THE GENERAL DATA PROTECTION REGULATION (GDPR)
A GUIDE FOR CONGREGATIONS

INTRODUCTION

The present rules governing how organisations should handle, or "process", personal data are set out in the Data Protection Act 1998 ("the current Act"). However, the law is set to change on 25 May 2018 when the GDPR comes into force. The need for changes to the law regarding data protection arose from the huge increase in the use of computers, with the attendant implications for the storage, sharing and security of personal information about individuals.

The GDPR, which will apply to all organisations that handle the personal data of EU citizens, will become part of UK law. Like the current law, it seeks to protect the rights of individuals, and to enable them to control how their data is gathered, used, stored and shared. A new Data Protection Bill is going through Parliament at present which will set out the detail of the new law as it will apply in the UK – the Bill will implement and supplement the keys provisions of the GDPR.

- The GDPR will apply to congregations, as to other charities and organisations.
- The main concepts and principles are **very similar to those contained in the current Act**, but a significant change is the **"accountability" principle**, which places a much greater emphasis on transparency, openness, and the keeping of appropriate documents to demonstrate compliance with the other principles.
- Congregations will have to be clear as to the "legal bases" on which they are relying for processing personal information.
- Often congregations will be able to process personal information without obtaining the specific consent of the individual, but in certain situations consent will be required.
- This guidance note aims to provide a summary of what is required of congregations to ensure that their data processing is legal and can be demonstrated to be so, and to generally assist in preparing for the coming changes.
- Other GDPR resources are available on the Free Church website.

SOME KEY DEFINITIONS

- Personal data
- Processing
- Data controller
- Data processor
- Special category data

Personal data

The GDPR defines personal data as:

"***any information relating to an identified or identifiable natural person (called a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or societal identity of that natural person***."

As under the current law, the definition relates to living individuals, and to data held electronically or on paper records/in manual filing systems. However, the explicit inclusion of location data, online

Free Church of Scotland
Scottish Charity Number SC012925

identifiers (e.g. an IP address) and genetic data is new and may result in additional compliance obligations.

Congregations should be aware that this definition includes digital photographs and videos, where images are clear enough to enable individuals to be identified. Other examples of the sort of personal data commonly held by congregations are: staff/payroll records; membership lists; baptismal records; information relating to pastoral care; information regarding those attending holiday clubs, camps or other activities; lists of children/young people attending Sunday schools, youth groups and creches; records of those for whom congregations hold contact details for various reasons, including volunteers working with children and young people and others, those attending churches, making Gift Aid donations etc. These are examples only and there may be other types of personal data held.

Note: Congregations with websites with a facility to collect data, such as a "contact us" form need to be aware that the information supplied by any enquirer is personal data and will have to be held by the congregation in accordance with data protection law. Further, if a congregation uses cookies on its website to monitor browsing, it will be collecting personal data of that individual.

Processing

Processing is basically anything at all you do with personal data – it includes collecting, editing, storing, holding, disclosing, sharing, viewing, recording, listening, erasing, deleting etc. Individuals responsible for processing personal information in congregations may include the minister and other office bearers, treasurers, administrators, group leaders, safeguarding coordinators and others.

Data controller

The "controller" means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. In congregations the data controller will be the charity trustees. The "controller" also includes all staff and volunteers who work for the controller entity, and when staff or volunteers process personal information on behalf of the congregation, as part of their role, they will be doing so as a data controller. It is important that such staff/volunteers are adequately trained in respect of what is required of them under data protection law, as any data breach by them could lead to the congregation being liable. For example, staff/volunteers should not use any personal information being processed on behalf of the congregation for their personal use. Personal information must be used only for the *specific* purposes for which it has been *lawfully* obtained – more on this later.

Data processor

The "processor" means a natural or legal person, public authority, agency or any other body which processes personal data *on behalf of* the controller. This could be a third party who has been asked by the congregation to carry out processing on its behalf, and the definition of "processor" would also apply to any staff/volunteers working for the processor in this role. An example would be an IT supplier engaged by a congregation to provide a new system on which personal information will be stored. The IT supplier's staff also come within the definition of "processor".

