The Gift of Knowledge

Introduction

New EU Data Protection legislation came into force on 25 May 2018. The General Data Protection Regulation (GDPR) strengthened the existing Data Protection Acts in the UK and RoI, particularly in the areas of accountability and giving individuals more rights in controlling what you can do with their information. Losing people's data, or not securing it properly, could lead to a 'breach' and might result in fines from the Information Commissioner's Office (UK) or Data Protection Commissioner (RoI). ***Every Methodist circuit and department needs to have a written data protection policy that makes sense to the people who are using it and can be implemented without delay.***

This booklet contains the notes from 'The Gift of Knowledge' Data Protection seminar as presented in the Spring of 2018. It gives an introduction to the theme of Data Protection including our current responsibilities, and then provides information on changes required due to the General Data Protection Regulation. Updates and further resources are available on the Methodist Church in Ireland website: http://bit.ly/DPresources

What *is* data protection?

Put simply, data protection is:

CAREFULLY USING AND LOOKING AFTER OTHER PEOPLE'S INFORMATION

You might have a savings account where you lodge birthday and Christmas cash gifts. The bank or building society looks after those gifts and puts them to work, using them for a variety of projects that provide a return to you in due course.

In the same way, when someone entrusts us with the gift of knowledge – details about where they live, how to get in touch with them, what they do with their income, and perhaps more sensitive information about their health, beliefs or background – they expect that we will look after that gift of knowledge and put it to work: most often in providing pastoral care to them and communicating about their local church, but sometimes in other ways that mightn't immediately appear obvious.

The key, as with the spiritual gift of knowledge, is to be accurate and to know when and how to share it in an appropriate manner. The emphasis is on ***taking care*** of information, remembering that this gift doesn't belong to you but to the person who has entrusted it to you. If in any doubt, follow this simple rule: **THINK PRIVACY**.

Before using someone else's information: THINK PRIVACY. Before sharing their details with other people: THINK PRIVACY. Before leaving their information vulnerable to loss or misadventure: THINK PRIVACY.

In a sense, if you can keep that 'THINK PRIVACY' message in your mind, and impress the 'THINK PRIVACY' message upon the other people in your church, circuit or department who have access to personal information, then we're well on the way. If we are all attempting to do our best with regard to the safekeeping and wise use of personal data, using a little common sense, then it's quite unlikely that anyone will fall foul of the law.

Of course, there's more to it than that, but be encouraged for taking data protection seriously. Yes, there are definitions to discover, regulations to respect, and policies to prepare. To stretch the alliteration a little bit, there are also hefty fines to affoid ☺

But through it all, just...

Come back to this page if you begin to feel overwhelmed!

What was covered by previous data protection legislation?

Before exploring the new legislation, here's a reminder of why and how previous rules already applied to you:

The **DATA PROTECTION ACT** applies to	• 1998 (UK) or 1988 as amended 2003 (RoI)
DATA CONTROLLERS who instruct	• Whoever determines how and why data is used - usually the organisation, including staff and volunteers... unless otherwise stated, we presume Circuit Executives are held responsible for setting the data protection policy and ensuring staff, volunteers & data processors are aware of their responsibilities
DATA PROCESSORS, both of whom	• The people who carry out tasks on behalf of the data controller - eg external mailing companies, data security companies... NB Church volunteers are considered **Data Controllers**
PROCESS the	• Doing anything at all with collected information - eg collect, record, file, combine, produce, etc...
PERSONAL	• Relating to a *living* individual who can be identified by it or by other information in the Data Controller's possession - 'other information' includes eg a FWO number that connects information to a person
DATA of	• Information that's recorded in some sort of structured manner - it doesn't matter whether it's in paper or electronic format
DATA SUBJECTS	• The individual whose details are being processed and who therefore can exercise privacy rights

What does the Data Protection Act require of you?

