



Royal Irish Automobile Club (RIAC)

Data Protection Policy

Last updated: 20/05/2019

DATA PRIVACY POLICY

This Data Privacy Policy specifies the information collected by the Royal Irish Automobile Club (RIAC), its members and affiliates, specifically how it is collected, processed, stored, maintained, shared and erased.

We reserve the right to amend this Data Privacy Policy at any time without prior notice. We advise you to check our website <http://www.riac.ie/> regularly for any amendments.

It is important that you read this, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using such information.

We will always comply with General Data Protection Regulation (GDPR) when dealing with your personal data. You can find further details on the GDPR at <http://gdprandyou.ie/>

All personal data is processed in accordance with the requirements of Irish and European data protection legislation, including the:

- General Data Protection Regulation (GDPR), or Regulation (EU) 2016/679
- Data Protection Act 2018

The Office of the Data Protection Commissioner is the independent national authority in Ireland for upholding the right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation.

The purpose of this Privacy Policy is to inform our members* about the collection and treatment of personal data collected, in accordance with the relevant acts mentioned throughout this document.

The General Data Protection Regulation ('GDPR') and the Data Protection Act

The GDPR and Data Protection Act set out rules for processing personal data i.e. information held about living individuals who can be identified from the data either by itself or when taken with other information we hold about them. It applies to some paper records and to those held on computer.

The Act has eight principles of good practice for the processing of personal data. This Policy addresses each of the eight principles, describing how the RIAC adheres to the requirements of the Act.

The principles for good information handling

The eight principles set out in the Act state that data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;

* 'Member' refers to all those who are members of the Royal Irish Automobile club or the Royal Irish Automobile Club Archives.

- Processed in line with the data subject's rights;
- Secure; and
- Not transferred to other countries without authorisation and adequate protection.

About Us

The Royal Irish Automobile Club (also known as 'RIAC', 'we', 'our' or 'us') understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of members and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

Registered Company Address: Royal Irish Automobile Club, 34 Dawson Street, Dublin 2, Ireland.

Our company number is 3100 registered in the Republic of Ireland as a Company Limited by Guarantee ("CLG").

Data Protection Officer

RIAC is the data controller and data processor as defined. A Data Protection Officer (DPO) does not need to be appointed.

Use of data

Data held by the RIAC may only be used for the purposes for which it has been collected and stored.

For RIAC staff and consultants, data may only be accessed and used in relation to day-to-day duties.

Exigent Network Integration Ltd T/A Paradyn (Registered in Ireland: 438887) and/or other appointed IT partners only may access RIAC data for the purpose of supporting the RIAC's IT systems.

We may collect some or all the following personal data; this may vary according to your type of relationship with us:

<i>Type of Information</i>	<i>Purposes</i>	<i>Legal Basis of Processing</i>
Member's name, address, contact number, email address and associated clubs.	Issuing and managing membership.	For the purpose of our legitimate interests in operating and governing all aspects of the membership organisation.
Member's business address, occupation, contact number, email address.	Issuing and managing membership.	For the purpose of our legitimate interests in operating and governing all aspects of the membership organisation.
Details of your first /second of membership. (including work contact details)	Issuing and managing membership.	For the purpose of our legitimate interests in operating and governing all aspects of the membership organisation.
Date of Birth	Administration of categories that are age related and organising overseas trips.	For the purpose of our legitimate interests in operating and governing all

		aspects of the membership organisation.
Medical Information	Providing accurate information to medical professionals in the event of an emergency.	Protecting the members vital interests and those of their dependents.
Medical Contact Details	Contacting the member's doctor in the event of an emergency.	Protecting the members vital interests and those of their dependents.
Member payment information	Taking payment for the applied membership, parking and restaurant fees.	Completing the agreed transaction before secure disposal.
Passport Details	Administration of categories that are age related and organising overseas trips.	The processing is necessary for the performance of a contract to which the member is a party.
Members/guests name and contact details.	Required for security and use of facilities such as the board room / clubhouse.	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Job applications	To process your application. Where we want to disclose information to a third party, for example, where we want to take up a reference, we will not do so without informing you beforehand. Personal information about unsuccessful candidates will be held for up to 12 months after the recruitment exercise has been completed, after which it will be destroyed, unless you have asked us to destroy it earlier or allowed us to retain it for longer by written request.	The processing is necessary for the taking of steps at the request of the data subject with the view to entering into a contract.
CCTV	Closed Circuit Television (CCTV) images to provide a safe and secure environment for staff and visitors and to protect the RIAC property from loss or damage. CCTV images may be retained for up to 28 days and then destroyed, save for where an incident has been recorded and there is an ongoing investigation of claim arising from it.	For the purpose of our legitimate interests in operating and governing all aspects of the membership organisation.