Under the GDPR, data processors will be jointly and severally liable with data controllers for data breaches, to the extent for which they are responsible. This is a change from the current law. Any congregation using, or considering the use of, a data processor should have an appropriate written contract with that processor.

Special category data

It is vital that congregations are aware of and understand these special categories of personal information, which are very similar to the "sensitive personal data" described in and provided for under the current Act. They are personal data which are stated to be more sensitive than other types, and so require additional protection and safeguards. They are defined in the GDPR as personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, for the purpose of uniquely identifying a person, or data concerning a person's health or sex life or sexual orientation.

Most of the personal information processed by congregations about individuals will come under the definition of special category data, either specifically, and/or by implication, as the mere holding of any information about a person by a congregation is likely to be indicative of that person's religious beliefs. Special rules apply to the processing of special category data. These are explained later in this guidance note, as part of the section covering "Principle 1 – Lawfulness, fairness and transparency".

DATA PROTECTION PRINCIPLES

Like the current Act, the GDPR is based on several data protection principles. These principles, listed below, are very similar to the present ones, and set out the main responsibilities for organisations. There follows some information on the meaning and implications of each of the principles, with more detailed information being required for some than for others. The principles are:

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy (*including keeping information up to date*).
5. Storage limitation.
6. Integrity and confidentiality.
7. Accountability.

As mentioned in the introduction to this note, the last of these, the "accountability" principle, will have a major impact. It means being able to demonstrate compliance with the first 6 principles ***and is the real practical change from the current Act***. It requires organisations (and therefore congregations) to *document* their "legal basis" or "legal bases" (lawfulness - the first principle) for processing information as part of their *evidence of compliance*.

Also, some guidance on when and how "consent" should be used as a legal basis for processing personal information is included under principle 1 below - lawfulness, fairness and transparency.

Principle 1 - Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (the person whose data are being processed). Under the GDPR, individuals have an increased right to be informed about the use of their personal data, and congregations must be clear and transparent about how and why they are using personal information. The current Act has already established specific "conditions", or purposes, for processing data, and under the GDPR and the new Data Protection Act these conditions will persist, although the terminology is changing in that they will be referred to as "legal bases" rather than "conditions" (the present terminology) for processing data.

Lawful processing

For data processing to be lawful, organisations must be able to identify and rely on at least one of the following 6 "legal bases" for processing, those highlighted being the legal bases most likely to be relevant for congregations. (*Note: This is the starting point for general processing of personal data – for processing of special category data an* ***additional*** *condition for processing such data must be identified, as detailed under "Rules for processing special category data" below*):

a) **the person has given consent to the processing of their personal data for one or more <u>specific</u> purposes** (*see below for further information on the use of consent as the legal basis for processing);*

b) **processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (such as keeping and maintaining staff/payroll records)**;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or another natural person (this really just relates to life and death situations);

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*. For many charities this will often be the legal basis on which they can rely (subject to human rights, e.g. privacy).***

"Consent" as a legal basis for processing personal information

It is necessary to give some detailed information on the use of consent as a legal basis for processing personal data. It may sometimes be the case that what organisations previously understood to be the appropriate condition(s) for processing personal data under the current Act, was/were either not correct or is going to change under the GDPR. It is therefore crucial for congregations to be clear as to which of the above listed legal bases for processing apply to their processing of personal information, so as to ensure compliance with the new law. In particular, under the GDPR the legal basis of "consent" gives individuals much more control over their data and its uses than they have under the current Act.

One of the themes of the GDPR is to move away from consent as the condition or first basis of choice for processing personal data (although consent is of course one of the permitted legal bases for processing and there will still be many situations where it is required). The GDPR sets a high standard for consent. But often congregations won't need consent. For example, it should often be possible to rely on either "legitimate interests" (and/or "legitimate activities" where the personal information is special category data) as the legal basis for processing personal information.

However, there will be situations where consent is the appropriate legal basis for processing personal information, e.g. when a congregation wants to collect contact details from individuals so as to keep them informed of activities and events; or to include their personal information in a congregational directory for distribution/circulation; or to include personal information on a website

(*see under "Rules for processing special category data" below*). In such situations it will be vital to ensure that correct procedures are followed.

