The General Data Protection Regulation (GDPR)

A Brief Guide for Scottish Episcopal Church Congregations

Introduction and Summary

What's happening and why is it important?

The General Data Protection Regulation (GDPR) will take 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 protection in how their personal data is used by organisations. Congregations must comply with its requirements, just like any other charity or organisation. This guide tells you what you need to do. The first four pages comprise a summary. More detailed guidance and explanations are contained in the subsequent pages.

We are grateful to the Church of England for permission to use its material as a basis for preparing this guidance for the Scottish Episcopal Church

A. Underlying Principles

Explaining the jargon:

- **Personal data** means information about a living individual which is capable of identifying that individual.
- **Sensitive personal data** means personal data revealing religious or philosophical beliefs, racial or ethnic origins, political opinions, trade union membership, and information concerning an individual's health, sexual orientation and genetic or biometric information.
- **Processing** is anything done with/to personal data, including collecting, using, storing, transferring or destroying it.
- The **Data Subject** is the person about whom personal data are processed.
- The **Data Controller** is the person or organisation who determines how and why data is processed. In a congregation this will usually be the Cleric or Vestry.

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

- must be Processed lawfully, fairly and transparently.
- must only be used for specified purposes that the Data Subject has been made aware of and no other.
- collected on a Data Subject should be "adequate, relevant and limited to what is necessary." i.e. only hold the minimum amount of data that you need for your specific purposes.
- must be "accurate and where necessary kept up to date".
- should not be stored for longer than is necessary, and that storage must be safe and secure to protect against unauthorised access or accidental loss, destruction or damage.

B. Vestries and Clerics as Data Controllers

It is important to be aware that each Cleric is considered to be a separate data controller from their Vestry because they are separate legal entities. Additionally, Clerics may hold pastoral information separately from the information held by the Vestry and will make decisions on how this information is used.

However, the Cleric and the Vestry may wish to rely on the same documentation / privacy notice for reasons of practicality. The example Privacy Notice in the Privacy Notices and Consent Forms Guidance Note has been drafted on this basis. If a new Cleric is appointed to a congregation, they will be made aware of the Privacy Notice and how they will be expected to process personal data.

We acknowledge that as a member of the Vestry, the Cleric will have access to the same information that the Vestry has access to. However, from a strict legal perspective under GDPR, there is a distinction that you should be aware of.

C. Areas for Action

Key areas for congregations to be aware of include:

1. **Data Audit**. This is the perfect time to review what data you hold, how you store it, and what basis you have for processing it. We have a simple audit template that you may find useful (see Appendix 1).
2. **Privacy Notices**. You will need to develop a Privacy Notice telling individuals what you do with their personal data. To develop a Privacy Notice you will need to identify (i) what personal data you hold; (ii) why you hold that personal data; (iii) where you store that personal data; and (iv) how long you hold that personal data for. The following pages along with the Privacy Notices and Consent Forms Guidance Note provide more detail on how you can develop such a Privacy Notice and what information should be contained within this Privacy Notice. The Privacy Notice should be issued to all individuals that you hold data about.
3. **Consent**. You may need to gain consent from some Data Subjects, for example, when you wish to issue promotional / fundraising communications to them through electronic means i.e. via e-mail or text or if you wish to share any sensitive personal data outwith the Vestry, such as the Communicants' Roll. If you have not previously operated on an 'opt-in' consent basis, you will need to re-collect valid consents in order to continue contacting individuals. Remember though that consent is not required for all processing of personal data. Other legal bases are available, for example, the processing may be in the legitimate interests of the church. These alternative legal bases are detailed in greater detail below and you should use these where possible. The following pages along with the Privacy Notices and Consent Forms Guidance Note provide more detail on when you should issue consent forms.
4. **Data Protection Fee**. You should consider whether you are required to pay the Data Protection Fee. 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 fee for charitable organisations from May 2018 is set at £40 however there are various exceptions. You should consider the more detailed guidance set out below and assess whether you will be required to pay this.
5. **Data Subjects' Rights**. Data subjects have a number of rights, including the right to know what data is held about them, the right to know how that data is used by the Data Controller, the right to have any inaccurate data corrected and the right 'to be forgotten' if the Data Controller no longer requires to hold that information. The Cleric/Vestry will need to have a process to provide information and make changes to information if individuals exercise their rights.
6. **Accountability.** 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. Such evidence includes a compliant privacy notice and a processing register. It is important that you look at the various types of data processing you carry out, identify the purposes and legal basis for this processing and keep a written record of all your processing activities, security measures and data retention practices. Such information may need to be supplied to the ICO if requested.

