GDPR - General Data Protection Regulation

A Guide for PCCs, Data Controllers and Data Compliance Officers.

This guide is intended to give the Clergy as the Data Controller, PCCs and Data Compliance Officers information on the new **General Data Protection Regulation (GDPR)**which comes into force on 25 May 2018.

This is not a definitive guide, as there is a wealth of information on external websites such as the ICO and the Church of England website. This document is designed to get PCCs thinking about the data they hold and what plans and actions they need to take to get compliant by the time the new regulation comes into being.

Further updates will be issued as more information becomes available and the Diocese will run training seminars in the autumn.

Each PCC will need a data controller and a data compliance officer . These are named individuals whose contact details appear on the consent forms and privacy notices .

The Data Compliance Officer will need to ensure that everyone in the PCC is aware of GDPR and that **everyone** takes responsibility for ensuring personal data is held securely and managed in compliance with the regulation. For clergy the role is one of data controller which means they will need to ensure overall compliance within their benefice(s).

PCCswill need to have clear simple policies in place regardingGDPR so there are stepsto take now to review all personal data held and its security.

In order to frame thinking, PCCs would do well to note the eight key rights of data subjects.
(Data subject is the individual whose personal datais held).

Eight Rights of Data Subjects

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The right to be informed. In order to ensure that personal data is processed fairly, PCCs must provide certain minimum information to data subjects, regarding the collection and further processing of their personal data. GDPR states that such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The right of access. Data subjects have the right to file a subject access request (SAR) and obtain from PCCsvia the data compliance officer, a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed. GDPR requires PCCs to respond to SARs with information, including details of the period for which the data will be stored (or the criteria used to determine that period) and information about other rights of data subjects. SAR must be responded to within one month.

The right to rectification. Data subjects have the right to require PCCs to correct errors in personal data held.

The right to erasure. Data subjects can request PCCs delete their personal data when the datais no longer needed for its original purpose, or where the processing is based on the consent and the data subject withdraws that consent (and no other lawful basis for the processing exists).

The right to restrict processing. This is a new feature of GDPR.In certain circumstances when personal data either cannot be deleted because the data is required for the purposes of exercising or defending legal claims or where the data subject does not wish to have the data deleted, the PCC may continue to store the data, but the purposes for which the data can be processed are strictly limited. E.g. A marriage certificate is a legal document and a data subject could not request the information is deleted.

The right to data portability. This is a new feature of GDPR. This permits the data subject to receive a copy of his or her personal data in a commonly used electronic format. E.g. Microsoft Word

The right to object. Data subjects have a right to object to processing of their personal data on certain grounds, in addition to the right to object to processing carried out for the purposes of profiling or direct marketing.

Rights in relation to automated decision making and profiling. Data subjects have the right not to be subject to decisions based solely on automated processing which significantly affect them. In reality for PCCs automated decisions are unlikely to be an issue but it is important to be aware of this right.

GDPR requires that personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Next Steps and Actions!

1. **Review all the personal dataheld.**
   - What data do you hold?
   - Why do you hold it?
   - Who has access to the data?
   - How is the data secured?

Carry out a Data Audit Exercise. Examine the various types of data processing carried out, identify the legal basis for carrying it out and document it.A simple table listing what you hold and why etc.will highlight where the gaps in your compliance are.This review process is a good way to capture all the data held and will be a good point of discussion at a PCC meeting to decide what needs to be done next.**See Appendix A for an example of an audit form.**

Who has access to the data should be clear. Only those that need to see it should have access.

2. **What policies and guidance do you already have in place?**

The Church of England website has a wealth of guidance policies on its Record Management page and these should be referred to by PCCs to form the basis of their own policies.

A clear policy for the retention of data is essential and personal data must be erased, without delay when:

- it is no longer necessary for purpose
- the data subject withdraws consent
- there is no longer any legal grounds to hold or process that data

Data cannot be kept indefinitely and PCCsmust remove data, when asked by the data subject. There are exceptions to this removal request:

- For vital interests or public interest
- Archiving in relation to public interest, scientific/historic and statistical research
- Exercise of legal claims

If you already have Data Protection and retention policies in placereview existing policies and think about where the data is collected and how its usage is defined. Do the policies need to be amended to comply with GDPR?

Note: A generic template for a GDPR policy will be issued for PCCs to adapt in forthcoming bulletins, but PCCs should start thinking about their own individual needs now to ensure all issues are captured.

3. **Where is your data held?**

Think about where your data is held and its security.

- Does it reside with 3rd parties on IT systems such as cloud suppliers, church members homes etc.?
- Of the data you hold about data subjects are these records electronic or paper based?
- How are theIT or paper system protected? (Passwords, encryption, lockable drawers, safes).
- Who needs authorised access to this data and information?

Any systems used to store or process data need to consider security as part of their implementation. You should only collect the data you need and keep it only as long as needed in order to fulfil an agreed purpose and then delete it.
This means PCCs need to think very carefully about what data they have on people, where it is and who has access to it. This will include the technology used and security in place. For example, data encryption would be one way in which computer data held can be secured.