Consent of an individual means any freely given, specific (***this may often lead to more than one consent form being required from the same individual for different uses of their data***), informed and unambiguous indication of the person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Pre-ticked boxes do not demonstrate "clear affirmative action", and nor does any other method of default consent. Consent must also be easily withdrawn (*so individuals must be informed at the time of giving consent as to how they can withdraw it, and the procedure for withdrawing consent must be as simple as that for granting it in the first place*); clearly distinguishable; and the congregation must be able to prove compliance. It is important to be particularly careful about compliance if a congregation is relying on consent *alone* as the legal basis for processing (it is an option to get the consent of the individual *in addition to* another legal basis for processing personal information). If the data subject is a child, consent should be obtained in addition to relying on legitimate interests/legitimate activities.

A selection of template forms for use in different scenarios where congregations may require the consent of individuals for data processing are available on the website.

Signed forms should be kept as evidence that consent has been properly obtained. If you use a consent form which also contains a privacy notice, a copy of this should be given to the individual to keep. It is also permissible to obtain consent by obtaining an answer to a clear oral request. If you get consent this way, you will need to keep some proof of it, such as a note signed by the person who asked the question.

Checklists when using consent as the legal basis or processing personal information

The ICO has provided useful checklists for:

- Asking for consent
- Recording consent, and
- Managing consent.

These are available on the ICO website via the following link:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Additional rules for processing special category data

In addition to having to identify one of the 6 legal bases for processing personal information detailed above, processing of any of the special categories of personal data is prohibited under the GDPR unless one of several exemptions applies. 2 of these exemptions, detailed as follows, will be especially relevant and useful for congregations (although others may also apply):

- the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes.

- **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 are not disclosed outside that body without the consent of the data subjects.** *(This exception should cover much of the data processing carried out by*

congregations, but not data that is shared outside the Free Church, e.g. on a website – see below).

Further, it is important to note that meeting one of the exemptions for the processing of special category data is an **additional requirement** over and above the requirement to identify a lawful basis for general processing, as listed under "Lawful processing" above.

For some personal data processed by congregations, such as in connection with pastoral care and/or safeguarding matters, it will be obvious that it falls within the definition of special category sensitive personal data. So long as the processing is carried out in the course of the congregation's legitimate activities, with appropriate safeguards to keep it safe and secure, and it relates either to members, former members, or individuals in regular contact with the congregation, and that the personal data are not disclosed outside the Free Church without the person's consent, then it will be permitted under the "legitimate activities" exception above.

Other types of data processed by congregations will fall into this special category by implication. So, for example, in relation to membership lists, the personal information processed will come under this special category as by implication it relates to religious belief, but as the processing of such information for the purposes of maintaining an accurate membership roll is part of the congregation's "legitimate activities" it is permitted under the relevant exception above (in addition to falling within the "legitimate interests" general legal basis for processing) with no explicit consent being required. However, before such data could be used for other purposes, such as sharing with any other party, the explicit consent of the individual would be required.

It is important to remember that the "legitimate activities" exception to the prohibition on processing special category data is conditional on the data not being disclosed outwith the Church without obtaining the consent of the individual. So, for example, although the names of individuals on congregational rotas can be shared within the congregation, they should not appear on any church website unless the individuals concerned have given their specific written consent for that. Publishing any personal information on the internet, including photographs, is effectively making it available world-wide and should not be done without the consent of the individual, and the consent of a parent or guardian if the information relates to a child. **Template consent forms for use in these and other scenarios are available on the website.**

Special category data also includes personal data relating to criminal offences and convictions. Detailed information about special category data, and the conditions for processing such data can be read on the Information Commissioner's (ICO) website via the following link:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Principle 2 - Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not deemed to be incompatible with the initial purposes). It is therefore crucial that congregations are clear as to the reasons why they are collecting personal information from individuals.

Principle 3 – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4 – Accuracy

Personal data must be 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.

