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 (DPA) 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 DPA.

There is also a new Data Protection Bill being considered in Parliament. The Bill updates data protection laws in the UK, supplementing the GDPR, implementing the EU Law Enforcement Directive, as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data. Further guidance will be issued once the Bill becomes law.

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 relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held.
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 in the current DPA and 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 DPA, 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 outlined below).

Two of the key aspects of the GDPR are the emphasis on individual rights, that is, the right of the individual to control what you are doing with their data, and an emphasis on transparency and accountability.

The following guidance explains the principles and requirements of the GDPR in more detail.

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, 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.

You can also use the ICO's 12 step guidance here: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Some Dioceses have also produced their own guidance, so check their website or contact your Diocesan Office.

How do you ensure best practice regarding 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 or storing it in a pseudonymised format (a concept introduced by the GDPR and means removing an individual's name and substituting a reference so that the data can no longer be linked to a specific person without using additional information, which must be kept separately); 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 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 a data sharing projects; or using data for new purposes.

Accountability – What is it and how do I comply?

One of the main changes is that the GDPR places a much greater emphasis on transparency, openness and accountability i.e. the documents you need to keep in order to show that you are complying with the legislation.

This means you cannot just state you are compliant; you must prove it and provide evidence. There are several 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, any action plans you may have or minutes of any formal discussions you have in the PCC regarding your implementation of GDPR.

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 "Individual Rights Requests". The lawful bases for processing personal data are broadly similar to the processing conditions contained in the DPA. You should review the types of processing activities you carry out and identify your lawful basis for doing so and keep a list – this will form what is called a Register of Processing Activities (ROPA) which is required for accountability and may need to be supplied to the ICO if requested:

- identify the various types of data processing you carry out;
- the purposes and legal basis for this processing and keep
- a written record of all your processing activities, security measures and data retention practices.

What lawful basis should I be using?

Article 6 of the GDPR sets out the various legal bases for processing personal data. In the parish context the most relevant include:

- Legal obligation, (e.g. a legislative requirement, such as processing gift aid applications or processing data in relation to the electoral roll);
- Legitimate interest, (e.g. general administration of church groups – rotas);
- Consent, (e.g. sending out a newsletter), (see below for more details);
- Contract (e.g. leases granted in relation to the church hall).

Some of the personal data processed by a PCC or an incumbent will be classed as sensitive (included in the "special categories of personal data" under the GDPR) because it reveals "religious belief " and additional requirements are in place if you process this kind of data. You will need to identify both an initial basis for processing (Article 6) and an additional basis (as listed in Article 9). In a parish context these additional bases are most likely to be:

- Explicit consent from a person; or
- Legitimate activity - where the processing relates to either members or former members or to individuals with whom there is regular contact but is not disclosed to any third parties outside the Church of England without consent

For example, the processing of personal data in relation to the application for enrolment on the church electoral roll requires that a person reveals his/her religious belief, which is sensitive ("special category") personal data. This is a legal obligation (Article 6) and a legitimate activity (Article 9), as it is a requirement under the Church Representation Rules. But if you wanted to share this data with another party outside the ambit of the Church Representation Rules, you would require the explicit consent of the **data subject** e.g. if you took a set of individual's details from the electoral roll and sent it to an insurance company, this would fall outside the application of the Rules.

Please refer to the "GDPR – Privacy Notice and Guidance" at www.parishresources.org.uk/gdpr for more details in relation to the lawful bases for processing personal data.

Consent

Please note consent is not an easy option under the GDPR. A more detailed definition of what is meant by consent clearly indicates the additional obligations you will need to consider. As a result, you should first consider other legal bases, and only use consent if nothing else applies.

Where you do rely on consent as the lawful basis for processing any personal data, for that to be valid under the GDPR, consent must be freely given, specific, informed, unambiguous and able to be withdrawn at any time. You therefore need to take a view on what effect either the refusal or withdrawal of consent will have on your processing activity.

Where data processed by a PCC or an incumbent in a parish is sensitive (reveals "religious belief" or any other special category data) if consent is needed this will have to be explicit consent, i.e. "clear affirmative action" in writing. Silence, pre-ticked boxes or inactivity will not constitute consent.

if you need to use consent you will have to make sure that the 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 and suffers no detriment by not providing consent. 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). Consent may be relatively straightforward to achieve where it is being sought for a single purpose, for instance, signing up to a newsletter but it will be potentially much more difficult to be demonstrate that you have complied with all the conditions that constitute valid consent where the personal data is to be used for multiple purposes, as you will need to ensure that consent is valid in relation to each purpose.

You will also need to keep records of all consents received and periodically review (e.g. every 5 years) them to ensure that they are still valid, and a separate list of refused or withdrawn consent, so you do not process the personal data of that person for that purpose.

Remember consent is not appropriate in every case. 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 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. This is a legitimate activity of a not-for-profit religious body, enabling it to carry out a function in relation to its members or those that have regular contact with it. Of course, if it was intended to share the information outside the Church of England for a new, unrelated purpose, then you would need to obtain consent.

Do I need to register with the ICO?

There is no longer a requirement for **data controllers** to register/notify with the ICO, but there is still a fee.

