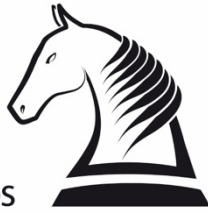


A.I.R.C.

Association of
Irish Riding Clubs



Reference: D151/21
Issued: 14/05/2021
Amended:

Privacy Policy

1. Introduction

The Association of Riding Clubs (AIRC), (“we” or “us”) is an association that strives to promote equestrian activities throughout Ireland. Our mission statement is, “Encouraging riding as a sport and recreation, to promote good fellowship among riders and to improve and maintain the standard of riding and horsemastership in Ireland”.

This Privacy Policy covers how we collect, process and store Personal Data where we are defined as the Data Controllers as outlined in the General Data Protection Regulation 2016/679 (“GDPR”) and the Irish Data Protection Act 2018. It ensures that we:

- are open and transparent in relation to how we collect, store and process individuals’ Personal Data,
- are compliant with the relevant data protection legislation and follow what is considered good practice in protecting the Personal Data collected, stored, and processed,
- protect the rights of our staff, members, volunteers, partners, visitors to our website or any other parties whose data we process, and
- implement appropriate technical and organisational measures to protect the Personal Data we process and keep it secure.

2. Scope

This policy covers the processing activities of AIRC as a controller of Personal Data.

3. Key Definitions

The key definitions are set out in the Data Protection Act 2018 and the GDPR and are summarised below.

The term "**Personal Data**" is information related to a living individual who is or who can be identified:

- a) from the data, or
- b) from the data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

The term "**special categories of Personal Data**" means Personal Data revealing:

- racial or ethnic origin,
- political opinions,

- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data for the purposes of uniquely identifying a natural person,
- any form of health information, and
- a natural person's sex life or sexual orientation.

Data "**processing**" includes obtaining, recording or holding information and carrying out any operation on the information such as organising, altering, using, disclosing, erasing or destroying it.

A "**Data Subject**" is an individual who is the subject of Personal Data. This includes partnerships and groups of individuals, but not limited companies.

A "**Data Controller**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

A "**Data Processor**" means any person (other than an employee of NearForm) who processes the data on our behalf.

"**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

4. Privacy Essentials

Principles of Data Processing

Article (5)(1) of the GDPR covers the principles of data processing. We are mindful of these principles at all times, and we ensure that Personal Data is:

- processed lawfully and fairly and that we are transparent about how and why we process data ('lawfulness, fairness and transparency'),
- only collected when there is a specific purpose to do so and that we do not further process data in a manner that is incompatible with the original purpose ('purpose limitation'),
- adequate, relevant and limited to what is necessary for the purpose for which it was collected ('data minimisation'),
- accurate and, where necessary, kept up to date ('accuracy'),
- only kept for as long as it is necessary for the purpose for which it was collected ('storage limitation'),
- kept secure at all times and is protected against any unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'),

As per Article (5)(2) of the GDPR we must also be able to demonstrate compliance with, the above listed principles and be held accountable at all times ('accountability').

Data Subject Rights

Individuals have certain rights regarding their Personal Data, and it is important to us that we respect these rights so that you feel in control of your data. There are certain exemptions to these rights; should you look to exercise any of these rights, we will always be clear in our communications with you and inform you if an exemption applies.

Right of access: You have the right to ask if we hold any of your Personal Data and, if we do, to receive copies of this data as well as details relating to the processing and any third parties in receipt of the data. However, we cannot give you access to a copy of your data if this would adversely affect the rights and freedoms of others.

Right of rectification: If any of the Personal Data we hold is inaccurate, you have the right to request us to correct it.

Right to be forgotten: In certain circumstances, you have the right to request that we delete your Personal Data. Examples include:

- where the data is no longer needed for the purpose for which it was originally collected,
- you have withdrawn your consent for us to use your data (where there is no other legal reason us to use it),
- there is no legal reason for us to process your data,
- deleting the data is a legal requirement.

Right of restriction: You can restrict the use of your data unless we have an overriding legitimate lawful purpose for continuing to process the data.

