Section 19

19

GDPR for Sports Clubs

The General Data Protection Regulation (GDPR) took effect on the 25 May 2018, replacing the earlier data protection framework under the EU Data Protection Directive. As a regulation, GDPR does not generally require transposition into Irish law (regulations have 'direct effect'). Organisations involved in processing personal data of any sort (including sports clubs) need to be aware that the regulation addresses them directly in terms of the obligations it imposes.

The act set out various obligations on data controllers and rights for data subjects. It also sets out the powers and responsibilities of the Data Protection Commission. As a club operating in UCD you need to be aware of the implications of the legislation in terms of how your club processes personal data.

The information contained in this section is based on a presentation given by the UCD Data Protection Officer in February 2020. Please refer to the UCD Sport website for the presentation slides.

19.1 What is the difference between using personal information in a purely private context versus your work or studies?

If you use personal information in a purely private context, which always remains private and does not spill over into your professional or university life, you can make use of the so called ***"household exemption"***, where GDPR does not apply.

However, anything you do with personal data in the context of your work or study needs to strictly follow GDPR, as it is within a public and professional context. This includes how you interact with fellow students as part of your study and courses.

Consequently, anything you do with personal data collected from your members and third parties for your club must follow GDPR.

19.2 What is personal data?

The term 'personal data' means any information concerning or relating to a living person who is either identified or identifiable (such a person is referred to as a 'data subject').

An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, social identity of that individual.

Personal data doesn't have to be in written form, it can also be information about what a data subject looks or sounds like, for example photos or audio or video recordings, but data protection law only applies where that information is processed by 'automated means' (such as electronically) or as part of some other sort of filing system.

19.3 What is special category & sensitive personal data?

Special category data includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- health data
- sex life or sexual orientation

Other sensitive data includes:

- financial data
- criminal convictions and offences

19.4 What is data processing?

Data Processing covers a wide range of operations performed on personal data, including by manual or automated means.

It includes the 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 of personal data.

19.5 What are the valid grounds for processing data?

There are six legal bases under GDPR:

- Consent
- Contractual necessity
- Compliance with legal obligation
- Vital interest
- Public interest
- Legitimate interest

You need at least one, which needs to be decided in advance of data collection, and individuals (data subjects) have the right to know which legal basis you are processing their data under.

19.6 What does 'consent" mean under GDPR?

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

That means:

- Need to have full information before making a decision.
- No pre-ticked boxes.
- No catch-all consent.
- Not to be pressured into giving consent.
- Being able to prove that consent was received.
- Consent needs to be easy to withdraw at any time.

19.7 What happens if consent is withdrawn?

- Processing of personal data has to stop.
- Processing that already happened before withdrawal of consent is lawful, but processing after withdrawal is not.

19.8 What are the 7 principles for processing personal data?

Article 5 of the General Data Protection Regulation (GDPR) sets out key principles which lie at the heart of the general data protection regime.

1. **Lawful, fair & transparent processing**

   This means you need:

   - One or more valid grounds for your processing.
   - To handle people's data in ways they would reasonably expect, or if it is unexpected, you can explain why any unexpected processing is justified.
   - To be clear, open and honest with people from the start about how you will use their personal data.

2. **Purpose limitation**

   This means you need:

   - To process the personal data only for the purpose(s) you collected them for and in line with what individuals expect.
   - To ask individuals for their permission / consent if you want to use their personal data for a different purpose. You need to do this in advance, and they need to have allowed you to get back in touch with them.

3. **Minimisation of processing**

   This means you need:

   - To only collect personal data, you actually need for your specified purpose(s).
   - To have sufficient personal data to properly fulfil your purpose.
   - To periodically review the data you hold and delete anything you don't need any longer.

4. **Data accuracy/quality**

   This means you need:

   - To take all reasonable steps to ensure the personal data you collect, or hold is not incorrect or misleading.
   - To correct any personal data once you find out they are incorrect or misleading, or erase the incorrect personal data as soon as possible

5. **Storage limitation**

   This means you need:

   - To keep personal data only for the minimum time you need it to do what you said you would do.
   - To periodically review the data you hold, and erase or anonymise it when you no longer need it.

- To tell the individuals for how long you will keep their personal data.

6. **Integrity, confidentiality and security**

   This means you need:

   - To protect the personal data by technical and organisational security measures.
   - To ensure that personal data are protected from various forms of unauthorised access and data breaches.
   - To be very mindful of and restrictive with sharing any personal information with others. Only share it with people who have a valid relevant business reason to see the data.

Simple steps you can take in your club to keep electronic personal data secure & safe:

- Encrypt & password protect mobile devices, e.g. Smartphones, Tablets.
- Avoid using USB keys. If you cannot avoid using it, be sure to encrypt the device or at very least the file.
- Encrypt personal data before transferring it across the internet, e.g. email. The decryption password should be communicated separately, e.g. phone call, text.
- Passwords should be strong and never shared.
- Use Anti-Virus Software on your device.
- Backup data regularly.

7. **Accountability**

   This means you need:

   - To take responsibility for what you do with personal data and how you comply with the other principles.
   - To keep track /a record of what you do with the personal data.
   - To put in place measures and processes that keep the data safe and secure.

