PROTECTING PERSONAL DATA

Rotary

Protecting Personal Data

Course Description

Learn how to identify and protect the personal data of Rotary participants. The course will review why data privacy is important; the definition of personal data, and the different levels of data sensitivity; and how to protect personal data at any level of the organization.

Content

Introduction to Data Privacy

Rotary connects you to more than a million other Rotary members and program participants — whether in your club or halfway around the world. Those connections may mean that you've looked up a fellow club member's phone number to discuss a club board decision, sent an email to people attending a district training meeting, or managed the funds and accounts for a grant project to improve a community in another country.

In these situations and many more, you might access or use someone's personal data to conduct Rotary business. Handling that data responsibly is vitally important to maintaining the privacy and security of your fellow Rotary participants.

Why is data privacy important?

Data privacy refers to the ways that data is used and how it should be handled according to the type of information it is. New laws and regulations are being implemented around the world to help protect personal data. Rotary International and The Rotary Foundation have an obligation to comply with these laws and regulations. Our commitment to protecting personal data helps Rotary participants feel secure in supporting our organization through their membership, donations, and participation in programs and grants.

Because so much of the Rotary experience takes place at the local level, we also rely on club and district leaders to protect the personal data of all Rotary participants. To promote a culture of data privacy, clubs and districts should adopt their own privacy policies and train anyone who collects or uses personal data to follow those policies. In addition, clubs and districts are obligated to comply with local laws and regulations about handling personal data.

So what is personal data, and how do you protect it?

Understanding Personal Data

What is personal data?

Personal data is any information that can identify a specific individual, either by itself or when it's combined with other information.

A large amount of information can be considered personal data, including people's names, dates of birth, and gender; their contact information, names of family members, and marital status; employment information; government identification numbers and bank account numbers; photographs that identify them; and much more.

When might I encounter personal data?

In conducting Rotary business, you may encounter personal data in many ways, such as by:

- Accessing a list of Rotarians' names and classifications on a club website or in a club directory
- Taking payment details, such as bank or credit card information, from someone registering for your event or conference
- Adding new members of your club and their email addresses to My Rotary
- Handling travel documents or immunization records for a Youth Exchange student
- Reviewing the details of contributions from donors in your district in a My Rotary report
- Collecting the names of the partners of people attending a district training event
- Supplying the phone numbers of vocational training team members on a grant application
- Using photos of project beneficiaries in a grant report or People of Action ad

How do I determine the sensitivity of personal data?

You or someone in your club or district may need others' personal data in order to plan events, service projects, or fundraisers. But not all personal data is equally sensitive. Depending on the type of information, losing or otherwise mishandling it can have a range of negative effects both on the person and on Rotary. The more sensitive the data, the greater the need for protection.

To help you determine the level of protection that personal data may need, Rotary International has categorized some common examples into three levels of sensitivity: high, medium, and low. Click on each tab below to review the types of personal data that are in each category.

High Sensitivity

Personal data that is considered highly sensitive requires the most care and protection. This includes:

Government identification numbers, such as from a passport or driver's license

Bank account details

Credit or debit card numbers

Personal data about a child under age 16

Health, medical, biometric, or genetic information

Race or ethnicity

Political opinions

Religious beliefs

Trade union membership status

Sex life or sexual orientation

Medium Sensitivity

These types of personal data are less sensitive, but they still require reasonable and thoughtful protection. Personal data of medium sensitivity includes a person's name **in conjunction** with any of the following:

Home address

Phone number

Email address

Gender or sex

Marital status

Spouse's or partner's name

Parents' names

Occupation

Employer

Date of birth

Foundation giving history

Wealth data

Low Sensitivity

This information is most likely already public, so it would probably have little to no adverse effect on Rotary or the person if it was mishandled. This includes:

Name (first, last, or both)
Website

Depending on your role in Rotary, you may have access to reports that include contact information or donation history. Typically, the reports that Rotary International provides include personal data of only medium or low sensitivity. But locally — for example, for a RYLA event that includes children under age 16 — you may need to collect highly sensitive data. For this reason, it is important to be aware of the different levels of sensitivity and think about how the data you handle can affect Rotary participants.

Check your understanding

Now that you've reviewed the sensitivity levels of personal data, test your knowledge by dragging the following examples of personal data into the correct levels.

A) High sensitivity | B) Medium sensitivity | C) Low sensitivity

1) Rotary club roster with members' names and addresses
2) List of a district training event's participants and their partners
3) List of event participants' names and email addresses
4) Health information about a member of a vocational training team
5) Payment form that includes a person's bank account number
6) List of a Rotary Club's members and their classifications
7) Passport number of someone traveling for a Rotary grant
8) Photo of a 15-year-old student taking part in Rotary Youth Exchange
9) Full name of a member
10) List of Rotarians' websites

Answer:

(1) B   (2) B   (3) B   (4) A   (5) A

(6) B   (7) A   (8) A   (9) C   (10) C

Protection at Every Stage

Protecting personal data includes making informed decisions about **collecting, accessing, sharing, storing, transporting,** and even **disposing of** that data.

