Rotary - GDPR Preparation Checklist

This 12-point checklist is designed to assist Rotary clubs and districts in preparing themselves for GDPR. The checklist can be cross referenced to the **infographic chart** produced by the FSB (Federation of Small Businesses) and available on the Rotary GDPR webpages as a resource guide. Additional information on Rotary and GDPR, including some of the steps outlined below, can be found on the Rotary website **here**. Further information can be found on the Information Commissioners Office website **here**.

1. Audit time

Do an internal audit to determine what data the club/district has, how you use it and where the data goes. The club/district should be clear in their audit documentation to record not only the individual officers or members that collect, access or process data but also any third parties that they share data with, such as hotels when organising events.

2. Get aware

Familiarise yourself and your club/district members on GPDR and how it will impact on the club/district. Issue a communication to all members of the club/district to lay out expectations (there will be a sample communication under GDPR Resources on the website).

3. Record it

Make sure all your data security, handling and processing arrangements are set out in written policies or procedures, i.e. for any Rotary activity that includes the collection of personal data. Be sure to update regularly. Club/District Secretaries should keep GDPR documentation in one place and hand them over to your successor.

4. Delete it

Clubs/Districts should make sure that they safely and securely delete any data they don't need or use. They have a responsibility to also ensure that individual club members/district officers also safely and securely delete any data they hold as per the Rotary, club and/or district policies and confirm this to the Club/District Secretary.

5. Keep it under lock and key

Make sure any systems used by clubs and districts store personal data properly and securely. Seek the guidance of the Club/District Information Technology Officers.

6. Give me access

Clubs/Districts should prepare a plan or policy for handling 'subject access requests' to make sure you are ready if someone asks to see their personal data that you hold. Test your system.

7. Secure it

Clubs/District should prepare a security framework for how the club/district will handle personal data and what is expected of individual members. See the RIBI website for information on security tips applicable to all members. Clubs/Districts should also prepare a plan that outlines what to do in a breach – remember under certain circumstances, you may need to notify the ICO within 72 hours. Your security plans should be issues to all members.

8. Policy review

During the course of Rotary activities, clubs/districts work with, or engage the services of, outside organisations/suppliers. Clubs/Districts should review and amend the existing privacy policies they have for working with these organisations/suppliers. Ensure any new contracts are GDPR compliant and include appropriate privacy policies.

9. Consent review

Clubs/Districts should review how they obtain, record and manage occasions when consent is required to collect and process personal data and whether any changes need to be made. Whilst Rotary collects personal data for members via the DMS/RIBI Template database and My Rotary under Legitimate Interests for processing membership services, if clubs/districts collect personal data outside of these areas they need to do so on the basis of Consent, i.e. when organising a club trip, and must have policies and procedures in place with explicit privacy notices. Consent must always be obtained for data collected and processed in respect of partners or non-members.

10. Choose a lead

Clubs should identify someone to take responsibility for data protection compliance. This is most likely to be the Club Secretary, however, consider if there is someone more appropriate within the club to take on this role, i.e. someone who has current and relevant experience in GDPR through their work role. Districts have already appointed District Data Protection Officers as of the 2018/19 Rotary year.

11. Age matters

Review your policies and procedures for Rotary activities involving children/youths. Clubs/Districts must follow the ICO guidance for working with children, together with the guidance in appropriate Rotary manuals, i.e. youth competition manuals. Clubs/Districts must make sure they put systems in place to verify individuals' ages and obtain parental or guardian consent when needed. Privacy statements must be in an age appropriate language.

12. Cross-border processing

Clubs/Districts should check if they have any third party service providers who may be hosting personal data on behalf of the Club/District outside of the European Union, i.e. a district using a third party software company to host their online conference registration process and that company's hosting environment is outside of the EU. If so, take steps to ensure that contracts are in place and GDPR compliant in respect of the transfer of personal data abroad. Service level agreements are in place between RIBI and RI for data shared via My Rotary and the DMS/RIBI Template which is GDPR compliant.