D. Basis of Processing

1. In order to process personal data, you require to have a legal basis for such processing. There are a number of legal bases including (i) having the consent of the individual, (ii) processing in compliance with a legal obligation and (iii) processing for the legitimate interests of running the Vestry. 'Legitimate Interest' means that you can process personal data if (i) you have a genuine and legitimate reason for doing so; and (ii) you are not harming any of the Data Subject's rights and interests.
2. People need to give their **consent** before you send them electronic promotional materials, fundraising materials and other communications (primarily e-mail and texts), for example, in relation to any events. This consent will need to be clear and unambiguous – i.e. some form of positive action is required to 'opt-in' for specific and identified purposes. You cannot communicate with people outside of the scope of the consent that you have obtained. Therefore, you should review the template Consent Form in the 'Privacy Notices and Consent Forms' Guidance Note and assess whether you would wish to communicate with people for any other purposes. Obtaining a comprehensive consent will mean that you do not need to obtain multiple separate consents.
3. 'Opt-out' consents will no longer be permitted under GDPR. Therefore, you may need to gather this consent if you do not already have it or refresh this consent if you have been operating on an opt-out basis.
4. Where you collect consents, e.g. to be added to an email mailing list, you will need to keep a record of those consents.
5. Consent can be withdrawn at any time. Therefore, where possible, we recommend that you rely on another legal basis.
6. Remember though that consent is not required for all processing of personal data. Examples include:
    a. Consent is not required if you are issuing general communications (i.e. non-promotional / fundraising communications) by e-mail or text to provide a congregation with information that they need to know about the church. This can be done on the basis of the church's legitimate interests. For example, if you are informing members of the cancellation of a service due to adverse weather. The requirement to obtain consent for electronic communications is specific to promotional / fundraising communications; or
    b. Consent is not required if you are issuing promotional / fundraising communications by post. This can be done on the basis of the church's legitimate interests. This difference is due to the legislation in place around promotional / fundraising communications. However, you should give individuals the ability to opt-out to receiving such communications. For an example of this, see the example consent form in the Privacy Notices and Consent Forms Guidance Note.
7. In such circumstances, other legal bases are available, for example, the processing may be in the legitimate interests of the church. These alternative legal bases are addressed in greater detail below and you should use these where possible.

E. Basis of Processing – Sensitive Personal Data

1. If sensitive personal data is being processed, for example, personal data revealing an individual's religious beliefs or health, then there are additional legal bases that must be met including (i) having the explicit consent of the individual or (ii) processing by the Cleric/Vestry of information relating to members or former members (or those who have regular contact with the church in connection with those purposes), provided there is no disclosure to a third party without consent. That means that a Cleric/Vestry can obtain, hold and process sensitive personal data without consent for use internally but must obtain consent to share it, for example, with another Vestry, with a Diocese or with the General Synod.
2. You should note that not all personal data processed by the Scottish Episcopal Church is sensitive personal data simply because the Scottish Episcopal Church is a religious organisation. Rather, it is where decisions are made as a result of religious belief, ethnicity, sexual orientation or health that Vestries would be deemed to be processing sensitive personal data.
3. An example of processing such sensitive personal data is holding and updating the Communicants' Roll. As this is a declaration of faith, the consent of the individual will be required to include their details on the Communicants' Roll and to share their details within the wider Scottish Episcopal Church. However, an individual's name and address on a flower rota would not be processing sensitive personal data as no decision is being taken on the basis of their religious beliefs and so would not require consent as the Vestry could rely on a legitimate interest that members of the rota would expect the rota to be shared. The difference here is that legitimate interest may be a valid legal basis for sharing personal data (provided you inform the individual that you are doing so) but is not a valid legal basis for sharing sensitive personal data.
4. For the same reason, the entry of an individual's name and address on the Adherents' Roll may not be sensitive personal data as this is simply a means of recording the contact details of individuals who may have attended the congregation or may have had contact with the congregation. It is not used as a declaration of faith and an individual will not be treated any differently through being recorded on the Adherents' Roll.

