Cónaidhm Rámhaíocht Chósta na hÉireann
Irish Coastal Rowing Federation Ltd.

ICRF Data Protection Policy

2018

Terms of Reference

'ICRF'	**:**	**Irish Coastal Rowing Federation**
'Associations'	**:**	**Associations/Councils affiliated to the ICRF representing coastal rowing clubs throughout the island of Ireland**
'Clubs'	**:**	**Coastal Rowing Clubs affiliated to the ICRF**
'Members'	**:**	**All individuals who are registered as a fully paid up member of a Coastal Rowing Club that is affiliated to the ICRF**
'Volunteers'	**:**	**Members of the local community who provide on the ground support for the management of regattas or the All Ireland Championships.**
ICRF Board	**:**	**Elected Committee Members**
Sub-Committees	**:**	**Sub-Committees established by the ICRF Board for a specific purpose.**

Purpose

The purpose of this policy is to outline the rights and responsibilities under the Data Protection Act 1988, the Data Protection (Amendment) Act 2003 and the General Data Protection Regulation 2018 (GDPR). The Irish Coastal Rowing Federation (ICRF) is committed to complying with its legal obligations with regard to the data protection legislation.

The Data Protection legislation imposes obligations on Data Processors and Data Controllers regarding how they process personal data and sensitive personal data. The purpose of this policy is to assist the ICRF to meet its statutory obligations as a Data Processor and/or a Data Controller, to explain those obligations to ICRF members and to inform data subjects how their data will be processed. The GDPR applies to Organisations that:

- are established in one or more Member State(s);
- process personal data (either as controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

Scope

This policy applies to all Members, Clubs and Associations affiliated to the ICRF and to all members of Sub-Committees established by the Board and to all members of the ICRF Board itself.

Policy

Under the Data Protection legislation, employees and volunteers have a right to receive information on data collection, access their personal data, have inaccuracies corrected, have information erased and have a right to data portability.

Personnel records held by the ICRF, Associations and Clubs come within the terms of the Data Protection legislation. Members can make access requests for information held about them. All Members and Volunteers are required to process personal data in line with this policy.

Data Protection Principles

The ICRF and its affiliates will comply with the data protection principles set out in the General Data Protection Regulation, 2018.

The Irish Coastal Rowing Federation ensures that all data is:

1. Obtained and processed lawfully, fairly and in a transparent manner

The ICRF will meet this obligation by informing Members of the purpose(s) for which their data is being processed as well as the legal basis for the processing; to whom their data may be disclosed and if the ICRF intends to transfer data to a third country or international organisation outside of the EEA.

Where processing is necessary for the purposes of the legitimate interests of the ICRF, The ICRF will inform Members of the legitimate interests being pursued. Where the ICRF intends to record activity on CCTV, signage will be posted in full view.

The Organisation will adopt appropriate data protection notices at the point of data capture e.g. application forms.

2. Collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.

The ICRF will obtain data for purposes which are specific, lawful and clearly stated. The ICRF will inform Members of the reasons they collect their data and will inform them of the uses to which their data will be put. Should the Organisation subsequently intend to use the data for another purpose, the consent of the Member concerned will be sought prior to doing so unless a relevant exemption applies.

Data relating to Members will only be processed in a manner consistent with the purposes for which it was collected. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

The ICRF will not share Members personal information for direct marketing purposes outside of the organisation.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data are processed.

The ICRF will ensure that the data it processes are relevant to the purposes for which that data is collected. Any personal data which is not required will not be collected in the first instance. Prior to obtaining personal data, the ICRF will ensure that the information sought is essential for the purpose for which data is being obtained and that data will not be kept for longer than is necessary for the purpose for which it was collected.

4. Accurate and up to date.

The ICRF is required to keep Members data accurate and up to date and will meet this obligation by:

- Obtaining and processing only the necessary amount of information required to provide an adequate service;
- Conducting periodic reviews to ensure that relevant data is kept accurate and up-to-date;
- Conducting regular assessments in order to establish the need to keep certain Personal Data.

If a Member or Volunteer informs the ICRF of a change in their personal information the ICRF will ensure this information is updated on all relevant ICRF internal systems and all third party providers are notified of this change where necessary.

5. Limited retention in a format that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The ICRF will ensure that the data is kept in a form that permits identification of Members or Volunteers for no longer than is necessary for the purposes for which the personal data was processed.