Principle 5 – Storage limitation

Personal data must be:

- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed. It is therefore crucial to be clear as to what the purposes are from the outset. It also means that data which has been anonymised can be retained;
- subject to appropriate security measures, data may be kept longer for public interest archiving, scientific and historical research and statistical purposes.

Principle 6 – Integrity and confidentiality

Personal data must be processed in a way 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. This is the same as under the current law. So, data should be kept on secure computer systems and/or in secure manual filing systems. In particular:

- passwords should be kept secure, should be changed regularly and not shared.
- if computers are in shared areas the user should lock or log off when away from his or her desk.
- It is recommended that emails containing personal information should not be sent to work/employer managed email addresses (other than "@freechurch.org addresses) to avoid the risk of such emails being accessed by others.
- It is recommended that joint or shared email addresses should not be used.
- where personal information relating to church matters is being processed on home computers it should be password protected.
- confidential paper waste should be disposed of securely by shredding.
- to prevent virus attacks care should be taken when opening emails and attachments or visiting new websites.
- hard copy personal information should be securely stored and not visible when not being used.
- visitors should be signed in and out of premises or accompanied in areas normally restricted to "staff".
- computer screens should be positioned away from windows to prevent accidental disclosure of personal data.
- personal data being taken off the premises should be encrypted if it would cause damage or distress if lost or stolen.
- back-ups of data should be kept.

Congregations must respect the individual's right to confidentiality. Great care must be taken to ensure that third parties cannot access the data without the permission of the individual concerned and that data about individuals is not disclosed – to third parties or others – without their consent, unless the church is allowed or obliged to disclose the data by law.

Particular care should be taken in dealing with any request for personal information over the telephone. The amount of information given out over the telephone should be limited and in any event identity checks should be carried out if giving information out over the telephone, whether by

way of an incoming or an outgoing call, to ensure that the person requesting the information is either the individual concerned, or someone properly authorised to act on their behalf.

There is a very high risk of breaching this principle by sending personal information to the wrong person by any method, but especially where the information is sent by email. Particular care should therefore be taken when sending any personal information by email.

Principle 7 – Accountability

The data controller is responsible for, and must be able to demonstrate compliance with, the first 6 principles.

Organisations now have to be able to prove that they are compliant, by providing evidence if asked. To be able to do this, congregations should, for example, document the decisions they take about their various types of data processing, record staff and volunteer training, review policies and audit processing methods and activities.

SOME RIGHTS OF INDIVIDUALS (DATA SUBJECTS) UNDER THE GDPR

The right to be informed

Individuals have the right to be informed, by being given "fair processing information" regarding how organisations will use their personal data, so congregations must be transparent about how and why they are using personal information. This should normally be done through a **data processing notice or privacy notice**, although it can also be done verbally, for example when taking personal information over the telephone.

These notices should include the identity of the congregation, how it is intended the information will be used, the legal basis for processing the information, how long the information will be retained for, and that individuals have a right to complain to the ICO if they are not happy with how their personal information is being processed.

A template Privacy Notice for use by congregations is available on the website.

Note: privacy notices and consent forms are not the same thing. Privacy notices tell individuals how their data will be processed and are required whatever the legal basis for processing is, whether consent or another basis, such as legitimate interests and/or legitimate activities, whereas consent forms are for use only where consent is being used as the legal basis for processing information. However, it can sometimes be possible to combine a consent form with a privacy notice specifically tailored to that consent (see template consent forms on website). In addition to such combined privacy notices/consent forms, congregations should always have a more general privacy notice to cover all the legal bases for processing used by them.

The right of access

As under the current law, individuals have the right to obtain a copy of their personal data from the data controller, by way of a "subject access request". They are now entitled to receive this free of charge (unlike the present £10 chargeable, although a reasonable fee can be charged if the data subject requests further copies), and within 30 days (shorter than the current 40-day period allowed). A further 2-month extension for compliance may be obtained in the case of complex or numerous requests, and in such circumstances the individual must be informed within one month of the receipt of the request and be given an explanation of why the extension is necessary. Organisations are entitled to refuse manifestly unreasonable requests.

It is important to verify the identity of the person making the request, using "reasonable means".

If the request is made electronically, the information should be provided in a commonly used electronic format.