There will be exemptions from this fee like those under the current registration/ notification regime, so PCC's and parish clergy should remain 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. It is likely that the fee for all charities will be capped at £40, (which can be reduced to £35, if the charity pays by direct debit). Even if you are exempt from the fee, all the other data protection obligations still apply.

More guidance on this is available on the ICO website: Guide to the data protection fee | ICO

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" which is unlikely to be the case for a PCC or incumbent. 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. There are other restrictions relating to individuals' rights or overseas transfers of personal data - these are 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 must 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); who you will share it with 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 if they ask. 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 seek a judicial remedy.

- **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 means that although a person can request that his/her personal data be deleted immediately, if the purposes for which the data was collected still exist then unless it was given by consent and they are withdrawing their consent, you do not have to agree. 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 . Information in parish registers cannot be deleted under any circumstances.

You should check your parish retention schedules and make sure they are up to date. 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 (see the link in the right hand pane) at: http://www.lambethpalacelibrary.org/content/recordsmanagement

- **The right to restrict processing**

Individuals have the right to restrict processing of their personal data in certain circumstances, for instance they may consider the processing to be unlawful and rather than request erasure, they ask that it be restricted, i.e. that the processing is limited in some respect; or where there is a challenge as to its accuracy, you may need to restrict the processing until this is resolved. If processing is restricted, you can still store the data but cannot otherwise use it, and you should retain sufficient information to alert you to the restriction applied.

- **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 and an individual is not happy with this they have the right to object to the parish processing their data.

- **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 the 1998 Act.

Processing personal data about children – What do I need to do?

The GDPR brings into effect special protection for children's personal data, particularly in relation to online services, such as social networking. If you offer online services directly to children and rely on consent to collect their information, you may need a parent's or guardian's consent to lawfully use that data if they are under the age of 13 (this is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).

You should also remember that you must 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.

Where you are processing children's personal data that is not part of a online service there are no specific additional requirements. The GDPR does state that specific protection is needed where children's personal data is used for marketing purposes or creating personality or user profiles. Ultimately, you must consider the need to protect children's personal data from the outset and design systems and processes with them in mind.

What is a Data Protection Impact Assessment and do I need one?

One way of ensuring compliance is by carrying out a data protection impact assessment ("DPIA"). A DPIA is mandatory 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 that appropriate protection is in place.

A DPIA assesses the impact of any proposed processing operation, for example the use of data for new purposes, 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. 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 such as safeguarding or security measures to protect personal data.

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 it compulsory to inform the ICO and 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 in the parish note this deadline and consult with their Diocesan Office 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, mitigating actions you taken or plan to take, and how you will address the problem.

What should I do about my contracts with suppliers?

The GDPR makes it compulsory that all 3rd party suppliers who are processing data on your behalf must only do so through a contract, and the contract must specify what you are asking them to do. For example, if the PCC is using an external company to provide IT or mailing services, you should review the contract and ensure it is compliant, it must state that the processor must:

- only act on the written instructions of the controller (unless required by law to act without such instructions);
- their staff or others who are processing your data are subject to a duty of confidentiality;

- ensure the processing is done securely;
- only engage a sub-processor with your prior consent and a written contract;
- assist you to provide subject access and respond to other individual rights requests;
- assist you to make notification of personal data breaches;
- assist you to complete data protection impact assessments;
- delete or return all personal data if requested at the end of the contract;
- submit to audits and inspections; and
- tell you immediately if it is asked to do anything that may contravene data protection law (by you or any other party in relation to your data).

If you need legal advice in relation to any contract, please contact your diocesan registrar.

When does the GDPR come into effect?

On 25 May 2018. As a Regulation, the GDPR has become law in the EU Member States automatically without the need for local legislation. If the UK leaves the EU this will happen after the GDPR has already come into effect, and the Government has confirmed that it will be introducing its own data protection legislation which will incorporate the terms of the GDPR .

What are the penalties for not complying with the GDPR?

There has been much publicity about penalties under the GDPR. Enforcement and criminal penalties are left to each country to decide.

What is important is that there has been a substantial increase in the maximum possible fines which could be up to 4% of annual turnover.

Under the GDPR some examples of how this could be applied:

- For a failure to get parental consent where children's' personal data are collected 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 that fines are a last resort and are most likely to be used where organisations systematically fail to comply with the law or completely disregard it, particularly when the public are exposed to significant data privacy risks. The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. As with the DPA, 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.

Where can I get further advice?

The ICO publishes useful and up to date guidance and resources for data protection: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The National Church Institutions GDPR Working Group can be contacted via gdpr@churchofengland.org

We have a useful checklist available online at: www.parishresources.org.uk/gdpr or at Annex 1 of this briefing guide. As Annex 2, you can also find a copy of the Data Audit form.

Please note

This guide is for general purposes only. For legal advice you must contact your Diocesan Registrar whose details can be found from your Diocesan Office or from the Diocesan website.

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, legal obligation)	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*	*Legal Obligation*	*Held by Gift Aid Officer. Also accessed by treasurer*	*Paper declarations kept in a filing cabinet. Spreadsheet on PC.*	*Six calendar years after last gift claimed on the declaration*	*Yes*	*Password protect the spreadsheet*