Applications for Garda Vetting

- Upon receipt of a successful vetting disclosure all personal data relating to the applicant will be destroyed;

- Applications pending for longer than one month (31 days) will be destroyed and the vetting process started again.

Applications for participation in the All Ireland National Championships

- Upon completion of the respective All Ireland National Championships all personal data relating to applicants will be destroyed.

Once the respective retention period has elapsed, the ICRF undertakes to destroy or erase personal data.

6. Secure and confidential processing of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

The ICRF will undertake appropriate technical and organisational measures in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, unlawful processing, accidental loss, destruction or damage of any personal data held by the ICRF in its capacity as Data Controller.

Only Members or Volunteers with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key- in the case of manual records / protected with firewall software and password protection- in the case of electronically stored data.

Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the ICRF's premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

Members and Volunteers are also expected to keep Personal Data secure by adopting the following measures:

- Using secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold personal data.
- Paper documents containing personal data should be shredded.
- Data users should ensure that individual monitors do not show Personal Data to passers-by and that they log off from their PC or password protect their PC when it is left unattended.

If the ICRF discovers that there has been a data security breach that poses a risk to the rights and freedoms of individuals, it will report it to the Data Protection Commissioner within 72 hours of discovery. If the breach is likely to result in a high risk to the data protection rights and freedoms of a Member/Volunteer, it will inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

7. The ICRF is committed to being accountable, liable and to comply with the Data Protection Principles.

Purposes for which Members/Volunteer records are held

Personal data records are provided to the ICRF by Members/Volunteers by way of a contractual requirement for the following purposes:

- The management and administration of the ICRF
- To enable the ICRF to comply with its legal obligations as a voluntary organisation including the preservation of a safe, efficient working environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act 2005 and the 2007 Health and Safety Regulations) and the Child Safeguarding Act 2015.

Collection and Storage of data

This Policy applies to all Personal and Sensitive Personal Data collected, processed and stored by the ICRF. In the course of its activities and in order to carry out its function, the ICRF processes personal data from a variety of sources. These sources include data in relation to its Members, Volunteers, service providers, suppliers, customers and any other Data Subjects in the course of its activities.

The main categories of Personal Data held by the Organisation ***may include***:

- Name, address and contact details,
- Details of any accidents/injuries sustained on ICRF property or in connection with the member/volunteer carrying out their duties
- Records of any interactions under the headings of grievance and discipline
- Training courses completed and qualifications awarded
- Occupational health reports
- Photographic/CCTV data
- Email system data
- Phone records
- Records of application for membership, Garda Vetting
- External appointees to sub committees

The ICRF will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection legislation.

Personal data is normally obtained directly from the Member/Volunteer concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties e.g. references

Data Processing in line with Members'/Volunteer's Rights

The Organisation will process data in line with Members'/Volunteer's right to:

- receive certain information regarding the collection and further processing of their personal data;
- request access to any data held about them by a data controller;
- have inaccurate data corrected;
- have information erased;
- object to the processing of their data for direct-marketing purposes;
- prevent processing that is likely to cause damage or distress to themselves or anyone else;

- restrict the processing of their information;
- where processing is based on consent, to withdraw that consent at any time;
- data portability;
- object to automated decision-making and profiling.

Right to opt-out

The ICRF will inform members/volunteers that information is being collected and used for these purposes prior to doing so. Members/Volunteers have the right to object to any specific type of data processing. Where such objection is justified, the ICRF will cease processing the information unless it has a legitimate business interest that prevents this.

Right to be forgotten

Members and volunteers may request that any information held on them is deleted or removed if there is no legitimate reason for the ICRF to keep it. Any third parties who process or use that data will comply with the request.

Storage of personal data

Personal data kept by ICRF shall normally be stored on the Members'/Volunteer's personnel file and/or electronic database.

The ICRF will ensure that only authorised personnel have access to an Member's/Volunteer's personnel file.

The ICRF has appropriate security measures in place to protect against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Changes in Personal Details

Members and Volunteers are responsible for ensuring that they inform the ICRF of any changes in their personal details e.g. change of address.

The ICRF will endeavour to ensure personal data held by it is up to date and accurate.

The ICRF is under a legal obligation to keep certain data for a specified period of time.

