, lessons, etc.;
- the categories of individuals and personal data – members, volunteers, etc. and name, address, date of birth, etc.;
- the categories of recipients – details of who the club shares personal data with, such as SGBs, etc.;
- details of if any personal data is transferred or hosted outwith the EU and safeguards – for example, MailChimp, which has Privacy Shield certification;
- retention periods – how long different records of personal data are kept; and
- details of security measures in place to keep personal data secure – for example, passwords, locked cabinets, restricted accounts, etc.

Clubs should also keep copies of privacy notices and consent statements so they can evidence that these have been provided to individuals.

Breaches

If a club loses personal data or suffers a data security incident then this would result in a personal data breach. Examples of breaches include: access to personal data by an unauthorised person; sending personal data to the wrong person; or losing computer or mobile equipment containing personal data.

If the breach is severe and could affect individuals (i.e. – risks their rights and freedoms) then clubs will be under an obligation to notify the Information Commissioner's Office (the ICO) within 72 hours of becoming aware of a breach. Clubs will also have to notify the affected individuals if there is a risk to their rights and freedoms.

If a club fails to notify either the ICO or affected individuals of a breach when required to do so, they could suffer a significant fine.

Sanctions

Clubs that breach the GDPR may be liable to a large fine (£20m or 4% of annual turnover (whichever is greater) for serious compliance failures). Individuals can also sue clubs for compensation.

Accordingly, it is important for clubs to prepare for the GDPR to reduce the risk of breaching it.

Action plan for Clubs

1. Identify all personal data is held by the club and what it is used for – create a table or spreadsheet, which can be used to maintain the required records of processing activities.
2. Use the template wording to create privacy notices and update club forms, websites, etc. to include the new privacy notices and issue these to current members, employees, etc.
3. Ensure that everyone within the club with access to personal data held by the club has a basic understanding of data protection and the club's obligations under the GDPR.
4. Adopt higher standards of data security – for example, create specific club email accounts to limit the use of personal email address for club business.
5. Use the template wording to get suppliers to sign up to written data processing contracts.

This briefing paper represents the proposed law and guidance as at 1 March 2018.