THE REPRESENTATIVE CHURCH BODY

Preparing for the General Data Protection Regulation

Your Readiness Checklist

If you have any queries, please refer to FAQ guide saved on Parish Resources section of the RCB's website

Step by Step Guide

1. Agree who is in charge of personal data in your Diocese/Parish

a. Appoint a Data Controller. This is the person who decides how personal data is collected and managed

b. Ensure they know that they are responsible for supporting GDPR compliance at a local level. They should:

Undergo training and up skilling as required

Become familiar with the Data Protection Commissioner (ROI) and Information Commissioner Office (NI) websites

Regularly visit the GDPR section under Parish Resources on the RCB's website

c. Publish the Data Controller's contact details on your notice board; website and other places visited by your data subjects

Outputs:

- Set up a GDPR file (online or filing system) to save all GDPR related documentation - this will be very useful if you are ever audited. The Data Protection Commissioner will expect to be able to see evidence immediately if they visit
- Include details of the Data Controller and how the decision to appoint them was made
- Share details of the Data Controller on noticeboards, on the website and in your parish notes
- The Data Controller should have full access to the GDPR file and should, with support, implement the following activities.

2. Review all the data you hold

a. Go through all the online and paper files to identify the personal data you hold (data audit template on Parish Resources section of the website)

b. Break the personal data into categories of personal data (e.g. gift aid; volunteer; group lists) and data subjects (e.g. parishioners; clergy)

c. List each type of personal data included e.g. name, address, bank details, photos

d. List the source of the personal data – e.g. where you collected it from

e. For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, legitimate interest

f. If special categories of personal data are collected, say what they are e.g. children's data

g. List the legal basis on which special categories of personal data is collected and retained e.g. explicit consent

h. For each category of personal data, list the period for which data will be held. As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place. Be aware of wider church and diocesan guidelines on retaining historical records

i. Identify actions that are required to be GDPR compliant e.g. delete data where you don't need to hold onto it; seek consent where it doesn't exist

Outputs:

- Record the process you undertook to review your documents and save this into in your GDPR file
- Document any actions arising from this review e.g. deleting old PPS / NIN numbers you have found; sending historical records to the RB Library to be archived

3. Managing Consent

a. If you use consent as your legal way to process data, you need to be able to show that all personal data is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data

b. If personal data you hold on the basis of consent does not meet the required standard under GDPR, have you re-sought the individual's consent to ensure compliance with GDPR? E.g. people now have to opt-in, rather than opt out; permission is required to use photographs; record people; share personal details and so forth

c. Have you got procedures in place to demonstrate that an individual has consented to their data being processed? If not, you need to develop a procedure

d. Are there procedures in place to allow an individual to withdraw their consent to the processing of their personal data? If not, you need to develop a procedure

e. As required, seek consent from parishioners, employees, others to process their personal data. Templates available from the Parish Resources section of the website. Remember, each individual's personal data belongs to them; so each person needs to give permission to use their data

Outputs:

- Ensure you have a procedure on how you get consent and how, as required, people can withdraw their consent
- Develop your consent form and save a template of this form in your GDPR file
- Issue a consent form to anyone whose personal data is used by the Data Controller
- Save returns in your GDPR file (locked; password protected)

4. Children's Personal Data

a. This is special category data. You need to have a procedure in place to get consent of a parent / legal guardian where required. Much of this may be done within Safeguarding Trust but where not; please ensure you have a procedure

b. Develop consent form for those aged 16years or younger (ROI) and 13years or younger (NI)

c. Document your procedure for getting explicit consent to use children's data

d. Issue consent forms as required to parent/legal guardian

Outputs:

- Ensure you have a procedure on how you get consent
- Save procedure in GDPR file
- Issue consent forms where you are using Children's data and existing consent does not exist
- Save returns in your GDPR file and keep very safe and secure; not to be shared.

5. Relying on Legitimate Interest

a. If legitimate interest is a legal basis on which personal data is processed, you need to do the legitimate interest test. The test is outlined in full in the FAQ guide on the Parish Resources section of the website and includes:

Ensure that there is a valid legitimate interest to processing the data

Ensure processing data is necessary

Ensure processing is not prejudicial to or overridden by the rights of the individual

b. You need to develop a legitimate interest policy which should include:

Evidence that you have done the test

Details that you understand your responsibility to protect individuals' interests

Justification of your decision for choosing legitimate interest

Evidence that you are only using individuals' data in ways individuals would reasonably expect

Measures to keep this data safe

Outputs:

- Do the legitimate interest test
- Develop a legitimate interest policy including results from test
- Save policy in your GDPR file
- Share the policy on your website or your noticeboard

6. Subject Access Requests

a. Do you have a documented policy/procedure for handling Subject Assess Requests? (see Parish Resource section of the RCB website for further information)

b. Are you able to respond to a Subject Access Request within one month?

c. Are procedures in place to provide individuals with their personal data in a structured, commonly used format?

