A Beginner's Guide to GDPR

This document provides some FAQs with answers to questions that are frequently being asked by members across the Church of Ireland. Some will be more relevant to you than others. This document is updated regularly so please ensure the date on your version is the same as the one on the website.

FAQs:

What is GDPR?	General Data Protection Regulation (GDPR) is European legislation that came into effect across all EU Member States on 25 May 2018. GDPR: • protects the privacy rights of individuals • places obligations on all organisations to safeguard individuals' personal data that they collect, use and store. • gives people more rights and protection about how their personal data is being used.
Why does GDPR matter?	GDPR is not only about safeguarding rights and compliance; it is also about meeting individual's expectations in our increasingly digital age. GDPR brings: • Additional rights for individuals on how their personal data is being used • Additional rights on erasure and portability of data • Tighter rules on transferring data on EU citizens outside EU • Ability for individuals to make compensation claims • Data processors can now be directly held accountable and responsible for data protection • Significant fines for non-compliance
What happens if I do nothing?	GDPR has introduced greater sanctions for non-compliance including a suspension of data processing activities. • Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for administrative breaches to non-compliance. E.g. inadequate monitoring • Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued depending on: ✓ Nature of infringement ✓ Intention ✓ Preventative measures ✓ History ✓ Cooperation ✓ Notification
What is personal data?	Personal data is information about a living individual which is capable of identifying them. A living individual is also referred to as a data subject. Personal data includes names, addresses, date of birth, PPS/NIN number, email addresses, Income and other factors specific to the identity of a person (data

	subject) and online identifiers such as an IP address and location data.
Special (sensitive) categories of personal data	These are specific categories of personal data related to a person's profile: race or ethnicity; political, religious or philosophical beliefs; sexual life or sexual orientation; health; genetic or biometric data; criminal record; or trade union membership. Please apply **extreme caution** if you are using any special (sensitive) categories of personal data and ensure you always have explicit consent.
How do we use (process) Sensitive Personal Data?	The GDPR provides that "suitable and specific measures are put in place to safeguard the fundamental rights and freedoms of data subjects" if sensitive personal data is processed. You must have explicit consent from the data subject (individual) to use their sensitive personal data. A sample of the measures referenced above include: • Limiting access to personal data • Strict limits for the erasure of personal data • Specific targeted training for those involved in processing the data • Encryption • Pseudonymisation
How should we handle children's data under GDPR?	Under GDPR children have equal rights as adults but their data is a special category data. You need to have a procedure in place to get consent from the parent/legal guardian where required - ensure you have a procedure on how you gather consent. Save this procedure in a GPDR file and keep very secure. Develop a consent form for those aged 16yrs or younger (ROI) and 13yrs or younger (NI). Document the procedure for getting explicit consent to use children's data. Issue consent forms as required to parents/legal guardians, when you are using children's personal data.
What personal data is included under GDPR?	GDPR covers all personal data, so both electronic and physical personal data. This includes physical files, emails, images or recordings of individuals. E.g. Name, address, phone number, email address, religion etc.
What does data processing include?	Processing personal data includes everything we might do with personal data. This includes collecting, recording, storing, adapting, using, disclosing and deleting data.
What do I need to do?	Data should be: • Processed fairly, lawfully and transparently • Used only in ways which are compatible for the purpose for which it is given • Accurate and up to date • Adequate, relevant and limited to what is necessary • Only kept for specified, explicit and legitimate purpose(s) • Retained no longer than necessary • Kept safely and securely
How can I use personal data?	There are 6 ways that you are allowed to use personal data. These are: • Consent

	• Legitimate Interest • Contractual Necessity e.g. collecting bank details to pay salary/wages • Vital Interest e.g. using emergency contact details • Public Interest e.g. CCTV for health and safety • Legal Obligation e.g. Revenue reportings
What is Consent?	Consent is an indication of an individual's wishes, by a statement or clear affirmative action, signifying their agreement to the processing of their personal data. Consent must be freely given, specific, informed and unambiguous. Consent can be withdrawn at any time. Separate consents have to be obtained if you use personal information for different reasons. Therefore you are best asking people to complete a consent form that includes all circumstances where you might process someone's personal data.
What are my rights under GDPR?	The right to: • Be informed about how your personal data is being used • be given confirmation that your data is being processed correctly, and have the right to have access to your personal data if required • Have your personal data corrected if it is inaccurate or incomplete • Be forgotten, and have your personal data deleted • Restrict processing of your personal data in certain circumstances • Obtain and reuse personal data for your own purposes across different services • Object to processing in certain circumstances • Be protected against the risk that a potentially damaging action is taken without human intervention
What is Legitimate Interest?	Legitimate interest is one way that we can legally use personal data without getting consent. It is when you use personal data in a way someone would reasonably expect. If you decide to use legitimate interest to process personal information you need to: A) Do the legitimate interest test (see below) B) Document your findings C) Develop a legitimate interest policy Legitimate interest can only be used to process a limited amount of personal data. Consent (or one of the other ways) should be considered when using greater amounts of personal data or if you are unsure that the person would be happy with you using their data. There is a test that should be taken to determine if personal data can be processed within the legitimate interest of running your parish. The test: • Identify a legitimate interest – e.g. personal data needed for the day to day running of the parish • Show that the processing is necessary to do this (achieve this) e.g. you need to process the names and email addresses of parishioners to achieve the successful running of the parish • Balance it against the individual's interests, rights and freedoms e.g. does the individual know what you are using their details for; would you be happy for them to see you using it in this manner etc.
If I chose	This policy should state:

