# GDPR in the Leisure, Health and Fitness Sector

**Membership Data**

Under Article 6 of GDPR, the lawful grounds for processing members data is fulfilment of contract, as the data subject is paying the club a fee in return for membership. In order to provide this membership. Leisure centres typically requires their name, address, date of birth, email and phone number.

During registration, Ireland Active Members will require bank details in order to process direct debit payments. The club should take extra precautions when handling this data and consider data minimisation where possible.

Leisure centres will typically have an undefined retention period for all member data held within their systems. Under Article 5's principle of Storage Limitation, data should only be held for a period that is appropriate for its intended purpose. Clubs should therefore look for any legal grounds it has for retaining personal data relating to old members and define an appropriate retention period. If there is no legal requirement for holding personal data, then the organisation must define its retention period based on what they believe to be best practice, taking the data subjects' rights under GDPR into account. This should be done for all personal data, including archived paper-based forms that are no longer needed for their original intended purpose.

Under Article 28 of GDPR, all processing carried out by a processor on behalf of a controller should be governed by a contract or other legal act. Clubs should put a Data Processor contract in place with their database provider to ensure they adhere to the responsibilities of a processor under GDPR.

Clubs should look to implement access controls within the database to ensure only people with appropriate clearance or authority can see certain data.

All clubs should create a policy for handling children's personal information, parental consent is required for a person under 18 to enter into a contract (e.g. membership), and parental consent should be sought for children under 18.

Clubs should update their privacy policy and implement appropriate procedures to mitigate the above issues. The organisation must also ensure that all staff are trained in these updated policies and procedures.

Privacy policies should be readily available on the club's website outlining exactly what data they are collecting on their members, what it's used for, how long it's stored and if it goes outside the organisation

**Human Resources/ Employee data**

Overall, HR access more information than they gather. The HR department can use a number of systems but is not necessarily the owner of the personal data held on these platforms. A HR Department can process personal data for legal, tax and insurance purposes. This basis therefore readily satisfies the lawful grounds of legal obligation and contract fulfilment, as detailed in Article 6.

Leisure clubs will often use a payroll system (e.g Sage) for processing employee data. Any data that is hosted on the system is specifically required in order to process employees' wages and therefore falls under fulfilment of contract, as described in Article 6. To ensure data minimisation, Finance should only collect data that is absolutely necessary for processing payroll. If they believe data is not necessary for this purpose, it should be removed from the system. The Finance Department will have requirements in relation to the retention period of financial and tax records, as well as obligations to retain certain categories of information for pension purposes.

Under Article 5, personal data should be retained for no longer than necessary for the original purpose of processing it. Clubs should therefore review their policies and procedures to verify whether the Finance Department respect this principle, and if not, update their processes.

Under Article 28 of GDPR, Clubs should ensure all processing carried out by sub-contractors (e.g Sage) is governed by a Data Processor contract or legal document and recorded appropriately.

Clubs should consider conducting a data cleanse where possible on any old paper copies of past employee details that are no longer needed for their original intended purpose. This would include employees that have left the organisation over 7 years ago.

**Garda Vetting**

Under the National Vetting Bureau (Children and Vulnerable Adults) Act 2012, anyone carrying out relevant work that involves access to children or vulnerable adults is required to be Garda Vetted.

Ireland Active carries out this process on behalf of their members. This requires employees of member organisations to send Ireland Active a signed document (NVB1/NVB3) giving explicit consent to this process. The personal data collected is stipulated from a template sent out by the National Vetting Bureau (NVB). Once completed, the document is sent on to the NVB for processing.

Upon completion of processing by the NVB, Ireland Active receive the Vetting disclosure document in softcopy. Ireland Active then send a copy of the document to the employer (member of Ireland Active). In accordance with the GDPR and data minimisation, Ireland Active members should look to minimise the amount of personal data they hold on individuals and should therefore only keep a copy of the reference number and date of issue of the disclosure as well as the disclosure itself, as they are the Data Controllers. Ireland Active members will be able to request information on the data subject from Ireland Active using the reference number should they require it.

