Data Protection & GDPR

Guide for Rugby Clubs in Scotland

This document is provided by the Scottish Rugby Union Limited ("Scottish Rugby") for guidance purposes only and not for the purposes of providing professional advice. Contents are believed to reflect law and practice in Scotland, but this document is not intended to be a statement of law. Scottish Rugby accepts no duty of care, responsibility or liability to any person, whether arising by way of negligence or otherwise, for any errors, omissions, or misleading statements within this document or within any links contained in this document, nor for any action or inaction of any person due to reliance on the contents of this document or any links contained in this document. This document is written in general, non-exhaustive terms and does not cover individual or specific situations. All persons *must* seek their own independent professional advice before making any decisions relating to the subject matter of this document.

What is the GDPR?

The General Data Protection Regulation (EU) 2016/679 (**GDPR**) will apply from 25 May 2018 and will be implemented in the UK from that date by the Data Protection Bill (replacing the Data Protection Act 1998).

The GDPR builds on existing data protection law and provides individuals with increased rights and transparency in relation to their data. The GDPR also places increased obligations on clubs in respect of data processing activities such as holding, using, sharing, securing and deleting personal data and requires clubs to be more accountable for such activities whilst being able to demonstrate ongoing compliance.

In the UK, the data protection regime is monitored and enforced by the Information Commissioner's Office (ICO). More detailed guidance and information in respect of data protection generally can be found on the ICO's website at https://ico.org.uk/.

Does the GDPR apply to rugby clubs?

Yes. Clubs will be "**controllers**" of the "**personal data**" that they collect, hold, use, share and delete.

Collecting, holding, using, sharing or deleting personal data is known as "**processing**" personal data. By processing personal data, the GDPR will apply to all clubs regardless of size and regardless of whether a club is incorporated or not (for example as a company).

"**Personal data**" is any information that relates to and can either directly or indirectly identify a living person (for example a player, volunteer, member, coach, referee or employee). This could therefore be somebody's name, address, email address, bank account or payment details, medical history or sporting history.

Personal data could be held by a club in either paper or electronic form through emails, membership lists, club spreadsheets, committee minutes, websites, disciplinary judgments, member application

forms etc. Personal data could be held at a club's premises, or on individuals' own equipment at their homes.

Each club must therefore comply with the GDPR and will itself be liable for any breaches of the GDPR as a data controller. Breaches will not be Scottish Rugby's liability. It is therefore vital that each club seeks its own independent advice as to how the GDPR applies to it and how to comply with the GDPR.

How can clubs comply with the GDPR?

Data Protection Principles

Clubs must comply with the data protection principles set out in the GDPR when processing personal data.

Clubs must:

- ensure that they have a "**lawful basis**" to process the personal data. The different types of "lawful basis" under the GDPR and are set out below. Each club will need to identify the "lawful basis" that applies before processing any personal data. Once this lawful basis has been identified, this must be explained to individuals in the club's Privacy Notice.

- Clubs must ensure that they have provided a "**Privacy Notice**" to each individual whose personal data is being processed. This must be provided at the time that such personal data is collected or received. Privacy Notices must clearly set out: i) what personal data is being collected, held or used; (ii) why it is being collected held or used; (iii) the "lawful basis" for the personal data being collected held or used; (iv) who the personal data might be shared with (and why); (v) where the personal data is kept; (vi) how the personal data is secured/protected; (vii) how long that personal data is kept for; and (viii) the various rights available to each individual as set out the GDPR. Privacy Notices should be included in membership application/renewal forms, booking forms and employment/volunteer forms where relevant. Clubs should also put their Privacy Notices on their website and provide individuals with a link to the relevant web-page. Clubs should also ensure that membership Privacy Notices provide for the club sharing personal data with Scottish Rugby through Scottish Rugby's Registration System (**SCRUMS**) and for other purposes such as PVG, insurance, disciplinary matters etc. **Sport**scotland has produced some generic template Privacy Notices that clubs may use, but clubs should note that these have not been endorsed or produced by Scottish Rugby and are provided for guidance only;