Legitimate Interest, what does my policy need to include?	• You have done the balancing test and checked that legitimate interest is the most appropriate way to process data • You understand your responsibility to protect individual's interests and data • You can justify your decision for choosing legitimate interest • You have checked that the processing is necessary and there is no less intrusive way to achieve the same result • You are only using individuals' data in ways individuals would reasonably expect • You have considered how to keep this data safe
Do I need permission to keep and use a list of members of the parish?	There is some data processing that we do as part of normal church management that we don't need consent for - holding lists of group members for example. This falls within Legitimate Interest. **What is a list of group members?** GDPR does not define the type or amount of personal data that can be included within a list of group members. This is something you need to define at a local level. However you are obliged to adhere to the 'test' and have a 'policy' as detailed in the points above. Legitimate Interest is applicable - If your list of group members only contains basic (and small amounts of) personal data you can process this personal data within legitimate interest of the day to day running of the parish. E.g. Rebekah Fozzard, Parish Secretary Legitimate Interest is not applicable - If your group list includes: names, addresses, email, date of birth, phone number etc. consent is required. E.g. Rebekah Fozzard, Parish Secretary, 22 church road, rebekahfozzard@xxxx.ie ; 21/12/99; 087 1234567. NEVER Legitimate Interest - If the list of group members relates to anyone under 16 years of age; or vulnerable adults; or contains any special category data (e.g. criminal record etc.) explicit consent is required.
How do I know what personal data we hold?	A data audit is an examination of all the personal information that is being held by the organisation and results in a personal data inventory. We have a template in parish resources that will support you. This audit should include all personal data held within the parish, whether such data is held in email accounts, desktops, mobile devices, back up storage and/or paper files. On completion of the audit, review this information and decide what needs to be included in your Privacy Notice.
What should be contained in your Privacy Notice?	A privacy notice is required to inform your parishioners of their rights under GDPR. We have a draft template in parish resources to support you in developing one. It should include what personal data you have, why you have it and who you share it with.
Does your parish need to appoint a Data Protection Officer?	No – however the rector of the parish along with one designated person will need to be in charge of data protection within the parish. The RCB has a Data Protection Officer – Rebekah Fozzard: Rebekah.fozzard@rcbdub.org
What is the role of the parish under	The parish is a joint data controller, along with the Bishops, the Diocesan Councils and the RCB. All four of the Church of Ireland's data controllers act with equal power.

GDPR?	Each joint controller has agreed areas of responsibility. For the parish: • Clergy • General Vestry • Select Vestry • Employees, contractors and volunteers
What is a Data Protection Impact Assessment? (DPIA)	This is a risk based approach designed to describe the processing of personal data, assess its necessity and proportionality and help manage the risks to "the rights and freedoms" of individuals. This is done by assessing the risks and determining the measures to address them. A DPIA is an important tool for accountability, as it helps to comply with the requirements of the GDPR. There is an Impact Assessment **template** on the Parish Resources section of the website under GDPR. You will need to do a DPIA or if you use CCTV, for example.
When will an individual have "the right to be forgotten"?	The right to be forgotten (the right to erasure) is allowed where: • Data processing is no longer necessary • A person has withdrawn consent or objects to processing • Personal data has been unlawfully processed • Personal data must be erased for compliance with a legal obligation. The GDPR specifically provides that an individual will not have a right to be forgotten if the processing is necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.
How long should we hold onto personal data?	GDPR states personal data "should 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'. The RCB has developed a Retention Guide which be found on the parish resources section of the website.
What do we do with parish records?	The RCB library is the official place of deposit for Church of Ireland for parish records that are no longer in local custody. Here each parish collections are assigned a unique record number, and each item within each collection is given its own unique identity. If you have any questions about a Parish Record Collection, please contact the RCB library directly: library@ireland.anglican.org
What about burial grounds?	Members of the clergy and select vestries need to be careful in terms of publishing details relating to graves in a burial ground or if a third party approaches wanting to publish such information. Any proposal should be scrutinized carefully by the select vestry which should obtain full details of the content of the intended publication, the form it would take and what exactly is being sought from the vestry. It is strongly recommended that neither images nor details of inscriptions on memorials erected within the past forty years ever be uploaded to the internet or published in any other formats. If you have any questions or would like further guidance, please contact the RCB library: library@ireland.anglican.org
Can I only use consent?	No, you can rely on another method of consent e.g. legitimate interest. Just document your reason why.