Everyone responsible for using personal data has to follow 'data protection principles'. Simply put, you must make sure the information is:

There are two other principles enshrined in the Data Protection Act that occupy a different part of the new legislation, which caution that data should be:

- handled according to people's data protection rights, and;
- not transferred outside the European Economic Area without adequate security measures [some other countries' privacy laws give less protection].

These principles are developed to a greater extent by the new legislation and are explored in the following pages.

In addition, there is stronger legal protection for more sensitive information. That means losing, misusing or not securing information such as ethnic background, political opinions, **religious beliefs**, health, and criminal records can result in a more severe penalty than 'normal' personal data.

Theoretically, recording someone as a member of the Methodist Church in Ireland means you are processing *sensitive* personal data. In addition, your pastoral notes about a person are deemed to be 'personal data' and can therefore be accessed by them upon request; your opinion on their health becomes *sensitive* personal data. Under GDPR these are known as *'special category'* data.

Introducing the General Data Protection Regulation

GDPR came into effect on 25 May 2018 across Europe, and will continue to apply in the UK even in the case of a 'hard Brexit' in 2019.

Essentially, GDPR covers much of the same ground as we have already covered – the Information Commissioner's Office (ICO) describes it as an 'evolution, not a revolution' of data protection law – but it does add some extra detail in response to the changing ways we use – or could use – people's information. Just think for a moment about how technology has changed the way we communicate since you got your first mobile phone, when sending one text message seemed like a major accomplishment!

Today, a small amount of personal data can be duplicated and spread globally in a matter of seconds, and once the horse has bolted it's too late to shut the stable doors.

Accountability

GDPR mandates that you not only carefully use and look after other people's information, but that you also ***prepare a plan that can be documented and implemented in your data processing***. Every Circuit and Department now needs its own Data Protection Policy, along with associated documents. There is help available along the way, including template documents posted to the Methodist Church in Ireland website, but it requires ministers and key leaders sitting down together for a few hours to ensure everything is covered and you have a plan on training whomever might need brought up to speed.

Individuals' Rights

The other key change is the area of ***strengthened rights of the individual*** – in your planning you will need to be aware of the rights that people have regarding *THEIR* information that they have given to you – the gift of knowledge! Those rights include: **to be informed** of data use; **access** (to the information you hold about them); **to have inaccuracies corrected**; **to have information erased**; **to restrict** the processing of their information; **data portability**; **to object** to direct marketing and use for historical or statistical research, and; **to not be subject to decisions made by automated processing** incl profiling. So we'll keep the rights of the individual at the forefront of our minds throughout the rest of this booklet.

GDPR Principles of Data Protection

You will spot the key themes of previous data protection legislation in the principles outlined in Article 5 of the General Data Protection Regulation, which requires that requires that personal data shall be:

used lawfully	"a) processed **lawfully, fairly and in a transparent manner** in relation to individuals;
used for limited purposes	b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
requested only if relevant & necessary	c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
accurate	d) **accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
not kept forever	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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
kept secure & confidential	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."

Twelve Steps to Data Protection Compliance

Article 5(2) of the GDPR requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The way you can demonstrate compliance with the principles is to have a plan in place that's followed whenever you process data. Most people call that a *'data protection policy'*. A template policy is available on the IrishMethodist.org website, along with other forms and helpful documents.

There is a journey to embark upon to become compliant with the new law, as you prepare to write your data protection policy. The following pages give you a process to follow that should protect you, your circuit or department from painful data loss issues in the future, but will also enable you to treat the information given to you by the people you rely upon and with whom you work, in the best possible way. It is based on similar documents provided by the ICO and DPC – 'Twelve Steps to Take Now'; their websites have more helpful facts and guides should you want to explore this issue further, for instance: ICO Guide to GDPR [www.bit.ly/ICOgdprGuide].

On Circuits, we recommend that this process is undertaken by a small group of ministers and staff on your circuit, along with Officers such as Stewards, Secretaries and Treasurers. Your Circuit Executive must be able to report to the District Synod each Spring that your data protection policy is in place and being followed.

