THE CHURCH OF ENGLAND BIRMINGHAM

General Data Protection Regulations (GDPR)

Key messages for Parishes

Please note:

This presentation is based on information as at March 2018

This presentation is guidance only and is our interpretation of the law and should not be read as legal advice

THE CHURCH OF ENGLAND BIRMINGHAM

Contents

- What is personal data
- What is Data Protection
- What is GDPR
- Terminology
- GDPR Principles
- Consent (or not)
- Stages in becoming compliant
- Practical steps and tips
- Questions

THE CHURCH OF ENGLAND BIRMINGHAM

What is personal data?

Personal data is defined as:

Any information about a living individual which is capable of identifying that individual.

Special catergories of personal data are defined as:

Any information relating to an individual's racial or ethnic origin, political opinions, ***religious beliefs***, trade union membership, physical or mental health or condition, sex life, alleged or actual criminal activity and criminal record.

THE CHURCH OF ENGLAND BIRMINGHAM

What is Data Protection?

Data Protection is about **avoiding harm** to **individuals** by misusing or mismanaging their personal data.

- Only collect information for specific purposes and don't then use it for other purposes
- Only collect what you need for the specific purpose
- Keep it accurate and up to date; and safe and secure
- Process information lawfully and allow subject access in line with the Act.

THE CHURCH OF ENGLAND BIRMINGHAM

What is GDPR?

It is the **General Data Protection Regulation**, which supersedes the Data Protection Act on 25th May 2018. The key changes from the current law are to strengthen rights of individuals and place more obligations on organisations in looking after personal data.

In order to comply with the **new** law:

- You must have a legitimate reason for processing data
- Consent must be freely and unambiguously given and can be just as easily withdrawn
- Data Processing activities must start with "privacy by design and default".

THE CHURCH OF ENGLAND BIRMINGHAM

What is GDPR? … continued

- Subject Access Requests – will include how you process and share data not just what you hold and you'll have less time to respond
- Subjects can request data deletion – "the right to be forgotten", though only in certain circumstances
- There will be mandatory breach reporting
- Data processors will be held liable
- You must be able to demonstrate compliance with GDPR through documentation
- While the ICO say it is a last resort, the potential fines are much greater than at present – up to 4% of annual global turnover or €20m

THE CHURCH OF ENGLAND BIRMINGHAM

GDPR / Data Protection Terminology

- The **data controller** is the person or organisation who determines the how and what of data processing.
- The **data subject** is the person about whom personal data is being processed.
- A **data processor** is the person or organisation who takes an action with the personal data you control – this might be a 3rd party acting on your behalf ie Payroll service
- **Processing** is anything done with/to personal data, including storing and deleting it.
- The **Data Protection Officer (DPO)** is a specific role which will be a legal requirement for many organisations including large church bodies such as dioceses. You are recommended to have a data compliance officer to keep data protection on your PCC agenda and ensure compliance

THE CHURCH OF ENGLAND BIRMINGHAM

Why does GDPR affect us?

- Applies to all **data controllers**
  - An individual or body which alone or with others determines the purposes and means of the processing of personal data

Incumbents are their own body and so are a separate **data controller**.

THE CHURCH OF ENGLAND BIRMINGHAM

GDPR Principles

- **Lawfulness, fairness and transparency** – as with Data Protection
- **Purpose limitation** – only collect for specific purposes and then don't use it for other purposes
- **Data minimisation** – only collect the data you need for the purpose you are using it
- **Accuracy** – as now, keep it up to date!
- **Storage limitation** – don't keep it for longer than you need to fulfil the purpose
- **Integrity and confidentiality** – keep it safe and secure e.g. encrypted if on a laptop or mobile phone.
- **Accountability** – you must be able to prove you have complied with the above.

THE CHURCH OF ENGLAND BIRMINGHAM

Can I still process personal data? Do I need consent?

- You can process personal data **without consent** where it is necessary:
  - For the performance of a **contract**
  - For compliance with a **legal obligation**
  - To **protect the vital interests** of the data subject or another person
  - In the exercise of **official authority** or in the **public interest**
  - For the purposes of **legitimate interests** you are undertaking
- ONLY if NONE of the above apply do you need consent.

THE CHURCH OF ENGLAND BIRMINGHAM

What do I need consent for?

- Non-physical communications – even if you are covered under one of the exempt categories
  - Email
    - BCC Emails
    - Unsubscribe option needs to be clear
- Sharing the information with third parties. Including Incumbent & diocese.

THE CHURCH OF ENGLAND BIRMINGHAM

Becoming compliant

▶ don't panic!

If you are complying with the Data Protection Act then you are well on the way to GDPR compliance

The Checklist

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 at *www.parishresources.org.uk/gdpr/dataaudit*

2 **Privacy Notice:**
Have you drafted a Privacy Notice. You can find guidance and a sample template at: *www.parishresources.org.uk/gdpr/privacy*

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 at *www.parishresources.org.uk/gdpr/consent*

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. See our guide at *www.parishresources.org.uk/gdpr*

Data audit

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

Keep this as a working document (and on the agenda at PCC)
to ensure that actions are completed

Privacy notice

- Needs to be available on your website (if you have one) or otherwise from the parish office.
- Should be referred to on all communications relating to personal data collection or processing
- Should include:
  - Identify the data controller
  - Purpose and what form the processing will take
  - The legal basis for processing of data
  - How/if/with whom data may be shared
  - How long data will be held
  - The data subjects rights – including the right to withdraw consent
- Review it

Additional consent

If you cannot justify not requiring consent under the exceptions you will need consent.

- Consent must be explicit
- Church membership forms or Electoral Roll forms are for that stated purpose only and the information supplied can only be used for making postal communications
- The main additional consents you may require are
  - to keep people informed about news of the parish via email
  - to include details in a parish directory
  - to share contact details with the diocese
- Data subjects should be informed they can withdraw consent at any time

Rights of data subjects

- Subject access requests
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to object

In case of a data breach

- The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

- You will need a policy on this which covers
  - Containment & recovery
  - Assesing the risks
  - Notification of breaches
  - Evaluation & response

Practical steps and tips

- Put GDPR on the PCC Agenda
- 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-virus etc.)

Practical steps and tips

- 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.
- Keep records of actions taken.
- Information Commissioner's Office (ICO) Registration

THE CHURCH OF ENGLAND BIRMINGHAM

Questions

Where to get more information

- Parish Resources: www.parishresources.org.uk
- Information Commissioner's Office website: www.ico.gov.uk
- The diocesan registry is available for queries
- https://www.churchofengland.org/more/libraries-and-archives/records-management-guides

Please note:

This presentation is guidance only and is our interpretation of the law and should not be read as legal advice