Outputs:

- Develop a procedure for handling Subject Access Requests (SAR)
- Save the procedure in your GDPR file
- Document all occasions when you have to follow this procedure including all actions undertaken

7. Deletion and Rectification

a. Are there controls and procedures in place to allow personal data to be deleted or rectified? (where applicable)

Outputs:

- Develop a procedure for how you will delete or rectify personal data as required
- Save the procedure in your GDPR file
- Document all occasions when you have to follow this procedure

8. Right to restriction of processing

a. Are there controls and procedures in place to halt the processing of personal data where an individual has, on valid grounds, sought the restriction of processing?

Outputs:

- Develop a procedure for how you will restrict processing personal data if someone requests it (where possible)
- Save the procedure in your GDPR file
- Document all occasions when you have to follow this procedure

9. Right to object to processing

a. Have you a procedure in place to halt the processing of personal data where an individual has objected to the processing?

Outputs:

- Develop a procedure for how you will stop processing personal data if someone requests it (where possible)
- Save the procedure in your GDPR file
- Document all occasions when you have to follow this procedure

10. Retention and Accuracy of personal data

a. Is personal data only used for the purposes for which it was originally collected?

b. Is the personal data collected limited to what is necessary for the purposes of which it is processed?

c. Have you a procedure in place to ensure personal data is kept up to date and accurate and where a correction is required, the necessary changes are made without delay?

d. Have you developed a retention policy to ensure data is held for no longer than is necessary (or kept; archived as appropriate)? Ensure rules that require a minimum retention period (e.g. tax records) are adhered too.

e. Do you have a procedure in place to ensure data is destroyed securely or archived safely?

f. Have you a procedure in place to ensure that there is no unnecessary or unregulated duplication of records?

Outputs:

- Become familiar with Church House, RB Library, Diocesan and local retention rules/policy
- Develop a retention policy including adding a cyclical review process to manage personal data
- Document how you follow your retention policy
- Save the policy and evidence of compliance in your GDPR file

11. Transparency and Communication - Privacy Notice

a. Are your parishioners, employees, colleagues fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form using clear and plain language?

b. If using CCTV or recording services or other events, ensure procedures are in place to proactively inform individuals of their rights

c. Place a poster on your noticeboard and inform parishioners on how their data is being processed

d. Inform your Select Vestry (or other stakeholders as appropriate) about the measures being undertaken to become GDPR compliant

Outputs:

- Develop a Privacy Notice for your diocese/Parish which should tell people, in a clear way how you intend to use their data, how long you will keep it for and the lawful basis you are processing their data (see Parish Resource section of the RCB website for further information)
- Save the Privacy Notice on your website and put a copy on your noticeboard
- Put a poster, or other relevant communications on your noticeboard
- If you use CCTV, develop a CCTV policy and notice. The notice should be available for all to see
- Save notices and policy in GDPR file

12. Supplier Agreements

Have agreements with suppliers and other third parties processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included?

Outputs:

- Document all agreements with suppliers and other third parties who process any personal data for you
- Ensure they are aware of their responsibilities under GDPR
- Save all details and discussions in your GDPR file

13. Data Security

a. Have you put measures in place to keep data safe and secure?

b. Have you documented a security programme/procedure that specifies any technical, administrative and physical safeguards for personal data?

Outputs:

- Document the security measures you have put in place
- Document how often these will be reviewed
- Save the document (and review process) in your GDPR file
- Put evidence of safety reviews into your GDPR file

14. Data Breach

a. Develop a response plan in case of a data breach

b. Develop procedures to notify the GDPR Coordinator, Representative Church Body, as required

c. Develop procedures to notify the Data Protection Commissioner when required

d. Develop procedures to notify the data subjects in the case of a breach

e. Ensure you have a method of documenting all data breaches, even the minor ones

f. Communicate with Select Vestry and other stakeholders so that they know what to do

Outputs:

- Document your data breach response plan
- Communicate with members of your select vestry
- Save in your GDPR file

15. Cyclical Review

a. Develop a cyclical review process where you review all steps outlined above

b. This should include a review (annual) of all your policies and notices and of all the personal data you hold

c. Add it to the agenda of any governance meetings held

(One suggestion is to review a policy/notice at every meeting; as so to keep this manageable)

Outputs:

- Document your cyclical review process
- Save in your GDPR file

Good luck and final thoughts…

The road to success is not straight. There is a curve called Failure, a loop called Confusion, speed bumps called Friends, red lights called Enemies, caution lights called Family. You will have flats called Jobs. But, if you have a spare called Determination, an engine called Perseverance, insurance called Faith, a driver called Jesus, you will make it to a place called Success.