



# Trail Riders Fellowship

---

Information Note and Policy GDPR V1.0 April 2018

General Data Protection Regulation (GDPR) Regulation (EU) 2016/679

**Document Owner** – Ceri Charlton TRF Data Protection Executive

**TRF Marketing Director** – Mario Costa-Sa

**TRF Membership Director** – Carla McKenzie

This document is not intended to be a GDPR tutorial, nor provide advice or recommendation; it is information for TRF Groups to consider in their own activities.

## What is GDPR?

-The General Data Protection Regulation (GDPR) is a European Union regulation scheduled to go into effect on the 25th May 2018.

GDPR aims to standardise and strengthen data protection policies for residents of EU member nations. It replaces the prior Data Protection Directive (95/46/EC) of 1995 and will apply immediately on the enforcement date. This means that it applies immediately, in every Member State, from that date. The UK regulator, the Information Commissioner's Office (ICO) has stated that even following Brexit, equivalent legislation will be adopted throughout the UK.

The term "Personal Data" refers to any personal information you store. This includes Group Officers, members and anyone else who you hold information about. If you hold records of your members, such as their contact details and addresses – that's Personal Data. Minutes of meetings containing names of specific individuals, or information by which they can be identified by is all Personal Data and it all falls under the requirements of GDPR.

Ignoring the requirements of GDPR legislation risks a fine of up to £20 million or 4% of turnover – whichever is the greater. Such fines are calculated at a "Parent Organisation" level, so a failure to comply at a regional level group that lead to a breach resulting in a fine, would likely be calculated to be 4% of the TRF's national turnover. Aside from having a moral obligation to take all reasonable steps protect the Personal Data of our Members, we want to ensure as much of our funds are available to serve the interests of our members and keep green lanes open, hence the importance of this topic.

### **Who Does This Affect?**

**Everyone.**

GDPR applies to all organisations. There is a misconception that if organisations are small, or volunteer based or only have paper records, they are exempt. This is not true. No data controller or data processor is exempt.

You must be careful not to mistake **business conducted from home** for **household activity**. GDPR does not apply to people using personal data in the course of **exclusively** personal or household activity. For clarity: if you hold or use personal details in relation to any activities that form part of your activities on behalf of The Trail Riders Fellowship, then you must comply with GDPR legislation.

### **I'm A Group Officer. What Does This Mean For Me?**

The **Data Controller** (The Trail Riders Fellowship) is liable for what anyone processing the personal information it has collected does with that data.

Volunteers are **NOT** personally liable for any data breach or misuse **BUT** The Trail Riders Fellowship would be liable if a breach or misuse of data were to be caused by a volunteer. Therefore, it is imperative that TRF Group Officers / TRF volunteers follow the policies and procedures set out by the Fellowship. Appropriate information and support can be provided: If you're unclear what to do, or have concerns, just ask; we're here to help.

2

---

### **What Do I Need To Know?**

The data you hold belongs to the data subject (the person) and that data subject has the **absolute right** to say what happens to their information - and seek compensation if it is wrongly used or used without proper explicit consent.

GDPR applies to all personal data that you currently hold. It does not apply only to data collected after May 2018.

### **What Do I Need To Do?**

Here are some of the things you need to do immediately:

- Create a register of the personal information you hold, where it came from and who you share it with.



- Review the current **Privacy Notice** of any TRF Group website or TRF social media forum and ensure it is GDPR compliant.
- Decide and document the **Lawful Basis** your TRF Group has for holding and processing each individual piece of personal data.
- Get consent to store, manage, use and maintain personal data, where appropriate.
- Check that you can respond to a 'Subject Access Request' – where someone asks for a copy of their data. You **MUST** be able to provide this to them in a secure, standard format.
- If you are asked to remove data or consent, do it, and make sure you can prove that you've done so.
- Have a process and plan for dealing with data breaches – in case you lose data or someone steals it. Ensure that this includes notifying the TRF Directors.

Here are just two ways in which we could be financially and reputationally exposed:

1. Breaching the requirements of GDPR such that the Information Commissioner imposes a fine and terms. Fines are up to £20 million or 4% of gross turnover – whichever is greater.
2. That you are pursued by an individual data subject (Member, individual whose personal data your group hold, etc) because they allege you have used their data in a way which has no legal basis or which they have not consented to.

