Data Controller's Guide to GDPR

PARISHES

The Representative Church Body, Dublin.

Parishes Guide to GDPR

The Church of Ireland, its officers and employees, are committed to delivering the highest standards of governance, risk management and compliance in relation to the processing of personal data, in a manner compatible with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (EU) 2016/679.

Personal data is information about a natural living person (data subject) which can identify them. It includes name, address, date of birth and online identifiers (e.g. IP address, Twitter handle).

Sensitive personal data (special category data) includes information about a data subject's religious beliefs, health, sex life, criminal convictions and all information relating to children and adults at risk. Sensitive personal data can only be processed with consent.

Role of the joint data controller:
The Church of Ireland has four data controllers, known collectively as joint data controllers.
Each controller has agreed areas of responsibility as illustrated below.

	Representative Church Body (General Synod)	Diocesan Councils	Parishes	Bishops	
				Individual	Collectively / as House of General Synod
Controllers	• Committees of: Representative Body General Synod Standing Committee • Standing Committee • RCB Library • Theological Institute • Employees, contractors and volunteers	• Diocesan Synod • Diocesan Secretaries • Members of Diocesan Synod and Council • Employees, contractors and volunteers	• Clergy • General Vestry • Select Vestry • Employees, contractors and volunteers	• Bishop's Office • Patron • Clergy • Employees, contractors and volunteers	• Selection Conference • Protocols
Processors					

- Joint controllers act with equal power. At times they may need to work together with regard to exercising the rights of the data subject. Therefore it is useful to designate a contact point, e.g. David Ritchie (Chief Officer and Secretary), is the contact point for the Representative Church Body (General Synod).

- Each controller is responsible for determining the purpose for which, and the manner in which, personal data is, or will be processed. For example, the parish has determined that personal information is required and will be processed with consent. The data processor (e.g. the incumbent) will process this personal information on behalf of the controller (the parish).

- Each controller must be able to demonstrate compliance with the six data protection principles:

  1. Lawfulness, fairness and transparency: determining that personal data will be collected, the legal basis for doing so (e.g. consent) and the type of personal data to be collected (e.g. name, address, phone number)
  2. Purpose limitation: collected for specified, explicit and legitimate purposes
  3. Data minimisation: adequate, relevant and limited to what is necessary
  4. Personal data is accurate and kept up to date
  5. Personal data is kept only for as long as completely necessary
  6. Personal data is processed safely and securely, with appropriate safeguards in place

Becoming Compliant: Responsibilities of Parishes

As a (joint) data controller, the parish is responsible for meeting the requirements as laid out above. Each controller is also responsible for supporting data processors, those processing personal data on behalf of the controller, through regular communication, facilitating attendance at data protection training and providing clear instructions about how data should be processed. The regulation also requires the controller to put in place appropriate technical and organisational measures to implement data protection principles and protect individual rights. Accountability obligations are ongoing; therefore it is necessary to review, and as required, update the measures the controller has put in place.

There are a number of steps that should be followed by the parish (controller) to become compliant. The implementation of these activities should be in partnership with those processing data on behalf of the parish (e.g. incumbent; parish secretary etc.).

1. **Communications & Training:** The controller should have a good understanding of data protection requirements and actively communicate these requirements with those processing personal information on their behalf (data processors). The controller and processor/s (as necessary) should attend relevant data protection training and should commit to attending refresher training on an annual basis.

Tips: Add data protection as a reoccurring agenda item at regular governance meetings e.g. select vestry. Attend refresher training at least once per year. Review processing activities regularly to monitor compliance. Ensure data protection implementation becomes 'the way things are done'.

Resources: There is a suite of resources and templates available from the Parish Resource section of the Church of Ireland's website (www.ireland.anglican.org/parish-resources). These are regularly updated. The Representative Church Body's (RCB) Data Protection Officer (Rebekah Fozzard) can provide communication and training material and, upon request, may be available to deliver controller and processor training at a national level.

