

Ensuring GDPR Compliance

Specific Steps for LGFA Clubs to ensure Compliance

It is imperative that every LGFA club understands the principles of Data Protection and how the upcoming changes in legislation will affect them. The following are key steps clubs should take

Increase Awareness

GDPR will benefit all of us, it will ensure that our Personal Information is protected from misuse by any organisation. It will also ensure that, as a Data Controller, each LGFA Club, County or Provincial Board will be accountable for how it collects, uses and stores information about the LGFA members under their remit. It is critically important that every member is aware of the changes that GDPR will bring and how that impacts them, either as a volunteer working on behalf of the club or as an individual Club Member.

This awareness will also benefit all of us in our personal lives as GDPR also relates to Banks, Insurance Companies, Utility providers, On-line Marketing etc. Clubs should ensure that information relating to GDPR is made available to Committee Members, Club Members, Coaches, Volunteers or anyone who is in anyway involved with the Club.

Ensure Understanding

As the saying goes, 'You can't manage what you can't measure' and this is especially true regarding Data Protection. It is imperative that each LGFA Club understands exactly what Personal Information it holds (and is responsible for). To ensure this is clear, it is important that every club makes an inventory of the personal data that it holds and examines it under the following headings:

1. Why is it being held?
2. How was it obtained?
3. Why was it originally gathered?
4. How long is it being retained for?
5. How secure is it?
6. Is it shared with any third parties?

Obviously, the primary source of Personal Information held by a LGFA Club is its Membership database. All registered members' information is stored on the LGFA's central Games Management System (Servasport) and responsibility for this information is jointly held by the LGFA centrally.

Specific consideration must also be given to Paper Membership forms and how these are managed once they have been completed and received by the club. It is OK to collect information on paper forms, and to retain them in hard copy after they have been completed, as long as the member is made aware of this at the time they are completing the form. Tick boxes (or similar) should be used to obtain the person's consent to process their information. It is vitally important that any completed forms are stored securely in a specified location.

The same logic should be applied to any other system or database used to assist a club when managing its membership. It is OK to use technology supports in this way but careful attention must be paid to how and where data is stored (it must be secure and should be encrypted) and individuals

must be informed if a third party is being used to provide a system for this purpose. Most of the third party providers of these kinds of systems (online registration, text messaging, fundraising) will be well aware of GDPR and will be able to advise on how they are ensuring compliance. If your club is using a third party system you should contact them to verify that they are in compliance with GDPR.

Other likely categories of Personal Information held by LGFA Clubs will include:

- Information required for Garda Vetting
- Cul Camp or other training camp applications
- Text or messaging systems
- Email lists or distribution groups
- Teamsheets, training attendance lists
- Information captured on club websites

There may also be others, depending on individual clubs, and it is important that each club has a record of all of the Personal Data that it 'controls'. An example of a Club Record of Processing Activities is available in the downloads section of this page.

Clear Communication

As noted above, it is required that individuals are made aware of certain information such as why their data is being collected and who will have access to it, before their data is obtained. Under existing Data Protection law, it has always been a requirement to provide some of this information to individuals. GDPR builds on this requirement and expands the information that must be given to Individuals in advance of collecting and using their data. It is fortunate that the LGFA Membership renewals occurs at an appropriate time to allow clubs to provide all of this information to its members in advance of the May 25th deadline.

Existing membership forms, and other forms used to collect data (e.g. Garda Vetting) must be updated to specifically tell individuals the following:

- The Clubs identity
- The reasons for collecting the information
- The uses it will be put to
- Who it will be shared with
- If it's going to be transferred outside the EU
- The legal basis for processing the information
- How long it will be retained for
- The right of members to complain if they are unhappy with the club's implementation of GDPR
- Other specific personal privacy rights relevant under GDPR (as outlined in Personal Privacy Rights section)

The LGFA has obtained legal advice on how the above requirements should be reflected on LGFA Membership forms and a sample membership forms is available from the download section on this page.

Ensure Personal Privacy Rights

GDPR enshrines certain rights for individuals that must be supported by every Data Controller, including LGFA Clubs. It should be noted by members that these rights extend to any entity that holds your information including Financial institutions, utility companies etc. These rights include:

- Access to all information held about an individual (Subject Access Request) – This allows for any member to request a copy of all information held about them. This must be provided within one month. Note: Maintaining the Inventory of Personal Information outlined above will be a critical enabler for processing Subject Access Requests in a timely manner
- To have inaccuracies corrected
- To have information erased
- To object to direct marketing
- To restrict processing of their information including automated decision making
- Data portability - Ability to receive all of their information in a standard format to move to another provider (more relevant for switching banks or utility providers than LGFA Clubs but must be supported)

Obtain and Manage Consent

GDPR is very clear that an individual must be informed of what their personal information is going to be used for, who will have access to it, where it will be stored and how long it will be held for. They must give their consent for their data to be used. Consent must be 'freely given, specific, informed and unambiguous'. Members cannot be forced into consent or unaware that they are giving consent. Obtaining consent requires a positive indication of agreement – it cannot be inferred through silence (not objecting), pre-ticked boxes or inactivity.

Consent must also be verifiable – Data Controllers must be able to demonstrate that consent was given and an audit trail should be maintained. Note: Where paper forms are used to collect personal information (e.g. Membership applications), the retention period (how long its kept for) for the form, or relevant portion of the form, should align with the need to demonstrate consent.

Under GDPR, children are not permitted to give consent for Data Processing. A child's Parent or Guardian must give consent on their behalf. Existing LGFA policy relating to Juvenile members already supports this legislative requirement.

Report Data Breaches

If unauthorised access to Personal Data occurs or Personal Data is lost or stolen, this must be notified to the Data Protection Commissioner within 72 Hours of being identified. This is a requirement for all paper information and all electronic information (unless the data is encrypted or anonymised). If the breach is likely to cause harm to the individual (Identity Theft or breach of confidentiality) then the individual must also be informed. A procedure to detect, report and investigate data breaches should be in place.

It is imperative that Data Breaches or possible Data Breaches are not ignored in the hope that no one will notice, they must be investigated and reported if appropriate to do so. Advice on data protection queries can be obtained by emailing dataprotection@lgfa.ie.

Note: The 72 hour deadline for notification to the Data Protection Commissioner applies irrespective of any steps being taken to understand the causes of the breach.

Ensure Privacy by Design

GDPR seeks to ensure that all significant new processes, initiatives or projects undertaken consider and ensure GDPR compliance. This requires that a Data Protection Impact Assessment must be undertaken to understand the potential impact of that project / initiative on the privacy of individuals. LGFA Clubs that are considering projects with 'high risk' processing (i.e. new technology) or installing CCTV should conduct a Data Privacy Impact Assessment by meeting relevant stakeholders, identifying potential privacy issues and agreeing ways to mitigate the risk of issues occurring.

Identify Data Protection Officers

Every LGFA Club should identify someone to coordinate their approach to meeting their Data Protection obligations. This will include identifying and recording the specific locations where data is held in each club, ensuring that consent is obtained in the appropriate manner and maintained accordingly. The LGFA centrally has a Data Protection Officer who will provide expertise and guidance for any Data Protection queries that require additional / legal advice. Queries of this nature can be submitted to dataprotection@lgfa.ie