A Brief Guide to General Data Protection Regulations GDPR for Presbyteries and Congregations

What's happening and why is it important?

The General Data Protection Regulation (GDPR) will take effect in the UK in May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. The good news is that if you were complying with the previous Data Protection Act you will already be doing much of what is required under the new legislation. Congregations, Presbyteries and The Presbyterian Church in Ireland – all separate charities in their own right - must comply with its requirements, just like any other charity or organisation. This guide tells you what you need to do.

Background to GDPR

We've evolved in the way we generate, store, access and use data. The types of data that are held by many organisations on individuals has also significantly changed and can include genetic and biometric data as well as image and sound. With the emergence of new technologies it has also become much easier to identify individuals from elements of personal data. It is therefore only reasonable and natural that guidance and protections will need to be reviewed and revised on a regular basis to ensure that individuals can be assured that their personal data is secure, accurate and not misused. The GDPR is EU generated legislation but will be implemented in the UK and the Republic of Ireland and there is no indication that it will cease to apply as a consequence of BREXIT.

The GDPR replaces the Data Protection Act and affects all organisations who process or store personal information. It's focused on looking after the privacy and rights of the individual, and based on the premise that consumers and data subjects should have knowledge of what data is held about them, how it is held, and how it is used.

Underlying Principles

The law is complex, but there are a number of underlying principles, including that **personal data**:

- will be processed lawfully, fairly and transparently.
- is only used for a specific **processing** purpose that the data subject has been made aware of and no other, without further consent.
- collected on a **data subject** should be "adequate, relevant and limited." i.e. only the minimum amount of data should be kept for specific processing.
- must be "accurate and where necessary kept up to date"
- should not be stored for longer than is necessary, and that storage is safe and secure.

Key terms

Personal data is information about a living individual which is capable of identifying that individual.

Processing is anything done with/to personal data, including storing it.

The **Data Subject** is the person whose personal data is processed.

The **Data Controller** is the person or organisation that determines the how and what of data processing.

Legitimate Basis for Processing, Consent, Rights and Accountability

- There must exist a legitimate basis for processing data. A long list of these has been published by the Information Commissioner's Office on their website, (see Further Help at the end of this paper), but the main ones likely to apply to PCI are:
    - 6(1)(f) – Necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

  Coupled with, (where sensitive 'special category' data is involved - and remember that religious belief is a special category),
    - 9(2)(d) – Processing carried out by a not-for-profit body with a ….. religious aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

  6(1)(f) coupled with 9(2)(d) is the main legal basis on which we are likely to rely since any data we collect will, for the most part, be in respect of members of our congregation and will be used within our congregation and not disclosed to a third party. There are situations however where we will have to share data with a third party or there is another legitimate basis for processing personal data:
    - 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
    - 6(1)(a) – Consent of the data subject
    - 6(1)(b) – Processing is necessary for the performance of a contract
    - 6(1)(c) – Processing is necessary for compliance with a legal obligation
    - 6(1)(d) – Processing is necessary to protect the vital interests of the data subject or another person
- Consent should not be considered where another basis is available, as it generally harder to obtain and can be withdrawn at any time. Where you are relying on consent this will need to be clear, informed, and unambiguous. You may need to gather this consent if you do not already have it or re-obtain it if your previous evidence of consent doesn't meet these higher GDPR standards.
- 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 the right to deletion or, 'to be forgotten', as it has been called. Presbyteries and Congregations will need to make provision for people to exercise these rights, including developing a Privacy Notice.
- The GDPR introduces a stronger requirement on accountability for data controllers. This means that you must be able to show that you are complying with the principles by providing evidence. What is this evidence? – if you follow the advice under the key actions section following you should be in a good position to demonstrate accountability and good governance.

Key Actions and Support

A number of regional training events have been organised for Presbyteries and Congregations and these will commence in March.

1. The first important action will be to undertake an audit of the Personal Data you currently hold and to record this and a number of important facts about this in a Data Inventory Register (DIR) (guidance and template has been circulated and will in due course also be available through the PCI website)
2. The DIR will lead to development of an action plan to be implemented by each Presbytery and Congregation. Each action plan will be different according to how you are currently organised to comply with Data Protection.
3. It is strongly recommended that you allocate the role of Data Protection Lead to someone within your Presbytery or Congregation so that they can assist with 1 and 2 above and help to coordinate your response to GDPR now and in the future (a suggested role description has been circulated and will also be available through the PCI website in due course)
4. It will be necessary to demonstrate good governance and this is achieved by developing policies and procedures, tailored to your own circumstances and approved by Kirk Session, for:
    a. Data Protection Policy (including security) (guidance and template pending)
    b. Privacy Notice (guidance and template pending)
    c. Obtaining Consent (guidance and template pending)
    d. Data Access Request (guidance and template pending)
    e. Data Retention and Disposal (guidance and template pending)
    f. Reporting a Data Breach (guidance and template pending)

Is it necessary to register with the Supervisory Authority?

Yes, unless you can be sure that you meet the exempt conditions for not-for-profit organisations referenced as 9(2)(d) under legitimate bases above. Bear in mind that the majority of churches will almost certainly be engaging in pastoral care to non-members as well as to members and this would require registration as would the use of CCTV. As the ICO Annual Fee for churches is only £40 (£35 if you pay by Direct Debit) (or €35 if you are based in ROI) you should register if you think you may be processing information which falls outside this exemption.

Both jurisdictions, United Kingdom and Republic of Ireland, do however generally recognise 'organisations that are not established or conducted for profit and that are processing data related only to their members and supporters and their activities' as exempt.

There is a Registration Self-Assessment tool on the Information Commissioner Office (ICO) website for those organisations designating the UK Commissioner as the Lead Authority. Please also note that if you use CCTV then you will need to register. If in doubt seek advice from the Commissioner's Office. For those designating the Data Protection Commissioner in RoI as Lead Authority again there is guidance on that website regarding registration and exemption from registration.

Please note that legislation is currently working its way through Parliament which will replace the requirement to register with ICO with a "data protection fee". The fee for all churches is

currently proposed to remain the same as it is currently and there will be no effect on existing registrations (i.e. you do not have to pay the new fee until the existing registration has expired). If you are required to register and you do not you will be breaking the law and risk having to pay a fine (currently the maximum fine is £4,350 for this offence).

What about our Suppliers or Data Processors?

Suppliers or third party data processors e.g. payroll management, cloud storage etc. will also need to meet GDPR standards as they are processing data that you hold as the Data Controller. You will need assurance from any organisation processing data on your behalf that they have in place all necessary policies and procedures to ensure GDPR compliance. Where possible PCI will seek this from the main suppliers of this this type of service to Presbyteries and Congregations. You may however in some situations need to obtain this contractual assurance yourself and we will provide a template that you may wish to use for this purpose.

Further help available ……

- The Information Commissioner's Website: https://ico.org.uk/
- The Office of the Data Protection Commissioner: performs the same function in the Republic of Ireland - https://www.dataprotection.ie/docs/GDPR/1623.htm

[Some aspects of GDPR have yet to be finalised - this guide may be modified and added to over time]

Issued: 9 April 2018