Similarly, departments of the Church need to be able to report their data protection arrangements to General Committee and/or Conference.

STEP	CONTENT	ACTION
1 Become Aware	Do our ministers, staff and organisation leaders who use personal data [names and addresses, dates of birth, phone numbers, e-mail addresses etc] realise that they fall under the 'data controllership' of the Circuit and have legal responsibilities because of that? And that those responsibilities are becoming more significant?	☐ Make a list of everyone who collects or uses personal information on behalf of the church. ☐ Decide how you will contact these people to make sure they are aware of their responsibilities.
2 Compile an Information Audit	Make an inventory of *all* personal data your church holds, and ask these questions: Why are you holding it? How did you obtain it? Why was it originally gathered (has the purpose changed)? How long will you keep it? How secure is it, both in terms of encryption and whether other people can walk in and see or take it? Do you ever share it with third parties and on what basis might you do so?	☐ Complete the '*Information Register*' spreadsheet *This is available on our website.* *A more thorough version is provided by the ICO at www.bit.ly/ICOaudit, useful for larger bodies.*
3 Communicate with Staff and Service Users	Review all your data privacy notices (eg on your website or membership forms) and make sure you keep members fully informed about how you use their data. If consent to use their information was previously implied, or if the way their information is used has changed, they should be notified and explicit consent requested (see Step 7).	☐ Check or write privacy notices used on any forms (paper or online) that collect personal information *Samples are included on our website. See also ICO guidance at www.bit.ly/ICOinform*

STEP	CONTENT	ACTION
4 **Be Aware of Personal Privacy Rights**	Be aware that the rights of individuals in relation to data you hold have been strengthened in the areas of: • being informed (their data is being processed) • access (they can ask to see all the information you hold on them) • accuracy (they can ask you to update their data) • erasure (they have the right to be forgotten by you) • opting out and limiting use of their data (they have the right to stop hearing from you and restrict how you use their information) • the portability of their data (any electronic data that you give them needs to be easily 'readable', eg not requiring a specific piece of software) – this right only applies to data processed under consent as the legal basis (see Step 6). • automated decision-making and profiling (unlikely to be conducted by MCI Circuits)	Ask: ☐ Who should people contact when requesting access to their records? ☐ Who is responsible for updating inaccuracies? ☐ Who would make the decision to delete any information? (Are there any reasons for holding data for a particular length of time before deletion – eg Gift Aid records?) ☐ How will you record a person's desire to *not* hear from you by post/e-mail/phone etc? ☐ Can electronic data be shared using a format that is commonly used? *The ICO offer guidance on this area at www.bit.ly/ICOrights*
5 **Prepare for Subject Access Requests**	You need a policy on how you will respond when someone asks to see the information you hold on them (you have up to one month), and written procedures to follow (eg when might a request be denied?).	☐ Write a Subject Access Request policy. *A sample is available on our website.*

STEP	CONTENT	ACTION
6 Decide Upon the 'Legal Basis' for Processing	There are six legal bases for processing personal data, two of which will be most used by churches: you will need to decide which one you are relying upon for each different use of information. ① ***'Legitimate interest'*** can cover *some* activities of a church (eg: pastoral visits to members; recording financial gifts; organising rotas; postal mailings about activities) – but not all. If the individual would not reasonably expect their data to be used in a particular manner, or its use is invasive, the main other legal basis is ② ***'Consent'***. Processing employees' data comes under ***'Contract'*** and is dealt with in the Methodist HR Data Protection Policy. If you don't have a legal basis to use a person's data, *you can't use it at all*.	☐ Decide which 'legal basis' you are going to use, and record it for each type of processing[1]. ☐ For Legitimate Interest, ask: ☐ Is this in the genuine interest of the church? ☐ Is this necessary? (does no other legal basis work?) ☐ Is this invasive to the individual? *Full guidance on lawful bases for processing, including the other bases available can be found at* www.bit.ly/ICObases
7 Understand Consent	Review how you seek, obtain and record consent. Are any changes necessary or further consent required? Example: have all members of your church given permission for their address details to be printed in a church directory? If not, you can't process their information for that purpose.	☐ Do you use personal information for any purpose that should be covered by explicit consent? ☐ Itemise these purposes and plan how consent will be acquired in the future.