Detailed Guidance

What's Happening and why is it important?
The law is changing. Currently, the Data Protection Act 1998 governs how you process personal data (i.e. what you do to/with data which can identify a living individual, including collecting, using, storing and managing such data). On 25 May 2018, the General Data Protection Regulation (GDPR) will replace the 1998 Act. The Government has now published the Data Protection Bill. You should note that the Bill supplements and implements the key provisions of the GDPR; outlines where UK law will deviate from certain GDPR provisions and updates and strengthens UK law to make the shift to GDPR (and the UK's withdrawal from the EU) as smooth as possible. You therefore need to know what things you should keep doing and what things you should do differently in order to comply with the new law.

What are the main differences from the 1998 Act?
The good news is that the GDPR's main concepts and principles are very similar to those contained in the current 1998 Act. The Information Commissioner's Office (ICO) will still be the organisation in charge of data protection and privacy issues. Therefore, if you are complying with the 1998 Act, much of what you do will still apply. However, there are some changes and additions, so you may have to do some things for the first time and some things differently (these are highlighted below).

One of the main changes to note is that the GDPR places a much greater emphasis on transparency, openness and the documents you need to keep in order to show that you are complying with the legislation – this is incorporated within the idea of "accountability".

Accountability – What is it and how do I comply?
The new accountability principle means that you must be able to show that you are complying with the principles. In essence, you cannot just state you are compliant; you have to prove it and be able to provide evidence. To do this there are a number of actions you should take, such as documenting why you process personal data in certain ways and other compliance activities – such as attending training on data protection, reviewing any policies and auditing processing activities.

How do I show that I am processing personal data lawfully?
Under the GDPR, it is now necessary to explain the lawful basis for processing personal data in a privacy/data protection notice (see below) and when you respond to Data Subject Access Requests. The lawful bases for processing personal data are broadly similar to the processing conditions contained in the 1998 Act. It should be possible to review the types of processing activities you carry out and identify your lawful basis for doing so. These lawful bases should be fully documented, which will help in complying with the accountability requirement.

The lawful bases most relevant to a Cleric/Vestry are likely to include:

- Having the consent of the individual,
- Processing in compliance with a legal obligation, and
- Processing for the legitimate interests of running the Vestry. 'Legitimate Interest' means that you can process personal data if (i) you have a genuine and legitimate reason for doing so; and (ii) you are not harming any of the individuals' rights and interests.

Therefore, for example, when a new member joins the congregation, it would be in the legitimate interests of the Cleric/Vestry to include their details on the Adherents' Roll or a membership list, provided of course, that the individual is informed that their information will be put on the membership list.

In addition, certain personal data processed by a Vestry or a Cleric will be classed as sensitive (called special category personal data under the GDPR) because it relates to "religious belief" and therefore, you will need to identify additional bases for processing the personal data. In the context of a congregation the most relevant lawful bases for processing are:-

- Explicit consent from a person; or
- Where the processing is a "legitimate activity" and relates to either members or former members or to individuals with whom there is regular contact, but is not disclosed to any third parties without consent

For example, the processing of personal data in relation to the Communicants' Roll, is likely to be sensitive (by implication, if not directly, because it relates to "religious belief"). As it relates to members (or individuals in regular contact with the congregation) this processing can be said to be a legitimate activity of the Cleric/Vestry. However, if you wanted to share this data with another party / publically, you would require the consent of any relevant individual(s). Such consent can be obtained through the Declaration for Inclusion of an Individual in the Communicants' Roll of a Congregation. Consent in respect of children is discussed in greater detail below.

Please refer to the separate "Data Protection – Privacy Notice and Consent Form" guidance for more details in relation to the lawful bases for processing personal data (including data which will be classed as sensitive).

Is all personal data processed by the Scottish Episcopal Church sensitive personal data?

Advice has been taken from the Information Commissioner's Office (the UK data protection regulator) on whether all personal data processed by a Vestry would constitute sensitive personal data on the basis that the Vestry is part of a religious organisation and therefore an individual's religion could be inferred through their association with the Vestry. The ICO has taken the view that not all personal data processed by the Scottish Episcopal Church will be sensitive personal data.