What is a Subject Access Request? (SAR)	**A right** conferred on a data subject **by LAW** to request a copy of data held about them, by an organisation. On submission of a written Subject Access Request, you have one month to: a) Provide information requested b) The information must be concise, transparent, intelligible and easily accessible c) Provided in writing or electronic d) Oral response allowed once ID can be verified e) Must respond in full within 1 month of receipt f) If request is electronic, response must be the same unless specified There are **times when you don't need to respond (exceptions)**. These include: where the request has not been in writing; fee has not been paid; insufficient identification has been provided; where the Data Controller believes the request is vexatious. For more detailed guidelines, please see our SAR process map and guide on the Parish Resources section of the website.
Does every website need a Data Privacy Notice?	Yes.
What are the GDPR policies a parish needs to have?	• Data Privacy Notice • Website Privacy Notice • Data Protection Policy • Retention Policy • Internal Security Policy • Acceptable Usage Policy Please see the Parish Resources section of the Church of Ireland website to see details on each of the policies in the Data Controller's Guide to GDPR: Parishes
Who are we regulated by?	Organisations working cross border are regulated by the Data Protection Authority where they have their main establishment. For the Church of Ireland, as Head Office is in Dublin, all administrative offices and functions are regulated by the Irish Data Protection Commissioner. Likewise, all Parishes in ROI are regulated by the Irish Data Protection Commissioner. Parishes in NI are regulated by the UK's Information Commissioner's Office.
Can we publish accounts with names, addresses and amounts of donations?	Not without explicit consent from every member to do this. You will have to demonstrate evidence of consent.
What can we do to keep data secure?	Have as much as you can online, don't have boxes of information unsecured. • Strong Password and Strong PINs • Watch out for Phishing • Protect your office space – tidy desk; lock your cupboards/door; • Shred confidential documents • Develop a security routine – e.g. Lock your Screen; Be suspicious! • Locked Cabinets

What will be the impact of Brexit?	The UK Data Protection Act (2018) empowers individuals to take control of their personal data and supports organisations with the lawful processing of personal data. Once the UK leaves the EU, the Act will ensure that the standards of the GDPR are enshrined in UK law. However, this is not something that your parish needs to worry about as long as the only data you're sharing is within the Church of Ireland.
GDPR & photography	Photographs are regarded as personal data. You can use photographs once the following applies: • Where a photograph can clearly identify an individual, consent should be sought, particularly if this photograph will be published on any external site (e.g. website). • Photographs should be treated the same as any other personal data • Where photographs of minors/children e.g. under 16 years old in ROI; under 13 years old in NI, then parent/guardian consent must be obtained – this is mandatory • Where a photograph cannot uniquely identify a person, so a data subject Fis not at risk should the data be comprised, it is possible to use this photograph within the legitimate interests of the work of the parish
What is a data breach?	This is something that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. If a high risk to the individuals involved, e.g. through identity theft, GDPR makes informing the Data Protection Commissioner/Information Commissioner compulsory.
What should I do to avoid a data breach happening with the suppliers my parish use?	You must ensure that your parish has a model contract clause in place with each of your suppliers. For instance, if your parish has a CCTV system, you must ensure that there's a data protection clause in your contract with the supplier.
If my parish has an administrator who works at home, how can they keep the data secure?	You must document a security procedure that specifies any technical, administrative and physical safeguards for personal data. Please see the Data Security Guide for specific guidelines on this.
Where can I find information for children and youth?	There are two resources on the parish resources section of the Church of Ireland website. One is a cartoon for children ages 5-10 years and the other is a poster for ages 10-16 years.
Where can I go with further questions?	• Rebekah Fozzard – RCB's Data Protection Officer: dataprotection@rcbdub.org / 01-4125660 • Irish Data Protection Commission: info@dataprotection.ie / 1890 252 231 • UK's Information Commissioner's Office (ICO): https://ico.org.uk/ or +44 1625 545 700.