Cookies

Our website uses cookies. Cookies are text files that are stored in the internet browser or by the internet browser on the user's computer system. If a user accesses a website, a cookie may be stored on the user's operating system. That cookie contains a string of characters (cookie ID) that enables clear identification of the browser and recognition of the user when the website is visited again.

That enables us to provide more user-friendly services to users of our website than would be possible without using cookies.

Users of our website can permanently disable cookies at any time by adjusting the settings of the used internet browser accordingly. Furthermore, already stored cookies can be deleted at any time via the relevant internet browser or other software programs.

All information on website cookies can be found in the RIAC Cookie Policy document on our website (www.riac.ie).

RIAC complies with its obligation under GDPR by keeping personal data up-to-date, by storing or destroying it securely, by not collecting or retaining excessive amounts of data, by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate measures are in place to protect personal data.

We use your personal data for the following purposes, to:

- enable us to provide our membership services
- administer membership
- manage our members
- maintain our own financial accounts, event records and invoicing
- supply you with information by telephone, e-mail or post
- ensure we are complying with the requirements of our insurers
- comply with EU regulatory requirements

Lawful Bases of Processing

We acknowledge that processing may be only carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity, which can be viewed in the above table.

Where no other lawful basis applies, we may seek to rely on the member's consent in order to process data.

Storage of Personal Data

All our administrators are aware that hard copy personal information should be kept in a locked filing cabinet, drawer or safe. They are aware of their roles and responsibilities when their role involves the handling and processing of personal data, and are instructed to store files or written information of a confidential nature in a secure manner so that are one accessed by people who have a need and a right to access them and to ensure that screen locks and enabled on all desktops and laptops etc. when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be encrypted or password protected, either on a local hard drive or on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer or safe. Personal data relating to members will not be kept or transported on laptops, USB sticks, or similar devices, unless prior permission has been received. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives etc. are not left where they can be stolen, and in the case of such an event occurring, to report the incident to the relevant authorities without delay

Your Rights

You have the following rights under GDPR:

- to be informed about the data we hold on you and what we do with it
- to access the data, we hold on you
- for any inaccuracies in the data we hold on you to be corrected
- to have data deleted in certain circumstances
- to restrict the processing of the data
- to transfer the data, we hold on you to another party
- to object to the inclusion of any information
- to regulate any automated decision-making and profiling of personal data

Access to Data

As stated above, all members have a right to access the personal data that we hold on them. To exercise this right, members should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the member making the request. In these circumstances, a reasonable charge may be applied.

To submit a Subject Access Request, please send a written request by e-mail to info@riac.ie or via post to our registered address; **RIAC, 34 Dawson St, Dublin 2, Ireland.**

Data Disclosures

RIAC may be required to disclose certain data to any person or third party. The circumstances leading to such disclosures include, but are not limited to:

- when required by or permitted by law or lawfully necessary to protect RIAC and its legitimate interests

- requests from authorities, law enforcement agencies, court orders, legal procedures, obligations related to the reporting and filing of information with authorities or insurers

These kinds of disclosures will only be made when strictly necessary such as the above purposes or if we have received your explicit consent for such transfer of your personal data.

RIAC does not transfer personal data to any recipients outside of the EEA, unless this on the specific request of the member.

Any third parties to whom RIAC data is disclosed must explicitly agree to

- abide by the requirements of the GDPR Act and this policy;
- use the data only for the purpose for which it was provided, and
- either return or destroy the data immediately after the approved use.

Contact Us

To exercise all relevant rights, queries or complaints please in the first instance contact **info@riac.ie** or on **+353 (0)1 677 5551**.

You can contact the Data Protection Commission via e-mail info@dataprotection.ie, or by telephone +353 (0)57 8684800 or at Data Protection Commission, Canal House, Station Road, Portarlinton, Co. Laois, R32 AP23, Ireland.