Right to data portability: You have the right to ask for your Personal Data to be returned to you or given to another Data Controller in a commonly used format. This right only applies to Personal Data being processed under the lawful basis of consent, or pursuant to a contract, and where the processing is automated and not manual. It does not apply where it would adversely affect the rights and freedoms of others.

Right to object: The instances where you have the right to object to the processing of your data are:

- when your objection is based on the grounds of public interest or legitimate interest including profiling based on these grounds;
- when data is used for direct marketing purposes.

Rights relating to automated decision making/profiling: You have the right not to be subject to a decision based solely on automated processing, including profiling, which has significant effects on you. This right shall not apply where the processing:

- is necessary for entering into, or performance of, a contract,
- is based on your consent, or
- is authorised by law.

Right to make a complaint: You have the right to make a complaint to a relevant Supervisory Authority, in Ireland this is the Data Protection Commission (“DPC”). The contact details are:

Email: info@dataprotection.ie
Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28.
Tel: 1890 252 231

5. How We Collect Information

In order to run our association and to provide our services to members, we must process certain Personal Data. This data may be collected by various means including:

The general operation of our association services: We receive and store information you provide directly to us when:

- you make inquiries about our association,
- you join as a member,
- you or your parent/guardian communicate with us for any reason,
- you engage with us in connection with any service or event,
- you sign up to become a volunteer.

Provided to us from affiliated clubs: We will receive personal information from affiliated clubs when:

- your club submits membership forms to us on your behalf,
- you register to participate in an event,
- your club shares your information for the purpose of providing you with a service you have requested.

From our website, social media pages or events: We may collect any personal information through the operation of social media pages or other online platforms or through the sharing of videos on You Tube when:

- you visit our website, we collect certain information related to your device,
- if you engage with us through our social media platforms,
- when you share a video on YouTube,
- when you attend an event where video footage is taken,
- if you engage with us through our social media platforms.

6. Types of Personal Data

We require certain Personal Data in order to provide our services to you and your club, and to operate our association, this includes:

Personal Data Type	Description
Identity	Name, gender, date of birth, guardian details (if under 18)
Communication & correspondence	Address, email, phone number's
Grading & membership data	Club membership details, photo, grading information, competition history, examination history, ownership or

	breeder information (on horse's passport), insurance details
Financial data	Payment information (transactions only we store do not store card details)
Web, events & social media	<u>Website</u> : your device's IP address, referring website, what pages your device visited, date and time of visit <u>Events</u> : registration details, contact details, grading level, competition history <u>Social Media</u> : photos, videos, achievements, general personal information publicly available
Volunteer data	Identity, contact details, riding club details, member number, proposer and seconder information, a biography and any other criteria relevant to your volunteer application such as Garda Vetting details
Employee Data	Identity, contact details, date of birth, education, qualification and training information, occupation, work history, salary details, PPSN, bank details and all other information that we are obliged to process under our duties as an employer.

7. Lawfulness of Processing

For all processing of Personal Data, we are required by law to identify a lawful basis on which the processing is based. These are defined in Article (6)(1) of the GDPR. Here we provide further information about the legal grounds we have for processing Personal Data:

Lawful Basis	Details
Performance of a contract	<ul style="list-style-type: none"> - to register members with our association, - to register you for events, training or courses run by AIRC, - to process payments for our services or to contact you regarding payments, - to record achievements at competitions, - to ensure your grading information is accurate and up to date.
Consent	<ul style="list-style-type: none"> - to send direct electronic marketing material to individuals where consent applies, - to use certain non-essential cookies on our website.
Legitimate Interests	<p>When using this lawful basis, we will ensure that the legitimate interest pursued does not infringe on your privacy rights. Our legitimate interests include:</p> <ul style="list-style-type: none"> - to carry out optional, anonymous surveys,

	<ul style="list-style-type: none"> - to inform members of changes to events or cancelled events, - to ensure the appropriate governance of our association, - to handle complaints or appeals, - to promote our events, - publishing achievements and competition results on our social media platforms, within our sport at a national level, - to provide you with notice of general meetings, - to correspond with club officials, volunteers, contractors and staff, - sourcing and recruiting volunteers, - sourcing and recruiting staff and contractors.
Legal Obligation	<ul style="list-style-type: none"> - to carry out Garda Vetting and identity checks, - to ensure the health & safety of our members, staff, volunteers, - to report any accidents or incidents, - to meet our insurance requirements, - to meet our legislative and regulatory requirements, - to maintain proper accounts, - to fulfil our obligations as an employer,

Article (9) of the GDPR deals with processing special categories of data.

