UNIVERSITY OF CAMBRIDGE
Sports Service

Data@Sport

Guidance for GDPR and Data Security

2020-21 Edition

UNIVERSITY OF CAMBRIDGE
SPORT

UNIVERSITY OF CAMBRIDGE
Sports Service

Introduction and context

Guidance for GDPR and Data Security

This guidance document forms part of a series that has been produced by the University of Cambridge Sports Service to support University Sports Clubs in running safe, well managed, supportive and successful clubs. The other documents that form part of this series are:

- Club Registration and Operations
- Events@Sport
- Finance@Sport
- Safety@Sport
- Travel@Sport
- Welfare@Sport

Additional support materials and templates are also available on the University Sports Service Moodle site. It is important to note that all of these documents provide general guidance and signposting to clubs. Given that there are over 50 University Clubs playing sports that involve very different playing programmes, performance levels, regulatory frameworks and risks, it is impossible for us to cover all eventualities. It is therefore very important that Clubs consider their particular context carefully and refer to their National Governing Body (NGB) for more sport specific guidance and seek independent legal advice where appropriate.

FEEDBACK

We have done our best to provide helpful guidance to support clubs in managing their activities. However, given the diverse range of clubs at Cambridge we recognise that we will not have covered all relevant themes or issues. As such, we welcome your feedback on the value of the document. We will be reviewing and adapting it annually to ensure it becomes a useful reference point for Clubs in supporting students. If you wish to provide specific feedback or comments, please contact Registration@sport.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Sports Service

Contents

SECTION 1) PRINCIPLES OF GDPR

The General Data Protection Regulation (GDPR) shall have effect from 25 May 2018 across the member states of the European Union[1]. This EU regulation supersedes domestic legislation and provides a series of rights and protections over personal data for natural living persons (i.e. individuals in their lifetime).

Here are some of the key definitions that appear in the Regulation and in this guidance:

Personal data:

Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Consent:

Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Many requirements of the GDPR extend those previously contained in the Data Protection Act 1998. In particular, the following principles should be observed by Sports Clubs in relation to the collection and processing of personal data (which could, for example, be in the form of information provided on membership forms):

Principle	Explanation
1) Personal data should be processed **lawfully, fairly** and in a **transparent manner**.	See section 2 for an explanation of the lawful bases that apply for data processing. Transparency involves being upfront and clear with members on how their data is collected and used.
2) The collection of personal data should be for a **specified**, **explicit**, and **legitimate purpose**, and not processed in a manner incompatible with that purpose.	This means that individuals must be made explicitly aware of the specific purpose of the collection of their data, and once collected, the data is only processed in ways needed to achieve that purpose.

[1] Note that it is expected for the effect of this regulation to remain in the United Kingdom after leaving the European Union.

3) Data should be **adequate**, **relevant,** and **limited** to what is necessary in relation to the purposes for which they are processed.	This means that clubs should be precise with data collection; for example, it may be contrary to this principle to collect data on political views or sexual orientation if members are signing up to take part in sporting activities. Conversely, collecting relevant medical information is important to achieve a safe response to any potential medical emergencies that may occur.
4) Data must be **accurate** and kept **up to date**. Inaccurate data should be erased or rectified without delay.	For example, it is likely that alumni data, or data about longstanding members, may become out of date over time. Every reasonable step should be taken to ensure that inaccurate information is either updated or erased.
5) The form of the data which permits identification of data subjects should be kept for **no longer than is necessary** for the purpose for which it is processed.	For example, once a member graduates and ceases to become an annual member of the club, there may no longer be a legitimate reason to hold their medical or emergency contact data.
6) Data should be **secured** and **protected** against unauthorised or unlawful processing and against accidental loss, destruction, or damage.	All personal information that your club holds should be processed securely. This may involve physically locking paper-based information away, and password protecting digital data. Robust procedures must also be in place to ensure that those with access to the data do not use or process it for unlawful purposes.

Overall, the approach of the GDPR is that information about individuals should be subject to privacy by default and design.

As a club, you are responsible for complying with these principles, and must be able to demonstrate compliance.

SECTION 2) LAWFUL BASES

A valid lawful basis is required to process personal data. For example, using a member's email address to send promotional material would not be permitted if one of the lawful bases does not apply. Additionally, if a purpose can be achieved without personal data processing, no lawful basis is necessary.