8. **Data Subject Rights**

   Individuals have a number of specific rights under data protection law to keep them informed and in control of the processing of their personal data. The most commonly exercised of those rights are those found under the GDPR (in Articles 12-22 and 34).

   The data subject rights under the GDPR include:

   - Right to be informed if, how, and why their personal data are being processed.
   - Right to access and get a copy of their personal data.
   - Right to have their personal data corrected or supplemented if it is inaccurate or incomplete.
   - Right to have their personal data deleted or erased.
   - Right to limit or restrict how their personal data are used.
   - Right to data portability.
   - Right to object to processing of their personal data.
   - Right not to be subject to automated decisions without human involvement, where it would significantly affect them.

Information provided to data subjects when these rights are exercised must be transparent, understandable and easily accessible, using clear and plain language. The information should be provided in writing, or other means, including, where appropriate, electronically. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is clear or can be proven.

19.9 What are the key club activities that involve personal data?

Remember, your position comes with responsibilities. Any access you are granted to personal data in your function in the sports club, you must strictly limit to the specific purpose, nothing else!

At present committee members have access to the following data using UCD systems:

1. **Two committee members per club have access to InfoHub**

   Data you have access to includes:

   - student number
   - name
   - U18 Yes/No
   - committee position
   - team
   - phone
   - email address
   - emergency contact

Purpose of your access:

- To be able to add a student as a member of your club and then to send the student an email to inform them this has been done.

Data types involved in this processing operation:

- Student number, name, U18 Yes/No, committee position, team, phone, email address, emergency contact. These are all normal types of personal data.

2. **Two committee members have access to the clubs@ucd email and Google-drive**

Purpose of your access:

- Email: to send club relevant information to club members and, in your function, to communicate on behalf of the club to other entities.
- G-Drive: to store information relevant to the running of the club.

Things to consider:

- Be extremely protective of the password for the club email. Make sure it is changed when your committee changes.
- Don't use the club email for non-club business.
- When you send emails to groups, don't disclose individuals' email addresses to all by using the To, or CC function, but rather the BCC.
- Make sure you send information to the right recipient.
- On the G-Drive, only store files that are relevant for the business.
- Don't keep files with person information for longer than necessary.
- Don't access the drive through devices that have unsecure apps installed.
- Don't access your email or G-Drive via a non-secure wireless network connection like UCD wireless.
- For personal information on the G-Drive you inherited, check if something needs to be deleted by now.
- Don't process personal data unnecessarily and think what valid ground for processing applies to what you want to do.
- Your club email and G-Drive needs to follow GDPR. It is not your private life!

3. **Committee members may have access to coaching records**

Where your club engages coaches your committee members may have access to coaching records:

- Employee set up info, pps number, bank details, date of birth, address
- CVs
- References
- Time sheets

Purpose of access and processing:

- To select and hire coaches for your sports club.

Things to consider:

- CVs contain a large amount of personal information and have to be treated confidentially.
- Don't leave CVs laying around or in places where anyone can see them.
- References are very personal as well.
- You need permission from the candidate to contact someone to provide a reference and can contact the reference provider only at a point in time where the candidate is about to be hired, not far in advance.
- An employee set up form is likely to contain sensitive information (PPS number, financial info etc), keep this in mind and keep this info secure and only show it to people who are permitted to see it.

4. **Committee members may have access to scholarship applications**

Access to scholarship application is restricted to applications in their own sport.

Purpose of access and processing:

- This is required to adjudicate on the suitability of the applicant.

Things to consider:

- Many scholarship applications will contain a substantial amount of personal information, possibly special category data, which need to be treated with a higher degree of care.
- Keep the club member informed in advance of any processing activity involving their personal data, so that they can reasonably expect it.

5. **Committee members may have access to minutes of meetings, insurance matters, incident/accident reports, membership records and entry forms (name, number, medial details etc)**

Purpose of access and processing:

- To manage and run the club.

Things to consider:

- Minutes of meetings; Insurance matters; Incident/accident reports; Membership records; Entry forms; are all documents that are important to keep well organised and safely stored.
- For a number of these kind of records expected retention periods exist, which you should be aware of.
- Several of these documents might fall under the group of confidential data.
- When you send out such documents, be sure you send it only to people who should see them.

Any medical, health, performance and other data of this nature are considered SPECIAL CATEGORY data. There are considerable restrictions on processing such data; often you need the 'explicit consent' of the individual, whose data they are to do so.

6. Clubs may share some data with their National Governing Body

Purpose of access and processing:

- To register a student to play competitively in a national club the UCD Sports Club must register them in leagues/cups.

Things to consider:

- Keep the club member informed in advance of any processing activity involving their personal data, so that they can reasonably expect it.
- To register a student to play competitively in a national club the UCD Sports Club must register them in leagues/cups.

7. Social Media

Finally don't forget that GDPR applies when you use social media for your sports club! Let people know in advance what you plan to do.

Purpose of access and processing:

- To promote the activities and achievements.

Things to consider:

- In some instances you will need their active consent to use their personal data, photographs, audio or video footage.

Further information is available from the Data Protection Commission **www.dataprotection.ie**