Aontas Teilgin agus Amais Na hÉireann
Pitch and Putt Union of Ireland
IRISH SPORT HQ •NATIONAL SPORTS CAMPUS • BLANCHARDSTOWN • DUBLIN 15
Telephone: 01 - 6251110
Website address: www.ppui.ie E-mail address: office@ppui.ie

General Data Protection Regulation (GDPR) - Club Information

The following information is for club officers and members in relation to GDPR regulations which came into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive. It is important that clubs and members have the relevant information to prepare for this and make necessary changes.

Specific Steps for Pitch and Putt Union of Ireland (PPUI) Clubs to ensure Compliance

It is imperative that every PPUI 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 PPUI Club or County/Regional Board will be accountable for how it collects, uses and stores information about PPUI 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, Online 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

It is imperative that each PPUI 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 (membership forms, competition sheets, etc.) 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?

Specific consideration must 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. It is vitally important that any completed forms are stored securely in a specified location. The PPUI provide a template membership form for clubs to use. Clubs with existing membership forms will be able to insert a section in relation to Data Protection that has been recommended by the PPUI.

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 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 PPUI Clubs will include:

- Information required for Garda Vetting
- Application forms

• Text or messaging systems
• Email lists or distribution groups
• 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'.

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.

Existing membership forms and other forms used to collect data (e.g. Garda Vetting) should be updated to tell, where relevant, 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)

Ensure Personal Privacy Rights

GDPR enshrines certain rights for individuals that must be supported by every Data Controller, including PPUI 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 their information in a standard format to move to another provider (more relevant for switching banks or utility providers than PPUI Clubs but must be supported)

Legal Basis for Obtaining Information

Any organisation processing personal data (name, address, phone number, e-mail, etc.) must be able to refer to at least one Lawful Processing Condition under Article 6 of the GDPR, in order to justify each element of processing.

The following conditions are listed in Article 6:

- **Consent**: The Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes.
- **Contract**: The processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.
- **Legal Obligation**: The processing is necessary for compliance with a legal obligation to which the Controller is subject (e.g. a charity might be obliged to notify Tusla where they become aware of allegations of child abuse).
- **Vital Interests**: The processing of the personal data is necessary in order to protect the vital interests of the Data Subject.
- **Public Interest / Official Authority**: The processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller (e.g. where the charity is acting as an agent for the Department of Social Protection, or the HSE, in providing a service).

- **Legitimate Interest**: The processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

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. Where required 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 a consent or be 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.

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 info@ppui.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 that are 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. PPUI 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 on ways to mitigate the risk of issues occurring.

Identify Designated Data Protection Representative

Every PPUI 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 (files in houses/clubhouses, mobile phones, laptops etc), ensuring that consent is obtained in the appropriate manner and maintained accordingly. The PPUI has a Data Protection Person who will provide guidance for any Data Protection queries that require additional advice. Queries of this nature can be submitted to office@ppui.ie

Top Tips

1. Why is it being held?

For the purposes of registering a member to their local P&P club and getting further individual membership registered to the National Governing Body

2. How was it obtained?

By email, by post, by hand

3. Why was it originally gathered?

Take a look back at why you have it, what was the original purpose? If it was for the purposes of registering a member to their local P&P club and getting further individual membership registered to the National Governing Body, that's fine, if not, it's time to destroy the records

4. How long is it being retained for?

How long does your club intend on keeping personal information of members, specifically past members?

5. How secure is it?

Is it on my personal phone, my personal laptop – have I encrypted my devices if lost or stolen? Have I checked the attic? What ledgers, membership folders, or old record books do I still have, is it time to destroy old records. This only related to holding of personal data.

6. Is it shared with any third parties?

If yes, is there a legitimate reason in line with the purposes of collecting the data i.e. membership registration, competition entry etc, well then that's ok, if you require consent to share it, you must have it from the individual in question. If you have no legitimate reason to share, don't share!

Updated: May 2018