Consent

This is one of the three most relevant lawful bases to Sports Clubs and applies where there is **real choice** open to members about whether or not they want their data to be processed in a certain way, if at all. Below are some best practice notes to follow for this basis:

1. Consent requests should be unambiguous; there must be a definitive **opt-in** for each processing operation. Therefore, a pre-ticked box or a box that requires an opt-out would generally not be compliant.
2. Generally, the consent you are requesting should **not** be a pre-condition for signing up to membership (i.e. there cannot be an artificial choice).
3. Members must be able to withdraw consent after giving it; your club must have processes in place to ensure that this is actioned effectively.
4. If you cannot offer a genuine choice to members, consent is not the appropriate lawful basis for data processing.
5. Consent requests must be prominent and not 'bundled in' with other terms and conditions of membership.
6. You must manage and update records of consent effectively.

Examples where the consent approach may be most appropriate:

- Sharing contact information with sponsors or partners.
- Using photographs of members for promotional purposes.
- Recording medical information to enable the club to respond adequately to potential sporting injuries.

Contract

This basis can be relied upon if you process personal data in order to fulfil your contractual obligations to the data subject. When a member joins a Sports Club, most often a legal contract is formed – the member usually pays a membership fee, and in return, they receive access to training facilities, equipment, coaching, social events, etc. Part of this contract (even if a fee is not paid) may involve data processing necessary for the club to perform on these obligations, for example:

- Recording and sharing personal information to provide insurance to the member.

If the data processing is necessary for the performance of the contract, consent will not also be required. However, if special categories of data (see section 4) or children are involved, further explicit consent may be required. It is for this reason that health information cannot be processed under the contract basis, even though it would otherwise form part of the 'contract', and so instead consent is required.

Legitimate Interests

The 'legitimate interests' basis is likely to be appropriate when you use people's data in ways that they would reasonably expect; for example, using their email address to contact them with information about club activities or processing member data for statistical analysis. When using this basis, there should be minimal consequences for each individual's privacy.

- The basis is flexible but would not necessarily be appropriate if consent or contractual bases apply.
- Extra responsibility is involved with this basis – the club must consider and protect people's rights and interests.
- A three-stage test applies:
    - Are you pursuing a legitimate interest?
    - Is the processing necessary for that purpose?
    - Do the individual's interests override the legitimate interest?
- If you rely on this basis, you must tell people in your privacy information that this is the case.
- The member's right to object remains under this basis – i.e. they can ask you to stop processing their data in this way.
- The legitimate interests could be of a commercial nature, or interests of the data subject themselves (e.g. to receive information about club activities).

A consent or contract basis may apply first; however, some data processing will not fall under these options, and therefore the legitimate interest assessment may be an appropriate test.

SECTION 3) RIGHTS

The following rights must be protected under the GDPR:

1. The right to be **informed** about the collection and use of their personal data.

The purpose for processing personal data must be made transparent, and privacy information must be provided at the time the data is collected.

2. An individual's right to **access** their personal data.

Reasonable information requests should be replied to promptly, and no later than one month after receipt.

3. Right to rectification.

Individuals have a right to have inaccurate personal data rectified. Rectification requests should be responded to within one month.

4. Right to erasure.

This is the 'right to be forgotten'. If an individual requests to be erased, clubs must respond within one month. There are various exceptions to this requirement.

5. Right to restrict processing.

This usually only applies if the individual wishes to challenge the accuracy of their personal data or if data has been unlawfully processed.

6. Right to object.

If there is processing based on legitimate interests, the individual has a right to object to this processing.

SECTION 4) SPECIAL CATEGORY DATA

Additional protection arises for information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics
- Health
- Sex life
- Sexual orientation

Under Article 9 of the GDPR, processing of this information is forbidden without one of a defined list of exceptions. For Sports Clubs, it is likely that you will process **health** data (e.g. medical conditions that the club needs to be aware of to ensure safe participation), and this information should only be processed with **explicit consent** for that specified purpose.

It is unlikely that Sports Clubs will have any other lawful basis for collecting other special category data.

Because health data is often required as a condition of membership to ensure a member's safe participation, the individual's choice of consent in this instance is whether to join the club or not.

SECTION 5) CLUB PRIVACY NOTICES

Central University privacy notices exist, but these will not cover the local activities of your club's data processing. As such, clubs are required to have their own privacy notice (also known as a 'Data Protection Statement' or 'Policy'). A template can be found at the end of this guide, but every club must ensure that their notice is accurate and specific to their own data collection and use.

Because of the rights and obligations specified in the GDPR, as summarised above, your privacy notice should cover the following topics:

Topic	Example/Notes
1) The **purpose** of the personal data use.	"We collect any relevant medical or injury information to ensure that your participation in the sport is as safe as possible."
2) The **lawful basis** for the personal data use.	This will almost always be via contract or consent. "We will use your personal information in accordance with the consents you have given to us."
3) Any **recipients** of shared data, if applicable.	"We will share your email information with a third party email distribution software company for the purpose of sending you club mailings."
4) Where there is a **contractual** need to supply personal data, if applicable.	"We need your contact details so that we can keep you informed of club training times and locations."
5) How **long** data will be retained for.	"We will retain your medical information for as long as you remain a paying and active member of the club."

