A Parish Guide to the General Data Protection Regulation (GDPR)

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.

Explaining the jargon:
Personal data is information about a living individual which is capable of identifying that individual.
Processing is anything done with/to personal data, including storing it.
The **data subject** is the person about whom personal data are processed.
The **data controller** is the person or organisation who determines the how and what of data processing, in a parish usually the incumbent or PCC.

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 Commissioners 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 provide evidence. To do this there are a number of actions you should take, such as documenting the decisions you take about your processing activities and various other ways that show compliance – such as attending training, 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 your 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

© The Archbishops Council 2017

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.
Much of the personal data processed by a PCC or an incumbent 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 a parish context the most relevant being:-

- 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 electoral roll. In this case, the personal data processed is likely to be sensitive (by implication, if not directly, it relates to "religious belief") but it relates to members (or individuals in regular contact with it). It can be said to be a legitimate activity of the PCC, under the Church Representation Rules. Of course, if you wanted to share this data with another party, you would require the consent of any relevant individual(s). Please refer to the "Data Protection – Privacy Notice and Consent Form" guidance which can be found **here** for more details in relation to the lawful bases for processing personal data (including data which will be classed as sensitive).

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). As much of the data processed by a PCC or an incumbent in a parish is sensitive (relates to "religious belief), if consent is needed this will have to be explicit consent. 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, if 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).

For example, you cannot use the personal data from the electoral roll to send mail to individuals about events at the church without seeking consent first. If you have not obtained consent from individuals to do this, you will not be able to use their personal data in this way. You will need to keep records of all consents received and periodically review them (e.g. every 5 years) to ensure that they are still valid.

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 Readers rota or after service tea/coffee rota with other church members. In that instance, the information is shared with others in order to carry out a service to other church members. Of course, if it was intended to share the names outside the church for another purpose, then you would need to obtain consent.

Do I need to register (notify)?

The need for **data controllers** to register/notify with the ICO is removed under the GDPR (whether this will be the case under the new Government legislation remains to be seen). Nevertheless, 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.

However, the Data Protection Bill currently before Parliament allows the Secretary of State to make regulations requiring data controllers to: -

- Pay a charge to the ICO; and
- To provide information to the ICO to help the ICO identify the correct charge to be levied.

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. The amount as yet has not been finalised but will depend on the size of the organisation; it's annual turnover and the amount of personal data it processes. There will be exemptions from this fee and the ICO states that these will be similar to those under the current registration/notification regime, (so PCC's should remain exempt and parish clergy should also be exempt unless records of pastoral care discussions, (e.g. that relate to beliefs, relationships, opinions etc. rather than purely factual information)) are held on computer.

The ICO have stated that the new fee system will come into existence from 1 April 2018 but until that time data controllers should continue to register/notify as per usual. Once the new system is finalised the ICO has promised to let organisations know.

Will I need to have a Data Protection Officer?

Parishes are highly unlikely to be required to have a Data Protection Officer. 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 PCC and/or incumbent is unlikely to be classed as "large scale". However, you may wish to give one person responsibility for data protection issues, including providing support and guidance for others, such as the PCC and incumbent. This does not need to be a new member of staff, but rather added to the duties of an existing member of staff.

If a data protection issue comes up and you are unsure how to respond, you can contact your Diocesan Office, who will be able to help.

Is the incumbent a separate data controller from the PCC?

Yes - Each incumbent and each PCC is considered to be a separate data controller because they are separate legal entities who will be processing personal data.

What are the restrictions on the use of personal data?

The principles are similar to those in the DPA, with added detail at certain points and, as stated

above, a new **accountability** requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed separately.

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**
  Individuals continue to have a right to be given "fair processing information", usually through a privacy/data protection notice. 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.

You should note that in most cases you will no longer be able to charge for subject access requests. You will have 1 month from the receipt of the request 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 go to court.

- **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. The personal data on the electoral roll can only be deleted in accordance with the Church Representation Rules, examples include, if someone writes stating that they no longer wish to be included on the roll or a person no longer lives in the parish and no longer attends public worship there[1]. Information in parish registers cannot be deleted under any circumstances.

- **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 parishes**.

- **The right to object**
  Individuals have the right to object to processing in certain circumstances – e.g. If a parish 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 parish processing their data.

[1] The Church Representation Rules can be found here - https://www.churchofengland.org/about-us/structure/churchlawlegis/church-representation-rules/church-representation-rules-online.aspx

- **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.

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. If you 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. The GDPR sets the age when a child can grant consent at 16, (although the UK Government has proposed in its Data Protection Bill, currently going through parliament, that this be reduced to 13).

You should also 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.

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 and the individuals affected compulsory 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 in the parish note this deadline and seek the advice of the diocesan registrar about any suspected breaches without delay.

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, mitigation actions you plan to take, and how you plan to address the problem.