The first step is to determine why you need the data. If you don't need it, don't collect or keep it. If you do need to collect it, you must protect it — and when you no longer need it, you must securely dispose of it.

Why am I collecting this data?

You may collect personal data on Rotary International's behalf for core business purposes — that is, for reasons that are necessary to our essential activities.

These purposes could include:
- Supporting The Rotary Foundation, including fundraising efforts
- Facilitating convention and event planning
- Communicating key organizational messages
- Supporting the programs and members of Rotary
- Fulfilling Rotary's obligations to Rotarians and other individuals

If you are collecting personal data locally for other reasons, limit yourself to collecting what is adequate for and relevant to your business purpose. Always tell people why their data is being collected, how it will be used, and whether providing it is voluntary.

In some cases, obtaining explicit consent to collect personal data is necessary.

Explicit consent is a freely given, specific, and informed agreement through which someone actively chooses to provide personal data.

Get explicit consent if you collect:
- ☐ Personal data about a child under age 16 (get consent from a parent or guardian)
- ☐ Health, medical, biometric, or genetic information

☐ Information about a person's race or ethnicity
☐ Political opinions or religious beliefs
☐ Trade union membership status
☐ Sex life or sexual orientation

ⓘ If the personal data you need isn't on this list, you probably don't need explicit consent to collect it.

I've collected the data. Now how do I protect it?

Collecting only the personal data for which you have a clear business need is just the first step. You must protect the data at every stage: each time you **access** or **share** it and each time you determine how to **store** or **transport** it. Your security measures should match the level of the data's sensitivity.

Expand each category below by clicking the "+" to read about the best practices for protecting personal data.

Accessing

You should access personal data only when you need to do so, either to fulfill your duties or for a legitimate business purpose. For example, if you aren't involved in a student's Youth Exchange experience, you shouldn't access any of their personal data.

Sharing

Don't disclose personal data for any reason that's not related to the purpose for which it was shared with you. For example, don't share the email addresses of your club members with a speaker who wants to advertise their business.

Storing

Personal data should be stored in the way that best secures it. Be sure that you have policies for various methods. That may mean storing paper records with highly sensitive data in a locked drawer and protecting electronic files with passwords.

Transporting

Personal data should not be transported, in either paper or electronic format, unless it is secured in a manner consistent with its sensitivity. Don't enter highly sensitive personal data into instant messaging apps or email credit card or bank account numbers without encrypting them or taking other security measures.

What should I do if there is a security breach?

Data privacy policies and procedures are designed to protect personal data from accidental loss or disclosure. A data security breach happens when there is any unauthorized access to or disclosure of personal data held by Rotary or its participants. Breaches can include unauthorized sharing with a third party (by accident or by design), an attack on a computer network that results in exposed data, and more.

If Rotary International or The Rotary Foundation has shared personal data with you, and you suspect or discover a breach, immediately:

❶   Write to privacy@rotary.org.

❷   Write to your Rotary staff contact.

Take a few moments to think about what procedures your club or district can put in place to help prevent a breach, and what steps you will take locally if a breach occurs.

What if I don't need the data anymore?

Personal data should be kept only as long as it is needed to fulfill the specific purposes for which it was collected. One part of protecting data is safely and securely disposing of it when it is no longer needed — and doing so with the proper level of protection for its level of sensitivity.

See below for some recommended ways to dispose of personal data that you no longer need.

Shred paper records that contain personal data

Permanently delete email records with personal data

Delete personal data from all your electronic devices

Your club or district should have policies and procedures for securely disposing of any data you collect locally.

Proceed to the next lesson to review best practices and find suggestions about developing your own policies to protect personal data.

Principles and Responsibilities

Personal data is a valuable asset that's worthy of protection, and Rotary International and The Rotary Foundation have policies and procedures to ensure the security of the data we collect. We also rely on club and district leaders to protect that data responsibly and comply with privacy laws and regulations.

At the club and district level, consider data privacy as you plan events, projects, and programs. Review any local laws and regulations that apply to the handling of personal data. Look at your current practices and discuss with your club or district the steps you'll take to protect the data of your fellow Rotary participants. As you develop or update your policies, keep the following principles in mind:

- ☐ Collect and use personal data only for specific business purposes.
- ☐ Collect only the most necessary, relevant personal data.
- ☐ Be clear about how you'll use the personal data you collect.
- ☐ Securely dispose of personal data when it is no longer needed.

What are my next steps?

If you're in a leadership role, review Rotary International's Personal Data Use Policy by following the link to the right. The policy provides more information on the key guidelines in this course and details how personal data provided by RI will be handled.

Personal data use … https://my.rotary.org/en/personal-data-use-policy