# GDPR Policy – Appendix B

# Background

The General Data Protection Regulation (GDPR) came into force on 24th May 2016 and becomes enforceable on 25th May 2018, which means the Information Commissioner's Office (ICO) can take enforcement action against non-compliance. In many ways the GDPR just builds on the Data Protection Act 1998 (DPA) taking previous guidelines and recommendations and making them rules that must be followed.

## What is included

As with the DPA, GDPR covers all records - including paper records - which are kept in such a way that information about a living individual is readily identifiable.

## Definitions

Personal Data - The GDPR has a wide definition of personal information but for RSCM area committees' personal information will be individual names, address, contact telephone numbers and emails. Committees should not be collecting any other types of personal information.

Sensitive Personal Data - The definition of sensitive personal information in the GDPR includes medical, mental health and philosophical belief which includes religion. There are no reasons for an area committee to collect medical or mental health information. For an event you can ask if anyone needs assistance or adjustments but there is no need to ask for the underlying medical condition.

Most RSCM data on individuals includes the church of which they are a member. This makes it 'sensitive personal data' and the individual's explicit consent must be obtained to holding and processing the information.

Processing Data - The definition of what is data processing has expanded so significantly that it is easier to describe what is not data processing. Thinking or dreaming about personal information is not data processing but everything else to do with personal information is!

## GDPR Principles

The GDPR is based around six principles:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## GDPR requirements and how to comply

RSCM has taken these principles and produced guidance and examples of how area committees can comply with the GDPR and these are covered individually below.

### Collection

Collect the minimum information necessary to fulfil the objectives of the area activity or event, do not collect information "just in case"

For example:

> Do not collect an individual's address unless you intend to write to them or you need to confirm their residence.
>
> If you already hold an individual's address in your records do not collect the information again on a further event booking form .
>
> Only collect one contact telephone number preferably their mobile number.
>
> Do not collect emergency contact information on registration form information for a one-day event. If you feel it is an absolute necessity, collect a contact number on the day of the event and destroy afterwards. ***(Please refer to specific safeguarding advice in addition to this guidance)****

### Transparency

Be transparent in how you will use people's information. If you have a website, make sure there is a privacy notice and it is displayed prominently especially on any page where you collect information. If you do not have a website send out a privacy notice to all your members once a year and to any new members.

Be transparent how you have obtained personal information. For example:

> *An existing member would like a friend to come to future events and provides their contact details. Contact the individual and let them know how they have obtained their information and confirm they are happy to be contacted about events. If the individual does not reply after several attempts do not continue to contact them and do not retain the contact details.*

Or

> *A non-affiliated church has contact details of lay readers on their website. An area committee wants to contact the church to promote local events. An area committee member can contact the individual, but they must explain where they obtained the contact information.*

### Processing

Only use the personal information you have for your area events and activities and the charitable objectives. For example

> *One area committee regularly uses a local hall for their events, the hall is hosting a charitable exhibition and asks the committee to email all their contacts and invite them to the exhibition.*

The area committee cannot share the data and cannot email on behalf of a third-party as this is not the reason the local members' information was collected. However, the area committee could post a link on their website advertising the charitable exhibition.

You should also be careful about sharing personal information even with other area committees. For example:

*Area Committee A is organizing an event in its area and want to invite members of Area B and Area C and asks for a list of contacts details for members from Area B and C.*

The Area B and Area C cannot share their members details as they do not have the individuals' consent. They can, on behalf of Area A, email all their members with details of the event and invite them to contact Area A direct.

## Storing

You must store personal information securely; paper forms should preferably be stored in a cabinet with a lock and if you store records electronically on a computer or laptop, the computer must be configured to receive regular updates and have an up to date antivirus software installed. Where you store over 1000 personal records electronically on a laptop or tablet device the ICO will expect you to use encryption software.

If you collect and store personal information through a website it must have up to date security and be tested.

## Deleting

You should not retain information longer that it is needed for the original purpose. For example:

*An area committee holds an event which is attended by both members and non-members who pay £10 each. Everyone who attended was required to complete an application form containing their own information, emergency contact information and parental consent. After the event the committee keeps all paper work in a box in the attic.*

Once the event was completed there is no lawful reason to retain the information. They should keep a list of who staff and attendees and how much they paid for accounting purposes, but all other records should be destroyed. ***(Please refer to specific safeguarding advice in addition to this guidance)****

You should review the personal information you hold on an annual basis to confirm they are still an active participant. If they have not attended an event or corresponded with you for two years you should stop all communication and then delete them from your records.

Electronic records can simply be deleted from any system and paper records should be shredded or burned.

## Individual Rights

The GDPR provides individuals with extensive rights with regards to the processing of their information and their privacy and organization only have one calendar month to reply to their requests. Individuals can request:

To know what information an organization holds about them and be provided with a copy of that information.

That information is deleted or rectified

That organization stop processing their information.

You can see that the more information you hold the more challenging this can be and therefore it is important not to keep information unnecessarily.

Should someone ask you to update their details such as email address or phone number, just go ahead and comply.

Should someone ask you to delete their information or stop emailing them, just go ahead and comply but let the Data Protection Officer know.

Should someone ask you what information you process or hold on them, contact the Data Protection Officer immediately.

## Safeguarding

Data Protection compliance within Safeguarding will be addressed in separate guidance from the RSCM Safeguarding Officer (e.g. Parental Consent forms, booking information for under 18s etc)*

## Registration

The RSCM is registered with the ICO and this registration covers the area committees. The RSCM will produce guidance and assistance to ensure you comply with the GDPR. **There is no need to register separately**, as you are operating as a not-for-profit members organization within the RSCM. However, it is important you operate within the RSCM guidance as you could be deemed to be a data controller in your own right with all the possible consequences.

## Minutes and Reports of Meetings

It is good practice for the Chair to approve the Secretary's minutes before they are sent to Area Committee members. The minutes should remain confidential to the members of the Area Committee and not be sent out to others. It is important that minutes are sent to the RSCM Office (voluntary@rscm.com) and to the Regional Co-ordinator, Voluntary Forum Representative and committee members as soon as possible after the meeting, with action points listed, so that these may be followed up before the next meeting. The minutes should be formally accepted at the next Area Committee meeting.

Due confidentiality needs to be observed in the sending of personal letters or electronic communications which refer to the content of meetings, discussions or individual consultations with RSCM staff or volunteers.