### **What Is The Trail Riders Fellowship Doing?**

The TRF Directorate is aware of GDPR and ensure that its policies, procedures and systems are compliant. Staff directly involved in the administration of Membership details (our main store of Personal Data, at a national level), our IT systems, etc. have given particular focus to align to the requirements of GDPR. The Directorate are conscious that whilst many of the requirements can be met centrally, regional Groups may have their own systems and local registers of their Members, hence the issuance of this guidance note as part of our readiness for GDPR as an organisation. There is also a Directorate member whose core focus is in this are, who can be contacted at: [dataprotection@trf.org.uk](mailto:dataprotection@trf.org.uk) if you have any specific questions or concerns regarding this legislation.

## **TRF GDPR POLICY**

A Proposed Privacy Notice [For use when onboarding new members]:

*The TRF only uses the information you provide about yourself for the purposes of administering your membership. This includes sending you Trail Magazine, membership materials and contacting you about TRF matters.*

*We will not resell your information to third parties, nor will we use it to market non-TRF services to you.*

A Proposed Privacy Notice [For use by regional groups in their own materials]:

*We use the information you provide about yourself for the purposes of [Insert Name of Regional Group]. This includes organising rides, events and group meetings.*

*We share information about our members with the (national) TRF as necessary.*

*We will not resell your information to third parties, nor will we use it to market non-TRF services to you.*

Additional Guidance notes to Directors/Regional Officer using the above:

There are a number of exceptions provided within GDPR which remove the need for an organisation to attain explicit consent. The nature of the formal relationship between our Members and the TRF removes some of the obligations which apply to customers of commercial organisations. This situation does not typically apply to individuals who are not members of the TRF, so do not presume this exception covers any details you hold of non-members, or if your group uses the information it holds for other purposes.

The above has been drafted to hopefully be broad enough to cover the most common activities in which the TRF would administer personal data. If you are collecting data to do something outside of the stipulated purposes, you will need to gain, formally document and retain additional consent (explicitly mentioning this other purpose) from each of the persons concerned. Where you think this additional consent may be necessary, check the guidelines at:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>



The ICO's office have said that notice such as these should be displayed prominently, at the time you collect the information. In practical terms, this means that they mustn't be buried deep in a website, but on the (printed) forms or (web) pages where you're collecting the Personal data.

If you are in any doubt, please seek advice at: [dataprotection@trf.org.uk](mailto:dataprotection@trf.org.uk).

## DEFINITIONS

### Data Controller

A **Data Controller** is a person or organisation who determines the purposes for which, and the manner in which, any personal data is processed.

**Example:** The Trail Riders Fellowship is a Data Controller because it holds information about individuals (primarily members). It uses this information to administer membership and provide the services offered by the Fellowship.

### Data Processor

A **Data Processor** is a person or organisation which carries out the act of processing data on behalf of the **Data Controller**.

**Example:** The Trail Riders Fellowship uses an external organisation to send out mailshots its members. This organisation is a Data Processor.

### Lawful Basis

Lawfulness, transparency, and fairness are the key ingredients to the first principle of data processing in the General Data Protection Regulation (GDPR). This means that you must have legitimate grounds for collecting and using personal data. Other than Consent, all other lawful bases for data processing require the processing to be **necessary**. This means that organisations should only be collecting and processing information for a specific purpose.

The GDPR legislation sets out 6 possible options for Lawful Basis. These are:

Consent	Legitimate Interest
Public Task	Legal Obligation
Contract	Vital Interest



No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

**Example:** The Trail Riders Fellowship sends Trail to its members. The lawful basis of this is **Contract**, because the member expects to receive the magazine as part of their membership benefit and could not receive it without his/her personal data (name, address) being used.

**Example:** The Trail Riders Fellowship sends details about its payments to HMRC. The lawful basis of this is **Legal Obligation**: it must do this to comply with tax laws.

**Example:** A local TRF Group may want to keep details about individuals who have attended a ride, with the intention of using some of the names and photographs taken on the day to promote other upcoming rides, or in its activities to encourage new Members. The lawful basis for this is **Consent**, because individuals present have been notified that the pictures are being used and consent obtained from them to use their information for specific this purpose.

### **Privacy Notice/Privacy Policy**

A privacy notice is externally facing (usually it is displayed on an organisation's website), telling members, regulators and other stakeholders what the organisation does with personal information & why.

<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/>

A privacy policy is a statement that discloses some or all of the ways an organisation gathers, uses, discloses, and manages personal information. A privacy policy is internally focused, telling employees what they may do with personal information.

*If you/your Group has not done so already, visit the ICO website (<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>) for further information and advice.*