**General Data Protection Regulations**

Rowing Ireland wishes to update all our member Clubs on important changes to Data Protection legislation coming into effect. It is important that every Club and indeed every member is aware of how these changes in the law will affect the way in which members' personal information can be collected and used for Rowing Ireland purposes.

The following article summarises some of the practical changes that need to be made to support compliance with the legislation.

***What is Data Protection?***

***Data Protection legislation is intended to protect the right to privacy of individuals (all of us) and seeks to ensure that Personal Information is used appropriately by third parties that may have it (Data Controllers).***

***In essence Data Protection relates to any information that can be used to identify a living person such as Name, Date of Birth, Address, Phone Number, Email address, Membership Number, IP Address, photographs etc.***

***There are other categories of information which currently are defined as Sen sitive Personal Data which require more stringent measures of protection and these categories include religion, ethnicity, sexual orientation, trade union membership, medical information etc.***

**What is GDPR?**

The General Data Protection Regulations (GDPR) is new EU legislation that comes into effect on May 25th 2018.

It very clearly sets out the ways in which the privacy rights of every EU citizen must be protected and the ways in which a person's 'Personal Data' can and can't be used.

It places the onus on the person or entity that collects a person's information (Data Controller) to comply with the legislation and to demonstrate compliance.

**What does Data Protection Legislation mean to me?**

The legislation sets out rules about how this information (personal Information) can be obtained, how it can be used and how it is stored.

Every person must give their consent for their data to be collected and processed for a specific purpose which must be communicated to them at the time the data is obtained.

They must specifically OptIn and must be allowed to OptOut at any time. They must also be given the opportunity to review the consent they have given on a regular basis (i.e. yearly).

Data must be kept safe and secure and must be kept accurate and up to date.

An Individual can request a copy of all of the personal information held about them (this is called a Subject Access Request) and must be allowed to have all of their data deleted or returned to them, if they so wish.

**Data Protection can be summarised in the following 8 'rules'**

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was given to you initially
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request

**Specific Steps for Clubs to ensure Compliance**

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

1. **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 Club will be accountable for how it collects, uses and stores information about the 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.

Information regarding Data Protection can be found on the website http://www.dataprotection.ie

## 2. Ensure Understanding

It is imperative that each 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 Club is its Membership database.

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 Clubs will include
 Information required for Garda Vetting

 Training camp applications
 Text or messaging systems
 Email lists or distribution groups
 Team sheets, 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'.

### 3. 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) 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 its 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 (See below)

### 4. Ensure Personal Privacy Rights

GDPR enshrines certain rights for individuals that must be supported by every Data Controller, including 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 but Clubs but must be supported).

### 5. 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 it's 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.

### 6. 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.

### 7. 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.

## 8. Identify Data Protection Officers

Every 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.

## General Information

Information relating to Data Protection and GDPR is available on the Data Protection Commissioner's website http://www.dataprotection.ie