GDPR: A brief guide to the law and congregational resources

What is happening and why is it important?

The General Data Protection Regulation (GDPR) takes effect in the UK on 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protections with regard to how their personal data is used by organisations. Congregations must comply with its requirements, as there are no relevant exemptions for charities or small organisations. This is a brief guide highlighting the main things you need to know and the points that you will need to action.

Underlying Principles

The GDPR sets out a list of data protection principles. They are that **personal data must be**:

1. processed **lawfully, fairly and transparently**;

2. only used for a specific processing **purpose** that the data subject has been made aware of;

3. adequate, relevant and **not excessive**;

4. **accurate** and where necessary kept up to date;

5. not stored for longer than is necessary i.e. **storage limitation**;

6. stored in a safe and **secure** manner.

Key definitions

Personal data is information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held.
Processing is anything done with/to personal data, including storing it.
The **data subject** is the person about whom personal data is processed.
The **data controller** is the person or organisation who determines the manner and purposes of data processing.

There is also a new '**accountability**' principle which provides that the data controller must be able to **demonstrate compliance** with the first 6 principles.

Key Points for Congregations

1. There are several **legal bases** for processing data. The main one which will be relevant for congregations is **legitimate interest**. This allows for processing of information for general church management including dealing with membership lists and rotas, etc. Other legal bases include: legal obligation (such as processing Gift Aid); contract (e.g letting out the church hall); or consent (this will generally only be required if personal data is being shared with a third party e.g. by uploading it to a website, publishing it in a magazine or posting in on a noticeboard in a public place). For each processing activity, you will need to be clear about the legal basis for doing so.

2. If you are obtaining **consent** for the data processing described above, this will need to be clear and unambiguous with some form of positive action to 'opt-in'. You must ensure that you have this consent before any processing begins.

3. Where the data reveals religious belief it becomes "special category data" which requires additional care. Processing is prohibited unless one of the listed exemptions applies. Two of these exemptions will be especially relevant and useful for congregations: (i) the individual has given **explicit consent** to the processing of the personal data for one or more specified purposes; or (ii) processing is carried out in the course of its **legitimate activities** with **appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing **relates solely to**

the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is **not disclosed outside that body** without the consent of the data subjects.

4. Data subjects have a number of **rights**, including that of knowing how data is used by the data controller, of knowing what data is held about them, of correcting any errors and generally the right 'to be forgotten' (although this is not an absolute right).

5. The GDPR introduces a requirement of **accountability** for **data controllers**. This means that you must be able to show that you are complying with the principles by providing evidence. See the action points below.

6. Whilst the GDPR removes the requirement for data controllers to register with the Information Commissioner's Office (ICO), there will be an annual data protection fee. The good news is that Presbytery Clerks will continue to register for all congregations within their bounds.

Action Points

1. Carry out a **data audit [Link to data audit form**]to review what data you are holding, how you store it, and what basis you have for processing it. Review any historical records held (in electronic or manual form) and archive any records that you are obliged to keep. Consider deleting or destroying any records that are no longer required but take care over how you dispose of these.

2. **Appoint an individual** who has responsibility for information management within the congregation. This person should have formal responsibility for data protection issues and should keep data protection matters on everyone's radar.

3. **Training** is crucial. Ensure that all current (and any new) office bearers and any members of the congregation who handle personal information watch the data protection **GDPR training webinar [link to webinar]**. Keep records of those who have had training.

4. Implement the new **data protection policy [Link] and data retention policy [link]**. Make sure that they are appropriately communicated e.g. discussed with everyone who is handling personal information, printed and placed on the church notice boards, referred to in the intimation sheet, uploaded to the church website.

5. Issue a **Privacy Notice [Link]**. Again, make sure that this is appropriately communicated e.g. printed and placed on the church notice boards, referred to in the intimation sheet, uploaded to the church website.

6. Complete a **Legitimate Interests Assessment Form [Link]** to decide the legal basis of processing. Only obtain consent where this is needed.

7. Review how you store information to ensure security and consider whether the protections in place are adequate**. [Link to information storage hints and tips**]

8. Ensure that those handling personal information are aware of the **Presbytery security breach management procedure**. [Link].

9. Read the full note providing GDPR General Guidance for Congregations **[link].**