It is where decisions are being made as a result of religious belief, ethnicity, sexual orientation or health that Vestries would be deemed to be processing sensitive personal data.

Therefore, by way of example, the Communicants' Roll will be processing sensitive personal data as this is a declaration of faith and relates to religious belief. Consequently, the sharing of the Communicants' Roll with third parties such as the Vestry, Diocesan Bishop or Dean would require consent. (Included in the separate 'Privacy Notices and Consent Forms' Guidance Note is a specific consent form for use in connection with the Communicants' Roll. If all individuals on the Communicants' Roll provide such consent the Roll may be exhibited to the congregation, Diocesan Bishop or Dean.) However, an individual's name and address on a flower or Sunday School rota would not be processing sensitive personal data as no decision is being taken on the basis of their religious beliefs and so would not require consent as the Vestry could rely on a legitimate interest that members of the rota would expect the rota to be shared. The difference here is that legitimate interest can be a valid legal basis for sharing personal data (provided you inform the individual by a data protection privacy notice that you are doing so) but is not a valid legal basis for sharing sensitive personal data.

Consent

Where you rely on consent as the lawful basis for processing any personal data, you need to be aware that to be valid under the GDPR, consent must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, you will need to record how and when the consent was obtained (and review this over time). This can be done via a signed and dated consent form. Consent will require "clear affirmative action" and the ICO has noted that there is little difference between "explicit" and "unambiguous". Silence, pre-ticked boxes or inactivity will **not** constitute consent.

Therefore, where you wish to rely on consent, you will have to make sure that any consent wording is sufficiently strong to allow you to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting. You will also have to tell individuals that they have the right to withdraw consent at any time and ensure that the procedure for withdrawing consent is just as simple as granting consent, (e.g. by sending an email or (un)ticking a box).

You should note that consent may not be appropriate in every case. Remember there are other lawful bases for processing personal data. For example, you would not have to obtain consent to share the names of individuals on the flower rota or after service tea/coffee rota with other church members as this is not classed as sensitive personal data. In that instance, the information is shared with others in order to carry out a service to other church members and the sharing of such information is in the legitimate interests of the church. The difference here is that legitimate interest can be a valid legal basis for sharing personal data (provided you inform the individual that you are doing so) but is not a valid legal basis for sharing sensitive personal data. However, individuals should be informed that their details will be circulated to other church members, if that is what is intended.

Do I need to register (notify) with the ICO?

The ICO has confirmed that although there is no requirement to register/notify under the GDPR, there will be a new annual "data protection fee" which **data controllers** will be legally required to pay. Therefore, this could be applicable to both Vestries and Clerics. The fee for charitable organisations is to be set at £40. There are exemptions from this fee and the ICO states that these will be similar to those under the current registration/notification regime.

An exemption which is likely to apply to Vestries / Clerics is the "not-for-profit" exemption. This exempts organisations that are not established or conducted for profit. However, this exemption only applies if:

- you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it; and
- you only hold information about individuals whose data you need to process for this exempt purpose; and
- the personal data you process is restricted to personal information that is necessary for this exempt purpose.

This is a fairly narrow exception. If a Vestry's / Cleric's activities are restricted to these activities then it will not be required to pay the fee. However, if the activities go beyond this, then a fee may be required. Further information on whether you will be required to pay this fee is set out (here). You should consider these requirements to assess whether you are required to pay this fee.

Will I need to have a Data Protection Officer?
Congregations are highly unlikely to be required to have a Data Protection Officer as such. Data Protection Officers are required in certain circumstances, such as where organisations process sensitive (special category) personal data on a "large scale". The processing of sensitive personal data by the Vestry and/or Cleric is unlikely to be classed as "large scale". However, it would be advisable to designate one person as having responsibility for data protection issues, including providing support and guidance for others, such as the Vestry and Cleric.

If a data protection issue comes up and you are unsure how to respond, you may wish to contact your Diocesan Registrar, who may be able to help.

