RDA Ireland Data Protection Policy (May 2018)

Introduction

RDA Ireland (RDAI) holds information about riders, carriage drivers, volunteers and other people involved with our activities. We have a responsibility to look after this information properly, and to comply with the EU General Data Protection Regulation (GDPR) from 25th May 2018.

This Data Protection legislation safeguards the privacy rights of individuals in relation to the processing of their personal data. Good data protection is not just a matter of legal compliance and ticking the boxes, it is about taking care of people and respecting their privacy. Poor practice or a serious breach could not only harm individuals but would also have a serious effect on the reputation of RDAI as a whole.

Our legal basis for using people's data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, even deleting it – will have an acceptable legal basis. There are six of these:

- Consent from the individual (or someone authorised to consent on their behalf).
- Where it is necessary in connection with a contract between our organisation and the individual.
- Where it is necessary because of a legal obligation – if the law says you must, you must.
- Where it is necessary in an emergency, to protect an individual's 'vital interests'.
- Where it involves the exercise of a public function – i.e. most activities of government, local government and other public bodies.
- Where it is necessary in our legitimate interests, as long as these are not outweighed by the interests of the individual.

Data Protection Principles

The six GDPR Principles say that:

- Whatever you do with people's information has to be fair and legal. This includes making sure that they know what you are doing with the information about them.
- When you obtain information, you must be clear why you are obtaining it, and must then use it only for the original purpose(s).
- You must hold the right information for your purposes: it must be adequate, relevant and limited to what is necessary.
- Your information must be accurate and where necessary, up to date.
- You must not hold information longer than necessary.
- You must have appropriate security to prevent your information being lost, damaged or getting into the wrong hands.

Our policy sections below reflect each of these principles in a little more detail.

Transparency and purposes (1st and 2nd Principles)

We will make key information available to people at the time we collect it from them. This information is reflected in our Privacy Statement on our website. This information includes:

- The identity and contact details of the RDAI key personnel and the person who is responsible for Data Protection.
- The purposes we intend to use the data for and our 'legal basis' for this.
- Any specific recipients of the data (e.g. RDAI Council/Areas)

Other information will be made available where relevant. This includes:

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- Details of the individual's rights, such as to request a copy of all the data held.
- The right to withdraw consent if that is the legal basis for processing (but not retrospectively).

In such cases, we will only tell people things they won't already know. When a rider/carriage driver joins a group, they know that we will keep a record about them and their activities with us. When a volunteer joins RDAI the same will apply. This could include:

- Any additional purposes that we might use the data for – i.e. publicity (data can include photos, videos, CCTV, audio recordings etc, not only written records).
- Any direct marketing that we may want to carry out.

Data quality, record keeping and retention (3rd, 4th and 5th principles)

Our activities will be more effective and appropriate if we have good quality records about the people we work with. GDPR insists on this. We will ensure we have the information we need, but no more (it must be adequate, relevant and limited to what is necessary) and it will be as accurate as we can make it and – where necessary – kept as up to date as possible. We will not keep it longer than necessary.
We will have a clear policy on how long to keep information. We will draw up a retention schedule, taking each type of record we hold and specifying how long we normally keep it, and our justification for this. We will set up a process for ensuring that data is deleted or destroyed routinely at the appropriate time.

Security (6th principle)

We will take good care of the information we hold, whether on computer or on paper.
In particular, we will think about the risks when data is "in transit" – either on portable devices or when it is being sent out. For example:

- If people are using their personal phone, laptop, camera or other device for RDAI purposes, there will be clear expectations of how they should be secured.

- When sending information, particularly by email, we will take steps to prevent confidential information being sent to the wrong person e.g. by using password-protected documents and sending the password in a separate email.
- We will take care not to disclose people's email addresses or other information inappropriately by carelessly copying to a large number of people or forwarding an email that has been copied widely.
- Information on paper will not be left lying around and will only be taken out of a source location when this is really necessary.
- Where information is processed for us externally, we will expect the external organisation to be able to give us satisfactory guarantees about the security measures they take.

Responsibility for compliance with Data Protection lies with our organisation, not with any specific individual. The Trustees as a whole body will be responsible for keeping up to date with any developments, to check that RDAI is complying and have the evidence to prove it, and to handle any issues such as a data breach or a Subject Access Request. The Trustees may designate someone to be the lead person.

When we work in collaboration with other organisations we will agree and clarify who is responsible for what, in order that there are no Data Protection gaps.

If we engage external suppliers to handle data for us in any way, data will be processed and maintained in a safe manner and in a way that will not cause us to be in breach.

June 2018.