In accordance with GDPR's Article 5, principles of processing, Ireland Active members should define a retention period for any consent document and disclosure held in relation to this process. GDPR does not indicate a set retention period, so it is therefore up to members to define their time scale based on best practice and an appropriate risk appetite. The National Vetting Bureau recommends that the vetting disclosure is destroyed within 12 months of re-vetting occurring.

Ireland Active members should create a procedure that informs the relevant authorised Garda vetting Contact Person on how they are expected to process data related to Garda Vetting. This should focus on how to enter data correctly, appropriate security and data minimisation.

**Marketing**

Marketing is perhaps the most contentious department when examining GDPR compliance. It is the most likely to trigger complaints by individuals to the Data Protection Commissioner if the correct procedures and policies are not implemented.

The two lawful grounds to consider in direct marketing practices are consent and legitimate business interest. GDPR states, that 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.' This basis may be cited where consent is not viable or not preferred, though the DPC rightly stresses the fact that organisations will still need to show that there is a balance of interests between their own and those of the consumers being targeted. Consent is required if the balance of interest in direct marketing is shown to heavily favour the controller (e.g. a Leisure Club/Gym).

Of course, any individual can object to direct marketing. As one of the principles of processing under GDPR, objection is already well understood and easy to action by the general public, typically via an unsubscribe link or by contacting the company.

In the case of many Ireland Active members, a newsletter is often sent out on a regular basis to provide an update on events within a club. Leisure clubs are not necessarily selling anything through this newsletter and could therefore argue legitimate business interest as there is a balance of interest between themselves and their members in the communication they receive through the member newsletter.

**Event Photos**

Leisure clubs regularly take photos at events to market their venue. This has been a contentious issue as GDPR approaches. If photographs are being captured at an event attended by large crowds within a private area, then it is advisable that the attendees are informed of the photographer's presence. This could be made clear on event invitation cards or through displaying appropriate notice signs at the event. The notice should identify the photographer, how the photographs will be used and that guests should make themselves known if they do not want to appear in publicity material. Clubs can also include an opt in on membership forms for taking of photos of members in the club as part of their membership.

**Medical Data**

Medical Data is sensitive personal data, therefore clubs must be extremely vigilant when processing data of this kind. Clubs must reduce the amount of data collected on their registration form, if they collect any at all. If there is no legal requirement or legitimate business reason for doing so, clubs should strongly consider removing it completely. Clubs should delete any medical data held within the database on past members. It would be prudent to consult with Insurance providers to see if there is a requirement to keep any medical data (e.g. for potential legal claims) and for what period.

**Biometric Data**

Biometric data is sensitive personal data and requires extra precautions under GDPR when processing. Article 9 states clubs should only process Biometric data when they have gained **explicit** consent from member or employees

Leisure clubs often uses biometric data to monitor employees working hours, the data commissioner believes the operation of the system itself violates the principle of proportionality in relation to the specific purpose, the control of staff working hours and constitutes a disproportionate interference with the privacy of the individual. The only lawful basis to process this data will be explicit consent & in order for this to be valid it must be freely given, meaning employees **must be given an alternative option for monitoring working hours.**

**CCTV**

Leisure clubs must clearly display where CCTV cameras are in operation and for what reason, this should include notices around the facility pointing members to the organisations privacy policy. They should also look to limit the number of people who have access to the cameras and ensure appropriate security is in place. A policy should be implemented to decide when it is appropriate to save footage that was recorded (in the event of an incident) and when to show a member footage that they have requested to see. Any footage shown to individuals should only consist of the event that occurred and the people involved, any other individuals in the footage must be removed or fuzzed out.

**CV's**

The HR Department/Management is typically responsible for all recruitment. Clubs need to ensure their staff are aware of the implications of GDPR and handle this personal data appropriately. A policy should be put in place within the organisation to delete any applicants' CVs when unsuccessful. If an applicant was unsuccessful for a current position, but may be suitable for a future role, the organisation can keep the CV under the basis of Legitimate Interest. The data commissioner advises that CV's be kept up to a period of one year and no longer.

---

Further information can be found here: http://gdprandyou.ie/

GDPR e-learning certified by the Insurance Institute can be accessed here:

http://www.irelandactive.ie/general-data-protection-regulation-_gdpr (45mins to complete)

*Note: This document is for Ireland Active members information purposes only and is not to be taken as legal advice.*