4. Consent

Under GDPR, Consent cannot be assumed and must be laid out in simple terms in the forms individuals complete. Active consent is required and inactivity does not imply consent. Written consent is the recommended option because evidence of consent must be provided when asked by either individuals or the ICO. The person consenting must know exactly what the PCC propose to use their data for. If the data subject is under 16 then you must obtain parental consent. PCCs need to think about how they will handle requests to have data removed and how this would be done.

In order to achieve clear unambiguous consent from individuals to hold their data PCCs will probably need more than one consent form. One size will not fit all. Consent forms should clearly indicate how long the data will be held.

Children. GDPR sets the consent age at 16. Parental or guardian consent will be required if the person is under 16.

GDPR does not mean you cannot conduct "business as usual". What it does mean is that when you do hold individual's personal details, protecting these details is paramount andthe consent form must make clear what the data will be used for and for how long.

Practical Examples:

1. PCCs cannot collect data from parishioners to inform them about services and then use that data to fundraise. PCCs cannot profile certain people to target for fundraising. If you wish to use the personal information to contact individuals on fundraising the wording on the consent form must make this clear.

2. Information obtained from the Electoral Role cannot be used to direct mail individuals about events taking place unless you have explained this is what the information will also be used for and have the individuals explicit consent to contact them.

3. Personal data given for baptism, weddings and funerals cannot be used to mail individuals about services in the year unless the consent form makes it clear. In this case the form could say " we would like to keep in touch with you for the next two years about all our children's services or children's events in the parish. Do you consent to your data being held for this additional purpose?" A clear yes I consent box or no I do not consent tick box and space for a signature would also be required together with a process in place to remove the data after the two years have lapsed.

4. The Youth Worker stores the contact details of the under 16 youth group on an excel spreadsheet on his/her laptop. In this example the consent would be needed from the parent, and the reason it is collected is so the youth worker can communicate about events by email or phone. The PCC should however be aware that personal data is stored on laptop, who has access to it and what security measures are in place on the device to secure the data.

Under GDPR consent can be withdrawn at any time by individuals andPCCs must act on these requests immediately and remove the data/paper files for their records.

Note: Further information on consent and wording for consent forms will follow in the next bulletin but please start to identify now all the consent forms and processes you have for consent and deletion or removal of consent.

5. 3rd Party Risk

Is data shared with people/ organisations outside of your PCC?

If any personal data you hold is “processed” by another company you would be wise to confirm the company complies with data protection and GDPR. For clarity, if they are breached and a complaint is upheld, you as the data controller (owner) remain equally liable. You will also need to review contracts held with companies that process data on your behalf. It is the PCC’s responsibility to ensure the “processor “processes the data you give them, in accordance with GDPR.

Contracts with third parties that have access to the personal data you hold should have a statement within the contract confirming they comply with GDPR. Companies must demonstrate that they have the appropriate policies and security measures in place to protect the data. In these circumstance the PCC is the controller of the data and the 3rd Party Company is the “processor” of the data.

Practical Examples

1. IT databases, IT systems.
2. CCTV. If that is managed by a third party off site and they have the recordings or have access to it. PCCs will need to obtain written confirmation that their company complies with the new GDPR rules. Full information on CCTV is in Appendix B

6. Subject Access Requests (SAR)

Individuals have the right to request a copy of all the personal data held. This means providing copies of all electronic and paper documents that contain their details or reference to them.

Personal data also includes footage held on a CCTV system, where the individual is the focus of the footage and/or they are clearly identifiable.

You will also need to provide some additional information to peoplemaking requests, such as your data retention periods and the right tohave inaccurate data corrected.

The Data Compliance Officer (PCC Secretary is the obvious choice, but it could be a named employee) who will be the contact for any Subject Access Requests.

If the SAR request is valid and permissible the data has to be supplied within 30 days of the request being deemed valid. You should therefore ensure that the PCC and the Data Compliance Officer have procedures in place to comply with these requests promptly. Charging for requests is generally not permitted. Excessive requestscan be charged for or refused. If you want to refuse a request, you willneed to have policies and procedures in place to demonstrate why therequest meets these criteria.

What to do if you identify a breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

If your data is breached and the data breached could cause material or emotional harm to the individual you have just 72 hours to declare it to the ICO and if severe then also the data subject. You need to do this from the point that you are aware. Note: If the data is breached but is encrypted, i.e. it cannot be accessed by anyone and therefore will not cause harm you do NOT need to declare the breach.

Practical Example
If a spreadsheet containing names and addresses of people under 16 was accessed by someone unauthorised that is a breach. For example, allowing someone other than the approved members of the PCC to view personal data, is a breach. Other breaches such as Malware (IT) attacks, equipment theft, ID credentials compromised are equally relevant.