In the context of our role as an employer, we may be obliged to process certain health data to meet legislative requirements. It may also be necessary for us to collect specific health data from our members so as to ensure their health and safety where there are relevant medical conditions which may affect their riding.

Due to the Coronavirus pandemic, it may be necessary for us to process some special category data. When we do this, our lawful basis is “processing is necessary for reasons of public interest in the area of public health”. We will act upon the guidance of Public Health Authorities at all times to protect the health and safety of our staff, customers and the wider public when it is necessary to do so.

8. Data Sharing and Transfers

We do not sell any personal information, nor do we share it with unaffiliated third parties unless we are required to do so by law. Where we engage the services of Data Processors on our behalf, we ensure that this processing is done with respect for the security of Personal Data and will be protected in line with data protection law. A written contract will be in place with any Processors prior to any information being

shared, this contract places specific obligations on Processors and guarantees the security of the data.

Ways in which we may share personal information include:

- with HSI for the provision of certain services,
- with affiliated clubs to enable us to carry out our functions (a Data Sharing Agreement is in place with each club),
- with course providers, judges, coaches or any other such parties in relation to events,
- with volunteers so as to enable them to perform their duties, all volunteers are bound by obligations of confidentiality,
- to avail of web-based hosted services (eg. Dropbox, Amazon, Google),
- when contracting suppliers (Data Processors) to carry out processing on our behalf,
- to engage external IT providers so as to ensure the security of our IT systems in order to protect Personal Data (currently Hosting Ireland),
- to engage the professional services of third parties, such as consultants, auditors, solicitors or any other such business advisers. Any such parties are bound by obligations of confidentiality,
- if we are collaborating with external parties in organising an event, training, or similar activity,
- we engage providers to administer and evaluate our website,
- with our insurers or assessors when providing or reviewing information if an incident occurs,
- to assist the Gardaí and other competent authorities with investigations including criminal and safeguarding investigations,
- we reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal.

In cases where we transfer your data outside the EU, we will ensure that specific safeguards are in place prior to sharing your data. Such safeguards will be in line with Article 46 GDPR. At present, the only third party outside the EU with whom data is shared is Mail Chimp for the issuing of our Newsletter. Mail Chimp have provided us with their agreed Data Processing Addendum outlining how they meet their obligations as a Data Processor.

9. Security Measures

We ensure the confidentiality, integrity, availability, and resilience all data of which we are a Data Controller. We are obliged to protect the data from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing and our organisational and technical security measures deliver on our commitment.

Access Control

- Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their task,

- Staff and volunteers shall be identified by a unique user ID so that individuals can be held accountable for their actions,
- We instruct users ensure strong password are used (length, complexity),
- All users who have access to our systems are issued with new details whenever a role changes.
- When volunteers change, new details are issued to the new volunteers.

User Responsibilities

All users, which includes staff, volunteers and other individuals such as Club Secretaries, who have access to our systems are instructed to:

- lock their devices whenever they leave their desks to reduce the risk of unauthorised access,
- keep sensitive or confidential information secure at all times,
- keep their passwords confidential and not share them,
- always log off completely when ending a session,
- protect the Personal Data they handle during the course of their work.

Any third parties who process Personal Data on our behalf are contractually bound to process Personal Data in line with current data protection law practices and principles thus ensuring the security of the data.

Technical Securities

- Our IT partners ensure that our systems are protected and that backups are done and stored securely,
- We use cloud-based storage with Hosting Ireland, with appropriate security measures that are implemented under contract,
- All anti-virus software is kept up to date.