The right to rectification/correction

Data subjects have the right to have incorrect data rectified if it is inaccurate or incomplete. If the information has been disclosed to third parties, they must be informed of the rectification where possible. Organisations must also inform the individuals about the third parties to whom the information has been disclosed where appropriate.

A request for rectification must be complied with within one month, which can be extended by 2 months where the request is complex.

If no action is being taken in response to a request for rectification, an explanation as to why must be given to the individual, informing them of their right to complain to the ICO.

The right to erasure - "right to be forgotten"

Individuals have a right to have personal data erased by the data controller without undue delay where there is no compelling reason for its continued processing, in particular in any of the following circumstances:

- where the personal data are no longer necessary in relation to the purpose for which they were originally collected/processed.
- when the individual withdraws consent.
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data are unlawfully processed (i.e. otherwise in breach of the GDPR).
- the personal data must be erased in order to comply with a legal obligation.
- the personal data are processed in relation to the offer of information society subjects to a child (i.e. online services).

However, this does not mean that an individual is necessarily entitled to have data erased on request. If the purposes for which it was collected still exist then the data should not be deleted, *unless* the legal basis for processing the data was consent – in that event the data will have to be deleted if consent is withdrawn.

If the information has been disclosed to third parties, they must be informed of the erasure, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that where personal data is processed online, for example on social networks, forums or websites, organisations should inform other organisations who process the personal data to erase links to or copies of the personal data in question, although there may be exemptions in certain circumstances.

The right to restriction of processing

In certain circumstances, such as if an individual considers that their personal data are inaccurate, or if they object to the processing, they may have the right to restrict processing of their personal data. In such an event the data can continue to be stored but not used/processed in any other way.

The right to data portability

This is unlikely to affect churches.

The right to object

Individuals have the right to object to processing if they are not satisfied that the organisation has a legal basis for doing so.

The right not to be subject to automated decision making

This is also unlikely to affect churches.

PROCEDURE WHERE A DATA BREACH HAS OCCURRED

A data breach occurs where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Under the current law it is not mandatory to report a data breach to the ICO, although it is good practice to do so.

Under the GDPR, in the event of a personal data breach it will be compulsory for the data **controller** to report this to the ICO within 72 hours of becoming aware of the breach, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.

A data **processor** is required to notify the **controller** without undue delay after becoming aware of a personal data breach.

When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals the **controller** must communicate the personal breach to the data subject without undue delay. This is NOT required if the data is encrypted, which makes a strong case for the advisability of encryption where appropriate.

PREPARING FOR THE GDPR – 10 steps for congregations to take now

1. In general, ensure that all those who "process" (collect, hold, use, etc.) personal information (data) on behalf of the congregation are aware of the principles of the GDPR.

2. Carry out a review of the categories of personal information processed by the congregation (called a "data audit" – a template form for this is available on the website for use). Check where the information came from, and who it is shared with.

3. For each category of personal information held, decide which lawful bases you are relying on for processing this information. Remember that most personal information processed by congregations will come under the "special categories" of personal data, and that for such data you must identify 2 legal bases for processing – one from the general bases and one from the additional bases for special categories of personal data. Document this as evidence of compliance.

4. Prepare and adopt a Privacy Notice for the congregation. A template is available on the website.

5. Review whether consent is required for any personal information already held and obtain consents where appropriate. Retain consents as evidence of compliance. Several template forms are available on the website. **Remember that more than one consent form may be required from the same person for separate categories of data processing**.

6. Ensure that you are aware of each of the rights of individuals under the GDPR, as referred to in the guidance note.

7. Review data relating to children. Consent may not always be the most appropriate legal basis for processing, but, where it is, ensure that it has been appropriately obtained.

8. Review security, especially around access and the use of hard copy and electronic records.

9. Ensure that you have processes or systems in place to enable you to comply with any possible subject access request within 30 days of receipt.

10. Ensure that you have processes or systems in place to detect, report and investigate any personal data breach.

FURTHER INFORMATION

Further resources are available on the Free Church website. These will be updated and added to from time to time.

There is also extensive information and guidance regarding the GDPR on the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ .