

# GDPR: RI Frequently Asked Questions

## What you need to know about new data protection rules

The European Union's [General Data Protection Regulation](#) (GDPR) takes effect 25 May. Because Rotary staff members process the personal data of our European members, Rotaractors, program participants, and others, we're obligated to comply with this new data privacy law.

We know you trust Rotary to respect your privacy and protect your information, and we take this responsibility seriously. That's why we're using this opportunity to reinforce our data privacy and security methods for anyone who shares personal information with Rotary — no matter where they live.

Here is what you need to know about GDPR.

## What is the General Data Protection Regulation?

GDPR is a new European Union law that strengthens data protection rules for EU residents. The law applies to all companies that process data within the EU but also to foreign organisations, like Rotary International, that offer goods and services to EU residents. The law takes effect 25th May 2018 and replaces the EU's 1995 Data Protection Directive.

## What does Rotary International do to protect personal data?

Long before GDPR, Rotary's policies took care to protect your information. Rotary's Website Privacy Policy explains what information we collect, how we collect it, and how we use it. We also strive to give you control over your data so you can decide what personal information to share and review it whenever you want.

The measures we take to safeguard your personal data include using password-protected databases on secure servers behind firewalls and requiring all staff to attend information security awareness training each year.

## How has Rotary International prepared for GDPR?

First, we completed a readiness assessment and risk analysis. These helped us understand how the new regulation will affect our processes and what we need to change to comply with GDPR. Our analysis led us to focus on the following areas:

- **Process inventory.** We inventoried all of our personal data processing activities in order to comply with GDPR's Article 30.
- **Lawful basis.** We reviewed all data processing to ensure that we have a documented legal basis, or reason, for every process, according to GDPR.
- **Policy and notices.** We're updating our Website Privacy Policy to meet GDPR expectations. And we're making our notices about how your personal data is used more specific.
- **Records management.** We updated our schedules for retaining records that contain personal data to make sure we're keeping records only as long as necessary.
- **Data breach procedures.** We revised our guidelines for responding to a breach in accordance with GDPR expectations for notifying constituents of a breach.

## What does GDPR mean for me?

Rotary is applying these new standards globally, not just for our European constituents. So no matter where you live, if Rotary processes your personal data, you will have the following rights:

- **Right to be informed:** Rotary will regularly disclose to you what personal data we collect and for what purpose.
- **Right to object:** You can tell us if you no longer want your personal data to be processed in a certain way, such as for direct marketing.
- **Right to rectification:** You can write us at [data@rotary.org](mailto:data@rotary.org) to correct errors in your personal data.

## Do I need to give Rotary International consent to use my personal data?

In general, no. Under GDPR, consent is just one of six legal bases used to determine that processing someone's data is lawful. Rotary will generally rely on "legitimate interest" as the lawful basis for processing personal data, because doing so is necessary to effectively manage and operate Rotary and won't unduly infringe your legal rights. We will ask for your consent only when it's truly appropriate, for example, when we are processing special categories of personal data, like health information.

## My club or district is in the EU. Do I need to do anything?

Yes. If your club or district is in the EU and is processing the personal data of your members or other program participants, you are obligated to follow GDPR requirements. This may mean:

- Providing notice to your members about how their personal data is used
- Minimising the personal data that you have and keeping it secure
- Getting consent when it's appropriate (for example, for personal data of youths under the age of 16)

Further information can be found at [EUGDPR.org](http://EUGDPR.org) or on one of the many EU country data protection authorities' websites. You may also want to consult with local privacy experts to better understand your responsibilities under the law.

## I'm not in the EU. Do I need to do anything?

Possibly. Even if your club or district is not in the EU, you are required to follow GDPR rules if you process the personal data of EU residents. You may also need to comply with GDPR if you welcome European attendees at events, host exchange students from Europe, or partner with European members on service projects.

## What is Rotary doing to help clubs and districts with GDPR?

Before the law takes effect, we have updated Rotary's Website [Privacy Policy](#) with terms that align with GDPR. We will hold a [breakout session](#) at the Rotary International Convention in Toronto, where participants can learn more about our compliance efforts. It's *Data Privacy and Data Protection: Rotary's Compliance with GDPR* on 27 June, 13:00-14:00. And you can write us at [privacy@rotary.org](mailto:privacy@rotary.org) with any questions.

**Date: 24<sup>th</sup> May 2018**