This list is not exhaustive; if your club carries out data processing, you must ensure compliance with the principles and rights of the GDPR and be explicit and precise in your privacy notice.

SECTION 6) RETENTION PERIODS

When data is collected and processed for a certain purpose, the data should no longer be held or processed once that purpose ceases to exist.

In the context of University Sports Clubs, it is unlikely that special category data or ancillary data needs to be retained once a member leaves, or ceases to take part in club activities. If a member consents to being kept in touch with after their contract with or membership of the club terminates, data processing must then be specific and proportionate to this purpose.

SECTION 7) DATA SHARING

You should not publish or share the contact details of your members with third parties unless it has been clearly outlined to members in your privacy notice that you will do this.

Where you share personal data with a third party that handles the club's personal data on your behalf – such as a company that manages your mailings or cloud storage – you need to have a written agreement (e.g. a contract or a terms of service document) that outlines clearly the responsibilities of that company in handling personal data for you. The information that needs to be contained in this agreement is quite detailed. The ICO website provides a checklist to help.

If your society works with people or organisations overseas, personal data should not be transferred outside of the European Economic Area without your members' explicit consent (there are other lawful ways of transferring data abroad, but this is the most straightforward way to do this).

SECTION 8) DATA BREACHES

A serious breach of the GDPR can have significant consequences. Fines can be imposed of up to €20m or 4% of annual turnover, whichever is higher.

A breach may be a breach of security or an accidental loss, alteration, disclosure, or access to personal data (e.g. your membership database accidentally being published online). If a breach may pose a risk to people's rights and freedoms, there is a duty to report the breach to the Information Commissioner's Office (ICO). If a breach is not deemed this serious, the breach must still be documented, and the non-reporting justified. You must report a notifiable breach without **undue delay**, and no later than **72 hours** after becoming aware of it.

While handling a breach is your responsibility, in the first instance you can contact the University Sports Service for further guidance.

SECTION 9) SECURITY AND ERASURE

Data security can be maximised by putting in place proper procedures. Data can be stored in many mediums, including:

- Paper (e.g. membership forms and archives)
- Computer devices
- Online
- Electronic storage devices
- Film
- Honours boards and displays

It is important to audit all of your club's different mediums of data to ensure that each are processed correctly and protected from misuse.

Electronic Data

Data stored online and on electronic devices can be more vulnerable to misuse because of the easy portability between devices and over networks. If your club does store member data in this way, it is important to take, as a minimum, the following steps:

- Ensure that any online data is secured behind password protection and encryption (i.e. not open to the public).
    - You may also need to verify the robustness of the service provider you are using to ensure protection against cyber-attacks, and the data protection laws of the countries in which the provider operates/locates its servers.
- Password protect any electronic devices that contain access to data. This includes mobile devices that may be linked to online data storage apps.
- Ensure that virus protection is up to date on electronic devices holding data.
- Verify that only authorised personnel have access to electronic data and restrict the ability of authorised personnel to give access to third parties.

Physical Format Data

Data stored on paper (e.g. membership forms) or other physically recorded means should be physically secured. This may be achieved by locking the information in a safe or cupboard, or at the very least, storing it in a locked room with access limited to authorised personnel.

Erasure

One new aspect of the GDPR is the 'right to be forgotten'. If anyone you hold data on makes such a request, effective data erasure should be ensured. Destruction of physical copies may be possible via shredding, however electronic data may be more difficult to permanently remove. This is because of the possibility of copying data and multiple copies stored simultaneously. These problems not only emphasise the need for effective control and security of data when it is collected and processed, but also demand effective deletion procedures.

Expired Purpose

Remember that data processing is only permissible under the GDPR where there is a lawful basis and a purpose for doing so. If the purpose for holding or processing data 'expires', the data should be either deleted, or no longer processed.

One way of achieving effective controls over this is to specify **retention periods** for each of the data you collect. See section 6 for an overview of the principles of data retention.

SECTION 10) PERSONAL DATA AUDIT

In order to practically support the rules outlined above, and to manage your club's collection and use of personal data effectively, you will need to assess and audit:

- **What** personal data you hold – you should not collect or keep more than you need.
- **Why** you hold personal data – this is likely be membership administration for all clubs, but may also extend to marketing and/or fundraising.
- **How** you use personal data – you should keep it accurate and you should not keep it for longer than you need.
- **Where** you store personal data – you should hold it securely, with access limited to those who need to see it (see section 8 for further guidance).
- **When** you might share personal data with third parties (i.e. any individual or organisation external to the club).