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. Of course, the UK is leaving the EU but this will be after the GDPR has already come into effect. Regardless, 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. How can consent be withdrawn?;
- Review all existing privacy/data protection notices and make sure that they contain the additional information that is required under the GDPR;
- Review all current procedures for dealing with requests from individuals – Are they adequate?;
- Review all retention periods and can such periods be justified? What is the procedure for deleting personal data, is it adequate?;
- Check whether any existing IT systems are capable of deleting or correcting personal data and handling requests from individuals;
- Is a Data Protection Impact Assessment needed to ensure compliance and appropriate security controls are in place? Review all current data protection policies, procedures and practice guidance;
- Check what security systems are currently in place for protecting personal data;
- Review existing breach management procedures and ensure that you know what to do in the event of a breach.

How do you ensure best practice when it comes to data protection?

The GDPR makes clear that the protection of data should be considered when deciding what personal data you need and how you are going to process it, including how you are going to collect

it, store it, share it and dispose of it. Data protection by design and by default means implementing appropriate technical and organisational measures to safeguard personal data, including limiting access to it; storing it in a pseudonymised format (a concept introduced by the GDPR and is, in essence, the processing of data in such a way that the data can no longer be linked to a specific person without using additional information, which is kept separately. This could be in the form of a unique reference number for each person) and ensuring data is only used and retained as long as necessary for the purpose for which it was obtained.

With the introduction of GDPR, it is vitally important that everyone is aware of and understands the importance of data protection. Privacy and data protection should be a core part of any project design and planning and not merely an afterthought relegated to world of data protection specialists and lawyers. It is important that those designing and developing tools and projects consider data protection in the early planning stages in order to ensure a compliant solution. For example, when creating new IT systems for storing or accessing personal data; developing policy or strategies that have privacy implications; embarking on data sharing projects; or using data for new purposes.

What is a Data Protection Impact Assessment (also known as the Privacy Impact Assessment) and when is it needed?

One way of ensuring compliance, is by carrying out a data protection impact assessment ("DPIA"). A DPIA will become compulsory under GDPR for certain types of processing, (e.g. the large-scale processing of sensitive personal data). Although it is unlikely that parishes will be processing sensitive personal data on a large scale, it is still worth considering carrying out a DPIA, at the start of a project, to ensure compliance and that appropriate security is in place.

A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project. The ICO has produced a 51-page Code of Practice on PIAs, (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf). As a minimum, the GDPR requires that a DPIA includes: -

- A description: of the processing activities and their purpose;
- An assessment: of the need for and the proportionality of the processing; and
- the risks arising and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect personal data and comply with the GDPR.

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/ and for smaller organisations here.

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

The National Church Institutions Records Management staff can be contacted via archives@churchofengland.org

Finally, please note that this guide is for general purposes only. For legal advice on which you can rely you must contact your Diocesan Registrar – his/her details can be found at your Diocesan Office or from the Diocesan website.

Key data – What to keep and for how long

How long to keep information, including Parish Registers, Electoral Rolls, Gift Aid declarations and a range of other information typically held by parishes can be found in the guide to parish record keeping *"Keep or Bin: Care of Your Parish Records"* which can be downloaded from the Church of England or Lambeth Palace Library websites at –
http://www.lambethpalacelibrary.org/content/recordsmanagement

GDPR – Checklist See Appendix one

Parish Data Audit - See Appendix two

Appendix one

GDPR Checklist

The General Data Protection Regulation (GDPR) will take effect in the UK in May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. Parishes must comply with its requirements, just like any other charity or organisation. Use this handy checklist to make sure you're on top of what you need to do.

The Checklist

		SORTED	ACTION NEEDED & DATE COMPLETED
1	**Data Audit**: Use our template to review your data processing. This is a great first step to identify the other action you will need to take. We've provided a template here.	☐	
2	**Privacy Notice:** Have you drafted a Privacy Notice. Our template and guide will help you.	☐	
	Is it available online for people to access?	☐	
	Is there a date set to review it?	☐	
3	**Do you need to get additional consent….** It's likely that many parishes will need to get additional consent from people as either consent has been assumed, or the evidence of the consent is no longer available. See our example consent forms here.	☐	
4	**Are your procedures up to date?** Data subjects (those people about whom you hold personal data) have the right to see what data is being stored about them, to make corrections where there are errors, or to ask for their data to be deleted. Do you have processes in place to meet such requests?	☐	
5	**What if you had a breach** Review your breach management procedures and ensure that you know what to do in the event of a breach. If you don't have any, you will need to develop them.	☐	

Appendix two

PARISH 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, legitimate interest)	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*	*Consent given by completion of declaration*	*Held by Gift Aid Officer. Also accessed by treasurer*	*On paper, kept in a locked filing cabinet*	*Six complete calendar years after last gift claimed on the declaration*	*No – not yet written a privacy notice*	*Write privacy notice*

© The Archbishops Council 2016