2. **Understand the personal information processed**: Known as a data audit, this is a thorough examination of all the personal data processed[1] on behalf of the controller, across the entire scope of the controller's areas of responsibility. The following questions are useful to ask:

   a. What personal data is held?
   b. How was this information obtained? e.g. directly from the individual or from a third party
   c. Why is the personal data being held?

[1] Data processing includes any operation or set of operations which is performed on personal data. For example, the collection, recording, organising, storing, retrieving, using, disclosing, restricting, archiving, deleting of personal data.

d. Which lawful basis[2] is being used to process the personal data?
e. Does the reason the personal data was collected still apply?
f. Who has access to the personal information?
g. Is the personal information held safely with restricted access?
h. When should this personal information be archived or destroyed securely?

Note: If special category data is being processed, both a lawful basis for processing and a special category condition[3] for processing must be identified.

Tips: Identify personal information that is no longer required and develop a plan to archive or delete as soon as possible. Develop a systematic process to review personal information on an annual basis. Be aware that some personal information must be held for legislative or constitutional reasons. Remember the need to preserve the history of the Church of Ireland.

Resources: The Representative Church Body Library will provide guidance with regards to archiving information. They can be contacted at: library@ireland.anglican.org.

3. **Develop, update and implement policies:** Each controller has to demonstrate that processing has been done in a fair and transparent manner. A controller is also required to provide information to data subjects explaining the purpose of processing personal data, the type of personal data being processed, who this information is shared with, how long the data will be held and how it is protected. This is usually provided through policies and notices.

Policies required include:

a. **Data Privacy Notice** – explains to data subjects how their personal data is processed by the controller. This document should be publically available
b. **Website Privacy Notice** – informs online visitors how their data is collected and used. This notice should be available online on the controller's website
c. **Data Protection Policy** – outlines internal responsibilities, procedures and protocols in relation to legally processing[4] (also see footnote 2) and safeguarding personal data. This needs to be provided to all those processing data. This document is for internal use
d. **Retention Policy** – outlines statutory, constitutional and best practice requirements for keeping, archiving and destroying personal data
e. **Internal Security Policy** – outlines the security measures that should be implemented by when processing personal data e.g. passwords, encryption
f. **Acceptable Usage Policy (IT & Social Media)** – outlines internal responsibilities to safeguard personal data when undertaking web-based activity, storing data in the 'cloud' and using social media safely

[2] The six lawful ways to process personal data are: Consent, Legitimate Interest; Public Interest; Vital Interest; Contractual Necessity and Compliance with a Legal Obligation. One lawful basis must always apply.
[3] Special category condition for the Church of Ireland: as a not-for-profit body with a religious aim, processing is carried out in the course of our legitimate activities on the condition that the processing relates solely to members or former members of the body or to persons who have regular contact with it; and that personal data is not disclosed outside this body without consent.
[4] If Legitimate Interest is relied upon, a balancing test must take place and the results documented. This needs to be available upon request.

Tips: Monitor the implementation of the policies and notices and actively address any issues that may arise. Ensure processors are very clear how to meet their responsibilities. Personal data can be kept indefinitely for a number of reasons[5] once appropriate safeguards are in place.

Resources: There are draft policy templates available on the Parish Resource Section of the Church of Ireland Website or from the RCB's Data Protection Officer.

4. **Examine and update any forms that collect personal information:** Any form containing a request for personal data needs to have a data protection statement included. This ensures that the collection of data has been done in a fair and transparent manner. It also ensures consent, for example, is valid. Each form should outline the rationale and legal basis for processing personal information.

Tips: Identify all forms that collect personal data during the data audit and ensure they are compliant. Check for online forms as well as hard copies.

Resources: A data protection statement may read along the lines of:

> In line with data protection regulations, we are committed to protecting the personal information we hold on you. By completing this form, and by providing the information requested, you are giving us permission (consent) to process your personal information for the purpose of ……. We will keep your personal data safe and secure, and will retain it only for as long as is necessary. If you have any questions about how we process your personal data or are unhappy with how we process personal data, please contact Joe Bloggs at joe.bloggs@parishoffice.ie

(Note: information in yellow to be edited as required).