Is the Cleric a separate data controller from the Vestry?
Yes - each Cleric and each Vestry is considered to be a separate data controller because they are separate legal entities who will be processing personal data. Additionally, Clerics may hold pastoral information separately from the information held by the Vestry and will make decisions on how this information is used.

However, the Cleric and the Vestry may wish to rely on the same documentation / privacy notice for reasons of practicality. The example Privacy Notice in the Privacy Notices and Consent Forms Guidance Note has been drafted on this basis. If a new Cleric is appointed to a congregation, they should be made aware of the Privacy Notice and how they will be expected to process personal data.

We acknowledge that as a member of the Vestry, the Cleric will have access to the same information that the Vestry has access to. However, from a strict legal perspective under GDPR, there is a distinction that you should be aware of.

What are the restrictions on the use of personal data?
The principles are similar to those in the 1998 Act, with added detail at certain points and, as stated above, a new **accountability** requirement.

The GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that individuals should be told what you are going to do with their personal data before you use it and consent to such use;

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

(d) accurate and, where necessary, kept up to date. Personal data that is found to be inaccurate should be deleted or corrected without delay. All personal data should be periodically checked to make sure that it remains up to date and relevant;

(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. For instance, records of pastoral care

discussions should not be kept for a number of years without justification. Records could be kept, for instance, if all identification features were removed, referred to as "anonymisation"; and

(f) kept securely. Personal data storage should be safe and secure – in lockable filing cabinets or in password protected computer files. Names and addresses of individuals should not be left unattended.

What are the rights of individuals and how do they operate?
Generally, the rights of individuals that are granted under the GDPR are the same as under the 1998 Act but with some significant additions. The GDPR includes the following rights for individuals, which are briefly explained here: -

- **The right to be informed**
  When you currently collect personal data, you have to give individuals certain information, such as your identity and how you intend to use their information. This is usually done through a privacy/data protection notice. Under the GDPR there is additional information that you will need to supply. For instance, you will have to explain the lawful basis for the processing of their data; your data retention periods (how long you keep it for); and that individuals have a right to complain to the ICO if they think that there is a problem in the way that you deal with their personal data.

- **The right to access (includes subject access requests)**
  Individuals have the right to be given confirmation that their data is being processed; access to their personal data and supplementary information, (i.e. information that is usually supplied in a privacy notice).

    - **Subject Access Requests**
      The GDPR continues to allow individuals to access their personal data so that they are aware of and can check the lawfulness of the use and the accuracy of the data.

      In most cases you it will no longer be possible to charge for subject access requests. There will be a one month period from the receipt of such a request in which to comply rather than the current 40 days. You will be able to refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If you do refuse a request you must tell the individual why and that he/she has the right to complain to the ICO or a judicial remedy.

      There are limited circumstances where information may be withheld from the individual making the request, for example, if this would disclose personal data about a third party.

      If you receive a subject access request and are unsure how to respond, advice should be taken from the Diocese Registrar.

- **The right to rectification (correction)**
  Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, you must tell those third parties of the correction. You must also tell the individuals about the third parties to whom the data has been given.

- **The right to erasure (also known as the right to be forgotten)**
  Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

  This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. For instance, safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and proportionate – e.g. to protect members of the public from significant harm. Another example is that some financial information, such as that relating to gift aid, cannot be deleted immediately due to financial auditing regulations. Communicant Roll data should be deleted when it is no longer valid or if the individual withdraws consent to the processing.

- **The right to restrict processing**
  Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If processing is restricted, you can still store the data but cannot otherwise use the data.

- **The right to data portability**
  This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT system to another. It only applies in certain circumstances, and is **highly unlikely to affect congregations**.

- **The right to object**
  Individuals have the right to object to processing in certain circumstances – e.g. If a congregation has relied on legitimate interest to process data without consent and an individual is not happy with this they have the right to object to the congregation processing their data. If an individual exercises his/her right to object, the Cleric/Vestry should stop the processing objected to unless the Cleric/Vestry can demonstrate that it has a compelling legitimate ground that overrides the rights of the individual. This is a high standard to satisfy.