  Sportscotland Clubs Template Privacy Notice – Members

  Sportscotland Clubs Template Privacy Notice

- only collect, hold or use personal data for the specific purpose for which it was obtained (e.g. only use membership data for membership purposes);

- only collect, hold or use personal data that the club actually needs. This is not only a requirement of the GDPR, but will also help to mitigate against the potential for data breaches;

- keep all personal data accurate and up-to-date wherever possible;

- only hold personal data for as long as is reasonably necessary purpose for which it was obtained (e.g. when a member leaves the club, clubs should review all their data to see if they still need to keep it after a specific period). This is not only a requirement of the GDPR, but will also help to mitigate against the potential for data breaches; and

- protect personal data and keep it secure. This is not only a requirement of the GDPR, but will also help to mitigate against the potential for data breaches. Additionally, if a club can demonstrate that it did everything it could to otherwise secure personal data then this will assist in mitigating the club's liability if there is a data breach.

What are the types of "lawful basis" for processing?

When processing member personal data (e.g. admission forms, fee payments, AGMs etc), clubs will likely have a "**contractual basis**" to lawfully process that data. This is because the club needs to use that data for the purposes of club membership (but the club must only use that data for that purpose).

When processing employee personal data, again the club will have a "contractual basis" to lawfully process that data based on the employee's contract of employment (but again the club must only use that data for that purpose).

A club may also be legally required to process certain personal data to comply with legal obligations, for example for HMRC, PVG or health & safety purposes. This is the "**legal obligation**" lawful basis for processing personal data.

Another lawful basis for processing personal data is where the club (or a third party) has a "**legitimate interest**" for processing personal data, however these must be considered against the interests of the individual and must be clearly described in any club Privacy Notice.

Asking an individual for "**consent**" is another lawful basis for processing under the GDPR. However, there are specific requirements for asking for consent from an individual which mean it will be difficult going forward to rely on this lawful basis for processing. On that basis, another lawful basis for processing personal data should be identified wherever possible, such as a "contractual basis", "legitimate interest" or "legal obligation" lawful basis for processing an individual's personal data. If clubs do want to rely on "consent", they must provide a statement to the individual that:

- is a clear and affirmative action (an "opt-in" rather than an "opt-out" and no ticked boxes);
- is specific and informed;
- is separate from other terms and conditions and is not a pre-condition of signing up for a service; and
- is easy to withdraw.

"Special category personal data"

This is a separate category of personal data under the GDPR and includes data related to race; ethnic origin; politics; religion; health/medical; sex life; or sexual orientation.

If a club processes this type of personal data then they must not only have a lawful basis to do so (see above), but they must also have satisfied at least one other specified conditions as set out in Article 9 of the GDPR. Most likely this will involve having also obtained the express consent of the individual to process their data. Clubs processing special category personal data should take particular care and should seek independent advice prior to undertaking any such processing activity.

Rights of Data Subjects

Individuals (known as "**data subjects**") have certain rights regarding their personal data under the GDPR.

The rights available to data subjects are as follows:

- "**subject access request**" – data subjects can require clubs to provide a copy of any or all of their personal data that the club processes, as well as information on how the club processes the data (for example the purposes for which their data is being held and processed by the club, how and when the club obtained their data in the first place and who their data has or may be shared with;
- "**right to rectification**" – data subjects can require clubs to correct or complete any of their incomplete or inaccurate personal data held by the club;
- "**right to erasure**" - data subjects can require clubs to delete all their personal data held by the club (but only in certain circumstances);
- "**right to restrict processing**" - data subjects can require clubs to stop or limit the processing of their personal data (but only in certain circumstances);
- "**right to data portability**" - data subjects can require clubs to provide their personal data to them in a particular format for their own re-use (but only in certain circumstances); and
- "**right to object**" - data subjects can object to clubs processing their personal data (but only in certain circumstances). One example for clubs might be where a data subjects asks a club to stop sending the club's newsletter to them.