5. **Develop and implement procedures**: Controllers have a legal obligation to address the rights of data subjects within legally defined parameters. A data subject can exercise any of their rights at any time[6]. Procedures should be developed and implemented across all areas of responsibility. Processors must be trained in how to implement the procedures correctly and be aware of their responsibilities. Regular evaluation of the procedures is advised.

Procedures to be developed include:

a. **Data Breach** - outline how to respond, contain, communicate and prevent a data breach[7]
b. **Data Protection Impact Assessment** – this risk assessment is only required if the data controller undertakes any systematic monitoring of a public area e.g. CCTV in place
c. **Responding to data subject exercising their rights** - each procedure should include a step-by-step guide outlining how a request will be assessed, responded to and recorded. Timeframes of one month to respond in full usually apply [8]

[5] Reasons include public interest archiving, scientific or historical research or statistical purposes.
[6] Data subject rights include the right to: be informed; access a copy of their personal information; have personal data corrected; have personal data erased; restrict or object to processing; data portability; rights in relation to automated decision making
[7] A Data Breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It can include sharing information without permission, losing data, deleting data in error or data being stolen.

For example:

a) The right to have personal data erased (the right to be forgotten) can be made verbally or in writing and the data controller has one month to respond. This right is not absolute and only applies in certain circumstances.

Or

b) A Subject Access Request (request a copy of their personal information). This is where an individual has the right to obtain confirmation that their personal data is being processed, receive a copy of their personal data and other supplementary information as outlined in the data privacy notice (e.g. purpose of processing; type of personal data held retention periods). There is one calendar month to respond and no fee can be charged.

Tips: An individual is only entitled to their own personal data and not to information relating to other people. All data breaches must be recorded locally and serious breaches must be reported to the Data Protection Authority. All areas which fall within the remit of the controller are subject to a Subject Access Request. Renew procedures regularly.

Resources: Templates and further information on all areas are available from the Parish Resource section of the Church of Ireland website. The RCB's Data Protection Officer is available to support as required.

6. **Risk Management:** Controllers are responsible for managing risk and ensuring personal information is being processed lawfully. Risk is increased when personal data is shared from one controller to another or from one processor to another. To mitigate this risk it is recommended the following activities take place:

a. Identify when personal data flows outside e.g. to the accountant; the website provider; diocesan magazine. Ensure this is done in a safe and secure manner
b. Ensure contracts and agreements include a data protection clause regarding the protection of personal data
c. Before personal information is shared outside the European Union, ensure there is an adequate level of protection in place (RCB's Data Protection Officer can advise). Otherwise a data sharing protocol will need to be developed
d. Have a clear governance structure in place with delegated responsibility as required
e. Take responsibility for information governance
f. Ensure policies and procedures are signed off and understood by those implementing them
g. Have an appropriate system in place for the destruction of confidential waste, and obtain destruction certificates as necessary

Tips: Request proof of compliance from third party providers. Review their privacy statement, terms and conditions. Be satisfied that the personal data is being treated appropriately.

Resources: The RCB's Data Protection Officer is developing data sharing protocols to assist with the transfer of personal data across joint data controllers, across the Island of Ireland, across Europe and outside the European Union.

[8] In very limited circumstances, a SAR request can be extended by two extra months. In this case, the data subject needs to be given a full explanation why the extension within one month of the original application.

Final Comments

- Get to know and understand data protection and become familiar with the resources available
- Agree the ‘face’ of data protection. Who will be managing data protection compliance on a day to day basis?
- Follow the data protection principles and know exactly what personal data is being processed, why it is being processed and the legal basis for processing it
- Maintain a record of all processing activities – this will help demonstrate compliance
- Put measures in place to be and to remain compliant
- Manage the rights of individuals and data breaches
- Communicate with the data processors
- Remember to ‘phone a friend’ - there are four joint controllers for the Church of Ireland - work together.
- The RCB’s Data Protection Officer, Rebekah Fozzard, is available to help and provide advice as required. She can be contacted at: dataprotection@rcbdub.org / 003353 1 4125660