Disclosure of Personal Data to Data Processors

In the course of its role as Data Controller, the ICRF may engage a number of Data Processors to process personal data on its behalf. In each case, it is the ICRF's policy to have a contract in place with the Data Processor, outlining their obligations in relation to the personal data, the specific purpose or purposes for which they are engaged, and the requirement that they will process the data in compliance with the Data Protection legislation.

As a Data Controller, the ICRF ensures that any entity which processes personal data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Security and Disclosure of Data

The ICRF shall take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data.

Security measures will be reviewed from time-to-time having regard to the technology available, the cost and the risk of unauthorised access. Members and volunteers must implement all ICRF security policies and procedures e.g. use of computer passwords, locking filing cabinets etc.

- All affiliated clubs must ensure that all personal data relating to member applications is held in a secure/lockable location for no longer than is reasonably necessary;
- All affiliated clubs must not maintain a copy of individual Garda Vetting Applications. All applications must be submitted to the ICRF Child Protection Officer;
- All Garda Vetting Applications received by the ICRF Child Protection Officer will be secured in a lockable container and any data held on a computer will be password protected. All vetting applications will be destroyed:
    - Once the individual applicants vetting application has been completed;
    - After 31 days.
- All applications for participation at the All Ireland National Championships will be held in a lockable container and destroyed within one week of the completion of the respective Championships.

If any Association/Club is in any doubt regarding their obligations they should contact the ICRF. A briefing document will be issued to each affiliated club and association.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal.

Medical Data

Any personal data relating to the medical condition of any member/applicant/volunteer will be held for no longer than is necessary. Any member/applicant/volunteer has the right to request access to any personal medical data held by the ICRF.

Access Requests

Members and volunteers are entitled to request data held about them on computer or in relevant filing sets. This includes personnel records held by the ICRF. The ICRF will ensure that such requests are forwarded to the Chairperson in a timely manner, to enable them to process the request within the required timeframe. To make a subject access request, a Member/Volunteer should send the request by email to the ICRF Chairperson requesting access. In some cases, the ICRF may need to ask for proof of identification before the request can be processed. The ICRF will inform the Member/Volunteer if it needs to verify his/her identity and the documents it requires.

A data access request will be responded to within 1 month of receipt of the request though this period may be extended for up to 2 further months where necessary, taking into account the complexity and number of requests. The ICRF will write to the individual within 1 month of receiving the original request to tell him/her if this is the case.

Information will be provided in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If a Member or Volunteer makes a data access request, the ICRF will inform him/her of:

- The purposes of the processing;
- The categories of personal data concerned;
- To whom the personal data has been or will be disclosed;
- Whether the data will be or has been transferred outside of the EU;

- The period for which the data will be stored, or the criteria to be used to determine retention periods;
- The right to make a complaint to the DPC;
- The right to request rectification or deletion of the personal data;
- Whether the data has been subject to automated decision making.

Formal requests, invoking the right to access to personal data must be made in writing.

Members/Volunteers are only entitled to data about themselves and will not be provided with data relating to other Members, Volunteers or third parties. It may be possible to block out the data relating to a third party or conceal his/her identity, and if this is possible the ICRF may do so.

Data that is classified as the opinion of another person, will be provided unless it was given on the understanding that it will be treated confidentially. Members/Volunteers who express opinions about other Members/Volunteer in the course of the performance of their duty e.g. committee member should bear in mind that their opinion may be disclosed in an access request, e.g. performance appraisals.

A Member or Volunteer who is dissatisfied with the outcome of an access request has the option of using the ICRF's grievance procedure.

Retention of personal data

Personal data is retained for a period of time to meet certain legal obligations. Once the respective retention period has elapsed, the Organisation undertakes to destroy or erase personal data. If there is no legal basis for the retention of the data it will be destroyed once the purpose of the data has been fulfilled.

Responsibilities

The ICRF will endeavour to ensure that this policy is communicated to all Members/Volunteers and will ensure that the policy is maintained and updated in line with legislative changes.

Members and Volunteers are expected comply with this policy and to raise issues of concern to the ICRF Board.

Failure by Members or Volunteers to process personal data in compliance with this policy may result in disciplinary proceedings up to and including expulsion from the ICRF, Association and Club.

Complaints

Members and Volunteers have the rights to lodge a complaint to the Data Protection Commissioner if they believe their rights under the Data Protection legislation are not being complied with by the ICRF.