Clubs must consider and respond to requests from data subjects within one-month of the date of the request. Clubs will therefore need to have maintained sufficient records and systems (and to have sufficient control over these) to be able to respond to these requests within the prescribed one-month time frame. Clubs should also consider formalising internal processes and procedures to assist with responding to these requests within the prescribed one-month time frame.

Third-Party Data Processing

If a club uses any third-party suppliers, they should check whether any such supplier is given (or has been given) access to any personal data held by the club. Clubs might use third-party suppliers to send mailshots, host/administer websites (e.g. Pitchero), process payments or conduct surveys.

If personal data held by the club is shared with third-party suppliers, clubs should seek independent advice and should consider having such third-party suppliers sign up to a data processing agreement. **Sport**scotland has produced a generic template Data Processing Agreement that clubs may consider using in this regard, but clubs should note that this has not been endorsed or produced by Scottish Rugby and is provided for guidance only.

Sportscotland Clubs Template Data Processing Agreement

Accountability

The GDPR also requires controllers to be responsible for and to be able to *demonstrate* compliance with the data protection principles. This is known as the "**accountability principle**".

To comply with the accountability principle, clubs should keep complete and accurate records of all their data processing activities. Clubs should keep a document (such as a spreadsheet or table) recording the following in respect of the personal data they process:

- The reason for processing – e.g. for membership, competitions etc;
- The categories of individuals and types of personal data – e.g. members, volunteers, players, coaches, referees etc. and names, addresses, date of birth, email addresses etc.
- The details of who the club will share personal data with;
- Details of any personal data that is shared or hosted outside the UK or EU;
- Data retention periods – how long the club will keep different types of personal data for; and
- Details of security measures taken to keep personal data secure – for example passwords, locked cabinets, restricted accounts etc.

Some of the above information should also be included in the club's Privacy Notice (see above). Clubs should keep copies of all their Privacy Notices and any consent statements on file so these can be produced and evidenced at any time if needed.

What if a club fails to comply?

- If a club loses personal data or suffers a security breach then this will be a **personal data breach**. Put simply, a personal data breach is one that has affected the confidentiality, availability or integrity of personal data held by the club. There will be a personal data breach if personal data held by the club is lost, destroyed, corrupted or disclosed to an unauthorised person. Examples would include sending personal data to the wrong person (whether on purpose or accidentally), a hack or virus, or losing a computer or mobile phone that has personal data on it.
- If a personal data breach is severe and could affect individuals, then the club will need to inform the ICO within 72 hours of becoming aware of the breach. Clubs will also have to notify the affected individuals. Whether to notify the ICO of a personal data breach is a complex matter and will often depend on the facts and circumstances. Clubs should take independent advice if such circumstances arise. ICO guidance on personal data breaches and reporting can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.
- If a club fails to notify the ICO or affected individuals of a personal data breach when required to do so, then the club will be liable for a significant fine.
- Clubs in breach of the GDPR generally may be subject to ICO sanction, a significant fine (up to £20million or 4% of annual turnover, whichever is greater) and/or associated reputational damage. Clubs should also note that compliance with applicable laws (including data protection) is a requirement of each club's Participation Agreement and Scottish Rugby's Minimum Operating Standards.

Next steps for clubs

To prepare for the GDPR, clubs should consider taking the following steps:

- If not done so already, allocate responsibility for personal data and privacy to a named individual within the club;
- Identify all personal data held by the club and what it is used for – create a table or spreadsheet which can be used to maintain an ongoing record of the club's data processing activities;
- Update club Privacy Notices as required;
- Ensure that everyone within the club who has access to personal data held by the club has at least a basic understanding of the GDPR and the club's obligations under the GDPR;

- Ensure controls are in place to keep personal data held by the club secure. These can be both technological and practical measures such as ensuring anti-virus software is up to date, password protecting documents using locked filing cabinets etc; and
- Understand any third-party data processing activity and ensure that all suppliers who process personal data held by the club do so under a suitable written contract.

General ICO guidance
The ICO has also published a range of guidance on the GDPR and data protection, which can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Scottish Rugby
April 2019