FURTHER INFORMATION

This guidance is a summary of the law, and should not substitute a thorough understanding of official University and government advice. For more complex data activity within a Sports Club, independent legal advice may be required.

Some helpful resources can be found here: ICO Guidance:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

University Guidance:

https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/societies

APPENDIX 1 – Sample Privacy Notice Statements

Privacy Notice Template

The University accepts no liability for this template which is provided as a guide. If you have complex arrangements relating to personal data (particularly in relation to non-members), you may wish to check the ICO guidance and/or seek independent legal advice to ensure your compliance with this aspect of the law.

How we use your personal information – [name of club]

This statement explains how the [full name of club] ("we", "us" and "our") handles and uses the personal information we collect about our members [and other people] for processes relating to our operations and activities.

When changes are made to this statement, we will [publish the updated version on our website] [update our member handbook] [email you].

The controller for your personal information is [full name of club]. The person responsible for data protection within our society is the [role title e.g. President, Treasurer, Secretary] who can be contacted at [supply contact details].

How we use your personal information

We collect and process your personal information for a number of purposes, including:

[Add data statements here]

How we share your personal information

[Select, amend, add, delete and adapt as appropriate]

- We share some of your personal information with the University, only where there is a specific need to, including for registration as a University Sports Club, and to provide your blues and sporting records for your University records and for alumni communications and/or fundraising purposes specifically related to the sports club.
- We share some of your personal information with [name of third party] for the purposes of [insert details].
- We use University IT facilities to store electronic copies of personal information.
- We may share your personal information with certain organisations overseas, including [name of third party], as part of arrangements related to your membership of the club. In such cases, we will ask for your explicit consent prior to transmitting this information.

We may also be subject to a legal requirement (with or without your consent) to share your personal information with the University or a government agency (such as the police or security services or other statutory authorities with investigatory powers) under special circumstances (e.g. relating to tax, crime or health and safety). Where feasible and appropriate, we will notify you of our intention to share such information in advance.

Your rights

You have the right to access the personal information that we hold about you. You also have the right to ask us to correct any inaccurate personal information we hold about you, to delete personal information, or otherwise restrict our processing, or to object to processing or communications, or to receive an electronic copy of the personal information you provided to us. Please note that all of these rights are qualified in various ways.

If you have questions or concerns about how your personal information is used, please contact us using the above details.

If you remain unhappy with the way your information is being handled, or with the response received from us, you have the right to lodge a complaint with the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (https://ico.org.uk/).

Last updated: [date]

APPENDIX 2 – Sample Consent Request

All clubs are required to have a privacy notice, and members must be provided with this at the point they join, and subsequently these must be readily available (e.g. on your website). A template statement is available at the end of this guide for clubs to adapt.

Below are examples of wording that can be used in sports club privacy notices covering:

a) The data you are collecting

b) The purpose of the collection and processing

c) The lawful basis of the processing

d) The duration of the processing and/or storage

Note that statements must be compatible with the principles and rights outlined above. Although the examples provided may be suitable for your club, each privacy notice must be bespoke and highly specific to the data processing of your club. These should therefore not be seen as compliant or relevant for every club or every processing activity.

Medical Information:

'We require your consent to collect information about any relevant medical or health issues which may impact your participation in sport. We use this information to ensure that the Club and its coaches can deliver a safe and appropriate program of training for our members. We will retain and process this information for as long as you remain an active playing member of the Club.'

Club Communications:

'In order to provide you with information, per your membership contract, we will use your contact information to send you emails about club activities and notifications. We will retain your contact information for as long as you wish to be contacted by the club, both in your capacity as a current member, and your future capacity as an alumnus.'

Third Party Marketing:

'We require your consent to share your contact information with third parties who may wish to send you relevant marketing information. We will share your information for as long as we have consent to do so, and no longer than the duration of your membership with the Club.'

When you ask for consent for data processing, this lawful basis requires explicit and unambiguous means of obtaining it. The following example shows how this may be achieved for club social communications on a membership form.

Please note that any 'tick boxes' must not be pre-ticked, and consent should be **affirmative** – i.e. not an opt-out. If this option is required when a member fills out a membership form, it must be prominently placed on the membership form and not in the privacy policy, (though the consent statement may appear in the privacy policy as explained in Appendix 1).

If you would like to receive club social communications, please opt-in by ticking the box below:

Opt-in to receiving club social communications: ☐