[1] NB – Churches will nearly always need to combine their legal basis for processing with the *'Article 9(2)(d)'* exemption from the prohibition of using special categories of data (such as religious belief and health) available to non-profit organisations with a religious aim, when dealing with members, past members and people who have regular contact with the church.

STEP	CONTENT	ACTION
8 Give Special Attention to Children's Data	You can't presume you have permission to use children's data, even for things like birthday cards from the Sunday School. In practice, this means 'family' details need to be collected with specific consent granted by guardians for minors' information.	☐ Do you have adequate systems in place to verify individuals' ages and gather consent from guardians?
9 Be Ready for Data Breaches	If the personal data you hold is lost or stolen, and if it's likely to result in a risk to people's rights and freedoms, you must report it to the Information Commissioner/Data Protection Commissioner *within 72 hours*. NOT reporting can attract a fine, in addition to the breach itself. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. A breach has occurred if: personal data has been destroyed, lost, or altered by accident or without permission; personal data has been disclosed to someone else without their permission, or; anyone who doesn't have permission has been able to access personal data.	☐ Write a Breach Notification policy. *A sample is on our website.*

STEP	CONTENT	ACTION
10 Conduct Data Protection Impact Assessments	A DPIA is the process of systematically considering the potential impact that a project might have on the privacy of individuals; thus allowing organisations to identify and mitigate potential privacy issues before they arise. Any new technology or system bring introduced should prompt a DPIA, being designed with privacy at its core, and should gather and use as little personal data as possible.	☐ Are you preparing to undertake a new project that significantly uses personal data in a new way or introduces a new technology? If not, proceed to the next step. If so, refer to the ICO or DPC websites.
11 Appoint a Data Protection Officer	We won't need to designate a DPO 'officially', but even so, who will take responsibility for your data protection compliance? Will they have the knowledge, support and authority to do so effectively?	☐ Decide where the buck stops in your organisation – probably the Circuit Superintendent unless your Circuit Executive decides otherwise.
12 Select a Lead Supervisory Authority	The GDPR covers the entire European Economic Area, including the UK after Brexit; any Methodist departments or circuits operating in UK *and* RoI should select to engage with *either* the UK Information Commissioner *or* the RoI Data Protection Commissioner (wherever the bulk of data processing takes place, for circuits this is probably the minister's manse) as the 'Lead Supervisory Authority'.	☐ Decide whether ICO or DPC will be the Lead Supervisory Authority.

Further Resources

A number of helpful resources have been posted on the Methodist Church in Ireland website at www.irishmethodist.org/data-protection-resources. These include:

- Interpreting the Principles: A **Miscellaneous A-Z** of answered questions – this is a compilation of what are hopefully common sense approaches to issues that frequently arise with regard to the local church and her data protection responsibilities.
- **Information Register** – a spreadsheet that helps you to complete an information audit for your circuit/department.
- **Data Protection Policy template** – a sample policy that Circuit Executives can use as a launch pad for their own policy, including:
    - **Sample Privacy Notices & Consent Statements** – to give you an idea on what you should include as standard when seeking people's information.
    - **Subject Access Request Policy template** – a sample policy that can be amended for your use.

You will find a comprehensive range of guidance online from the UK Information Commissioner's Office (https://ico.org.uk/for-organisations/) and the Irish Republic's Data Protection Commissioner (http://bit.ly/DPCguidance). Sometimes guidance can be changed or refined – if the Commissioners' websites appear to contradict this document please follow their directions. If you spot any errors or omissions in this booklet please let us know.

Your notes

1 Fountainville Avenue, Belfast BT9 6AN | +44 (0)28 9032 4554