- **The right not to be subject to automated decision-making including profiling**
  The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This right is similar to that contained in the 1998 Act. **This is highly unlikely to affect congregations.**

Processing personal data about children – What do I need to do? Are there any additional steps?
The GDPR brings into effect special protection for children's personal data, particularly in relation to commercial internet services, such as social networking. Processing of data for such matters is known as processing for "information society purposes". Given the nature of such services, congregations are unlikely to be offering online services to children. However, it could apply if, for example, a Vestry or Diocese were to set up an app in order to attempt to communicate more effectively with children. If you do offer online services to children and rely on consent to collect their information, you may need a parent's or guardian's consent in order to lawfully use that data. Only children aged 13 or over are able to provide their own consent in respect of information society services (GDPR sets the age when a child can grant consent for information society services at 16, however the UK Government has proposed in its Data Protection Bill, currently going through parliament, that this be reduced to 13).

Separately, congregations may also collect children's consent for purposes other than "information society purposes", for example, when children are completing camp and health forms or when they are added to the Communicants' Roll. In such non-information society circumstances, the Data Protection Bill proposes that in Scotland (i) children aged 16 and over can provide consent and (ii) children aged under 16 can provide consent provided that they have a general understanding of what it means to give such consent. Children aged 12 or over are presumed to be of sufficient age and maturity to consent unless the contrary is shown. The effect of this is that unless there is reason to suppose that a particular child aged 12 or over is not able to give consent then such a child can themselves sign consent in relation to the Communicants' Roll but if the child is younger than that then their parent or guardian should sign for them.

You should remember that you have to be able to show that you have been given consent lawfully and therefore, when collecting children's data, you must make sure that your privacy/data protection notice is written in a language that children can understand and copies of consents must be kept.

Security

You should have security systems in place to protect personal data. The standard set by GDPR is to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing, for example, what damage could there be caused if you suffered a data breach.

Examples of such security measures include ensuring that personal data in hard copy form and which cannot be shared publicly is stored in locked cabinets with access restricted to those who need to use such data and password protecting computers and electronic documents which contain such data. This is particularly important if others (for example, other family members) have access to your computer where personal data is stored.

What do I need to do if there is a data breach?
A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Currently, data breaches do not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice so to do). The GDPR makes informing the ICO compulsory unless the breach is unlikely to result in a risk to the individuals affected. In addition, there is a requirement to notify the individuals affected in certain circumstances, (e.g. where there is a high risk to the individuals involved, for instance, through identity theft). Under the GDPR, you will have to notify the ICO of a data breach within 72

hours of finding out about this. It is important that those who are responsible in the congregation note this deadline and we would recommend that any suspected breaches are reported to the Diocesan Office or the General Synod Office without delay since such breaches may raise broader questions of the Church's public reputation beyond just the congregation in question.

More details can be provided after 72 hours, but before then the ICO will want to know the potential scope and the cause of the breach, planned mitigation actions, and how the problem will be addressed for the future.

Contracts

Vestries should consider whether they have entered into any contracts with third parties that involve the processing of personal data. For example, if the Vestry has contracted a web designer to create a website and that web designer has access to personal data, for example, Vestry Members' log-in details or a congregation list. If personal data is processed by that third party then the congregation needs to ensure that the contract with that third party is GDPR compliant. GDPR mandates that certain protections for personal data must be included in contracts with third parties that process personal data.

When does the GDPR come into effect?
On 25 May 2018. As a regulation the GDPR will become law in the EU Member States automatically without the need for local legislation. The exit of the UK from the EU has no effect on the application of GDPR to you. The Government has confirmed that it will be introducing its own data protection legislation which will incorporate the terms of the GDPR once the UK leaves the EU.

What are the penalties for not complying with the GDPR?
There has been much publicity about penalties under the GDPR. Individual countries keep the right to determine the particular penalty to be applied but the maximum penalties are set out in the GDPR. Criminal penalties are left to each country but will be compulsory.

What is important is that there has been a substantial increase in the maximum possible fines (in the UK it is currently £500,000).