7. Fines

The fines that can be imposed due to non-compliance depend on the severity of non-compliance. Examples of fines are:

- A warning in writing in cases of first and non-intentional noncompliance
- A fine up to 20 000 000 EUR

8. Finally - Practical To Dos and Tips

PCCs must:

- Put GDPR on the PCC Agenda, make everyone aware.
- Appoint a data compliance officer. This will be either a PCC member (PCC Secretary) or employee who will take overall responsibility for compliance with the Data Protection Act/GDPR.
- Consider which members of the church hold personal data. This will likely include clergy, administrators, directors of music, youth workers, Treasurers PCC Secretaryetc. Consider what access each person requires to the records.
- Confidential information in hard copy should always be held in a locked, fireproof container. Access to the information should be restricted to only those who have a legitimate need to view or use it.

- Confidential information on computer should be encrypted and protected by a password which should only be known to those who need to have access to the information.
- Maintain up to data security on computers. (Anti-virusetc.)
- Begin to think about what personal data you have and where it is and review it. When members of the congregation leave what information needs to be legitimately retained.
- Understand what risk is posed to individuals should data be accessed via an unauthorised means.
- Think about what to do to secure data to protect yourselves and the individuals
- What data can you erase, and how best could you do that?
- Do you need to get consent from those you mail/ email?
- If you use third party services such as email and CCTV how is the data managed and stored.
- The GDPR does not come into force until May 2018 but the existing Data Protection rules still apply and PCCs must comply and protect individual's personal data.

Further updates will be issued as more information becomes available.This will include information on consent forms and policy documents.

Appendix A – Data Audit Exercise.

Personal Data Audit

All databases, spreadsheets, paper documents and other lists of personal data held by the Parish of XX are listed below.

Description of the personal data held	Why is the data held and what is it used for?	What consent form is in place?	Does the consent form cover all activities the data is used for?	Who holds the data and who can access it?	What security controls are in place?	What is the retention & deletion procedure for this data?	If there are any issues, what steps are being taken to make the data complaint with GDPR

Highlight all questions unanswered or answers where there are issues. All these issues/queries will require action. New consent forms, new policies or procedures may need to be implemented to ensure compliance with GDPR.

Appendix B

CCTV in Churches.

There must be a legitimate reason for having CCTV installed and for Churches, CCTV should be used as a crime prevention tool. Churches install CCTV to reduce the threat of damage to property and to protect the building by acting as a deterrent. The recorded information from the CCTV can be used in the event of a crime being committed to the police and courts to bring a successful prosecution.

If CCTV captures images of people that are then personally identifiable you will need to register with the Information Commissioner's Office (ICO).

Registration can be accessed used this link. https://ico.org.uk/for-organisations/register/

Things to consider and implement.

The need for CCTV must be documented before purchase.

The risks to a person's privacy by having CCTV must be identified and documented.

The ICO Code of Practice recommends carrying out a privacy impact assessment to assess the extent to which CCTV is required. A simple table identifying the need, the risk,where it is required and at what times and actions should be sufficient.

A CCTV system must have the ability to be switched on or off. Do the recordings need to be continuous? If yes, the reasons should be documented.

The CCTV system should have the ability to stop capturing either footage and/or sound recordings both of which should work independently of each other. Capturing both could be deemed excessive and you need to demonstrate clearly the reasons for recording both and what legitimate grounds you are relying on to justify this.

If you capture sound recordings are they obtained when it is absolutely necessary and for this specific purpose? CCTV surveillance systems should not normally be used to record conversations between members of the public or members of staff as part of a working environment. Recording conversations is highly intrusive and unlikely to be justified.

The purpose of holding the data is to identify individuals performing criminal activity so the recordings should be of sufficient quality and be easily accessible if requested by the police. There should be a regular check that the date and time stamp recorded on images is accurate. You should also be able to access recordings easily in order to comply with a subject access request or police investigations.

All recordings from the CCTV system must be securely stored and only allow authorised persons from the PCC should have access to them and the controls and protocols should be documented.

There should be sufficient security safeguards in place to prohibit interception and unauthorised access. The CCTV system should be encrypted.

Information on the retention and deletion of the recordings should beincluded in your GDPR/Data Protection Policy

Personally identifiable information about a data subject must be 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.

Example

Images from a CCTV system installed to prevent fraud at an ATM machine may need to be retained for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement

In contrast, images from a CCTV system in a church may only need to be retained for a short period because incidents will come to light much more quickly. However, if a crime is reported to the police, the images will need to be retained until the police have time to collect them. Therefore your retention policy needs to take account of this.

Good signage should be in place to let people know they are in an area where a surveillance system is in operation and what their rights are and who to contact to access their recordings/images.

There are fines for any serious breaches of the act so please ensure that clear signage, goodadmin control of the data and security of the data is in place.

Subject access requests apply equally to CCTV recordings as to any other recorded data. Individuals therefore have a right to request a copy of their personal data, which includes footage held on a CCTV system, where they are the focus of the footage and/or they are clearly identifiable. Appropriate systems and procedures should be in place to comply with these requests promptly within 30 days.

The company providing the CCTV must comply with GDPR if they are holding any of the data.If the CCTV provider has access to the recordings the contract should reflect that they have the appropriate Data Protection controls in place. If the data is held only by your equipment and the installation company cannot access it then this is not required. Do not consider using any provider if the data cannot be encrypted and password protected

Finally, the installation of CCTV requires faculty permission from the DAC.