10. Cookies

Our website at www.airc.ie uses cookies to help us to provide a good user experience for visitors to our website and to make any necessary improvements to our site. Using cookies enable us to customise the website according to your individual interests from information stored about your preferences. They are also used to monitor which parts of the website are most popular to visitors.

We have implemented a cookie management tool on our website offering you the option to select your preferences in relation to what cookies you permit us to use during your visit to our website.

Full details can be found in our Cookies Notice in the footer on our website.

11. Data Retention

We only keep your data as long as it is necessary for the purposes for which it was originally collected or to comply with legal or regulatory requirements. When determining the retention period, we take into account various criteria, such as the type of services requested by or provided to you, the nature and length of our relationship with you, mandatory retention periods provided by law and the statute of limitations.

We retain certain information following cessation of membership with our association for the purposes of verifying grading details for returning members.

Should you require any specific information regarding the retention of your data, please contact us directly.

12. Privacy by Design and Default

Article 25 of the GDPR stresses the importance of Privacy by Design and Default. It puts an obligation on organisations to ensure that privacy is considered at all levels of the design and development of processing and this is particularly relevant to new technologies.

In any instances where we are introducing new technology for the processing of Personal Data, we will ensure that privacy is not an afterthought and will liaise with providers to address any concerns.

13. Personal Data Breaches

Article 4(12) GDPR defines a 'personal data breach' as:

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

AIRC may suffer a breach for a number of reasons including:

- the disclosure of confidential data to unauthorised individuals,
- improper disposal of documents,
- loss or theft of data or equipment on which data is kept,
- loss or theft of paper records,
- inappropriate access controls allowing unauthorised use of information,
- suspected or actual breach of our IT security,
- attempts to gain unauthorised access to computer systems, e.g. hacking,
- viruses or other security attacks on our IT systems or cloud storage,
- breaches of physical security,
- breach as a result of third-party breach, and
- emails containing personal or sensitive information sent in error to the wrong recipient.

In the event of a breach of personal data occurring, we will ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

Each breach will be handled on a case by case basis and the level of risk to individuals caused by the breach will determine our notification. Where we deem there to be a significant risk to individuals, we will inform the Data Protection Commission within 72 of becoming aware of the breach. Where it is deemed necessary, individuals will also be notified without undue delay.

14. Subject Access Requests

You have the right to be informed whether we hold data/information about you and to be given a description of the data together with details of the purposes for which your data is being kept. You must make this request to us in writing and we will accede to the request within one month if it is deemed valid. In certain cases, it may be necessary for us to first verify your identity to ensure the request is legitimate.

Where a subsequent or similar request is made soon after a request has just been dealt with, it is at our discretion as to whether or not we need to comply with the second request. This will be determined on a case-by-case basis.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable we must refuse to furnish the data to the applicant.

15. Data Protection and Covid-19

In order to ensure that we comply with the Public Health guidelines about what organisations must do to play their part in containing the spread of Covid-19, we may be obliged to process certain special categories of data, such as health data. Other additional details may be sought including: name, address and contact details, travel information, details of close contacts and other relevant information where it is deemed necessary and proportionate to collect this data.

The collection of data in relation to managing our response to the Covid-19 pandemic, is carried out on the lawful basis of Article 9(2)(i) GDPR Section 53 of the Data Protection Act 2018 which states:

“processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy”

Also, Recital 46 GDPR states:

“Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread”

We may be obliged to share this data with certain Public Authorities when they instruct us to do so.

16. Updates

This Privacy Policy may be updated from time to time to reflect changes in our privacy practices. Please refer to our website for the most up to date version.

17. Contact Details

If you have any questions, concerns or suggestions related to our Privacy Policy, you can contact us using our details below:

Email: info@airc.ie
Address: 1st Floor, Beech House, Millennium Park, Osberstown, Naas, Co. Kildare, W91 TK7N
Tel: 045 854 555

You have a right to complain to the Data Protection Commission (DPC) in respect of any processing by using the details below:

Email: info@dataprotection.ie
Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28.
Tel: 1890 25 22 31
Webform: <https://forms.dataprotection.ie/contact>