Under the GDPR some examples: -

- For a failure to get parental consent where personal data are collected about a child in the process of providing an "information society service", (e.g. online magazine/newspaper, buying/selling online), a fine of up to 10 million Euros or 2% of the data controller's annual worldwide turnover for the previous year;
- For a failure to provide adequate information to data subjects or to allow subject access, or to comply with the right of erasure (see above), a fine of up to 20 million Euros or 4% of the data controller's annual worldwide turnover for the previous year

The ICO has stated, however, that fines are a last resort. Organisations that systematically fail to comply with the law or completely disregard it, particularly when the public are exposed to significant data privacy risks, need to know that the ICO has these penalties available. However, the Information Commissioner has stated that the ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. In any event, like the 1998 Act, the GDPR gives the ICO various penalties to help organisations comply – warnings, reprimands, corrective orders. The ICO has stated that it shall use its powers proportionately and judiciously.

What do I need to do to prepare for the GDPR?

- Check to see what personal data you are holding and using and why, and with whom you share it;
- Check where/how is this personal data stored and who has access to it;
- Review all types of processing and ensure that these can be justified by one of the processing conditions (and are fully documented);
- If consent is relied upon, check to see that it explains what processing is being carried out and that it has been correctly obtained;
- Ensure that you put in place appropriate privacy/data protection notices and that they contain the additional information that is required under the GDPR;
- Ensure you have an adequate procedure for dealing with requests from individuals;
- Ensure you have appropriate retention periods relating to the data you hold;
- Check whether any existing IT systems are capable of deleting or correcting personal data and handling requests from individuals;
- If a project is likely to have a high impact on the rights of individuals, for example, if decisions will be made about them resulting from the project, then a Data Protection Impact Assessment may be needed;
- Review all current data protection policies, procedures and practice guidance;
- Check what security systems are currently in place for protecting personal data. For example is personal data held in locked cabinets, or is electronic data held subject to password protection?;
- Ensure that you have a breach management procedure in place so you know what to do in the event of a breach.

Where do I seek further advice?
The ICO publish useful and up to date guidance in relation to all aspects of privacy law – including data protection – See https://ico.org.uk/for-organisations/data-protection-reform/

The Article 29 Working Party, a body representing data protection authorities across the EU, is issuing new guidance to help organisations comply with the GDPR – See http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Finally, please note that this guide is for general purposes only. For legal advice on which you can rely you should contact your Diocesan Registrar.

Key data – What to keep and for how long
Some guidance on how long to keep information which might include personal data is set out in Appendix 2 below.

March 2018

We are grateful to the Church of England for permission to use its material as a basis for preparing this guidance for the Scottish Episcopal Church

Appendix 1

Congregational Data Audit

Getting ready for GDPR

Review all your databases, email lists, spreadsheets, paper documents and other lists of personal data. If there are any issues, identify what you need to do. If action is not clear, then highlight questions needing further insight. New consent forms, privacy notices, and new or revised policies or procedures may need to be implemented to ensure compliance with GDPR.

Description	**Why is the data held and what is it used for**	**Basis for processing data (e.g. consent, 9(2)d[1])**	**Who holds the data and who can access it?**	**What security controls are in place?**	**How long is data kept for?**	**Is this covered by our privacy notice?**	**ACTION REQUIRED**
Example: *Gift Aid Declarations*	*For claiming Gift Aid*	*Legitimate Interest*	*Held by Gift Aid Officer. Also accessed by treasurer*	*On paper, kept in a locked filing cabinet*	*Seven complete calendar years after last gift claimed on the declaration*	*No – not yet written a privacy notice*	*Write privacy notice*

[1] Section 9(2)d is a special processing basis which allows religious (amongst others) not-for-profit bodies to process sensitive personal data 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.

Appendix 2

Guidance regarding Retention Periods for examples of material which may contain Personal Data

Basic record description ***Cleric and other ministers***	**Keep in congregation**	***Final Action***
Ministers' correspondence and other papers on routine administration	Current year plus 3 years thereafter	*Destroy*
Communicant and Adherent Rolls	Update at least annually and keep for 6 years from each annual review	Destroy
Vestries		
Planned giving schemes	Current year plus 6 years	Destroy
Gift Aid Declarations	Keep as long as they are valid plus 7 years	Destroy
Personnel records relating to lay employees not working with children and vulnerable adults: including annual performance assessments, disciplinary matters, job descriptions, training and termination documentation.	6 years after employment ceases	Destroy
Personnel records with contact with children and vulnerable adults including all documentation concerning any allegations and investigation regardless of the findings.	50 years after the conclusion of the matter	Destroy