IRISH FA

DATA PROTECTION GUIDANCE FOR CLUBS

Introduction

The General Data Protection Regulation 2018 (GDPR) is the data protection law which replaces the Data Protection Act 1998. The law gives individuals greater control and protection over how their personal information is handled. The GDPR affects all organisations within the EU and this includes a football club.

This guide is intended to help a football club understand data protection and how it pertains to a club. This guide is not acting as a legal document, nor should it be considered an all-encompassing guide to achieve GDPR compliance. Further information about the GDPR can be found by visiting the Information Commissioner Office (ICO) website.

Terms and explanations to begin with:

Data protection can be a complicated matter. But here are some key data protection terms and explanations to help a club understand the GDPR.

- Personal data is any information relating to an identified living person
- Special category personal data is data which is more sensitive and so needs more protection. Special category data relates to personal information such as race, ethnicity, political opinions, religious beliefs, health, etc.
- Processing means anything that is done to, or with, personal data including collecting, holding, storing, sharing or deleting the personal data.
- The GDPR sets out key principles and there is a requirement to demonstrate that measures are in place to account for the principles.
- Data security is one principle to ensure personal data is secure and in the right hands. It requires using both technological measures, such as password protection on documents and devices, and organisational measures, such as determining who may handle the data.
- Individuals have enhanced rights with regards to how their personal data is handled.

Initial steps recommended for a club

The steps below should help to ensure a club has important data protection measures in place.

1. Make data protection a point on the agenda at all Committee/Board Meetings.
2. Identify who in the club is the Data Protection Officer.
3. Key stakeholders should learn the principles of the GDPR and understand how these apply to the club.
4. Keep a data inventory of all activity and ways you may handle personal data.
5. Continuously review technological and organisational measures to ensure the clubs data is secure.
6. Keep up to date privacy notices and statements so that the club informs people about how their data is handled.
7. Retain personal data only when there is a lawful basis to do so and for no longer than is necessary.
8. Educate all people in the club who handle personal information. Be sure to do this regularly.

Principles of data protection

A club should ensure that the following principles are considered in every activity which involves handling personal data.

- Data is processed lawfully, fairly, and in a transparent manner
- Data is processed with a specified and explicit purpose
- Data is limited to what is necessary for the purpose
- Data is accurate and up to date
- Data is kept no longer than is necessary
- Data is protected by both technological and organisational measures

There is a new accountability principle in the GDPR. This specifically requires a club to take responsibility for complying with the principles, and to have appropriate processes, documentation, and records in place to demonstrate that the club complies.

Rights of Individuals

Under the GDPR, individuals have enhanced data protection rights. Listed below are some of the main rights which may pertain to a club and some detail for a club to consider:

- The right to be informed – Individuals have the right to be informed about how a club processes their personal information. This includes where and how a member's contact details are shared. A club should inform people in a Privacy Notice on their website and Privacy Statements which are provided at the point of data collection such as on forms.
- The right to access (Subject Access Request) – Individuals have the right to request personal information a club may hold about them. If a club receives any request for personal information, it is important to immediately escalate this to the Data Protection Officer. The club must respond to the request within 30 days.
- The right to be forgotten – Individuals have the right to have personal data deleted. Individuals can make this request either verbally or in writing. If a club receives any request for personal information to be deleted, it is important to immediately escalate this to the Data Protection Officer.

Privacy Notices and Privacy Statements

A club's Privacy Notice(s) and Privacy Statement(s) should be easy to understand and kept up to date to reflect how and why the club is handling personal data. A club should use the following information to outline its Privacy Notice and Statements:

- What personal data the club processes
- Who the club collects personal data from
- Why and on what lawful basis the club collects personal data
- Who the personal data may be shared with
- How long the club will hold the personal data for
- Inform individuals of their rights under the GDPR
- Inform individuals of the clubs processing activities

Lawful basis for processing personal data

To comply with the right to be informed a club must be transparent and communicate clearly as to how and why the club is handling the personal data. The GDPR sets out that organisations must explicitly decide a lawful basis for processing. Here is brief detail of some lawful bases a club may choose to use:

Legitimate interest – for football administration activity which an individual would expect their personal data to be handled, may mean there is a legitimate interest and therefore a club can handle the personal data.

Consent – must be freely and positively given with sufficient information so that the individual knows exactly what the consent is being given to. An individual who gives consent has the right to withdraw their consent at any time. A club should be sure to keep a record of consent.

Legal Obligation – a club may handle personal data if there is a legal obligation to do so. Examples of this include complying with Employment Law (i.e. equality) and complying with Health and Safety legislation (i.e. accident reporting).

Contract – a club may handle personal data if it is necessary for the performance of a contract with the individual.

Special Category personal data

Special category personal data is data such as race, ethnicity, political opinion, religious beliefs, health, etc. Data relating to health is important for football clubs because health includes fitness assessments, details of injury, and medical information. To process this type of personal data a club must identify both a lawful basis for processing and a separate condition to so. For example, it is in the legitimate interest of the individual for a club to collect information relating to their health. In addition to this lawful basis, a club may also obtain consent to handle information about an individual's health. For information about handling special category personal data visit the ICO website.

Children's personal data

Processing children's personal data requires special consideration. A club should verify age and when communicating with children, information should be simple and easy for the child to understand. The club should use parental/guardian consent where necessary.

Breach Notification

Under the GDPR, a club is responsible to handle data protection breaches in a certain way. Examples of breaches are:

- a club official's player registration login and password is stolen/hacked
- data which the club is responsible for ends up in the wrong hands
- lost/stolen laptop or phone which contains personal data from the club.

As soon as a club becomes aware of a breach (or believe a breach may have occurred) it is important to immediately escalate this to the Data Protection Officer so that appropriate procedures are carried out. Significant breaches may mean individuals affected need to be told about the breach, and a club may be required to report the breach to the ICO within 72 hours of learning the breach has occurred.

Retention

A club must not keep personal data for longer than it is needed. Furthermore, a club needs to be able to justify how long the personal data is retained for and communicate to individuals how long they intend to hold the data for. A club should periodically review the data being held, and delete/dispose the data when it is no longer needed. A club may decide the best way to comply is to delete/dispose personal information once the season is finished.

Data Protection Officer

The role of the Data Protection Officer is to assist the club to comply with the GDPR, and act as a point of contact for data subjects and the ICO. A DPO can be an existing employee or externally appointed. Clubs should nominate, or appoint, a DPO as part of the club's governance.