Derry Diocese

General Data Protection Regulation (GDPR)

Guide for Parishes

2019

Contents

INTRODUCTION

What is the General Data Protection Regulation ('GDPR')?

The General Data Protection Regulation ('GDPR') is a European Regulation which regulates the processing of personal data relating to individuals in the EU. It has been hailed as the most momentous and important change in data protection and privacy legislation in 20 years. It came into effect across the UK and Ireland on 25th May 2018.

What are the main aims of GDPR?

- To set out the rules relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data;
- To require organisations to make a genuine commitment to lawful data processing;
- To enhance the enforcement powers of the regulatory authority, the Information Commissioner's Office, in the event of a breach.

Will GDPR be affected by Brexit?

In the short term, Brexit will not affect the application or relevance of GDPR. While GDPR is a piece of European legislation it has been adopted and incorporated into UK law by the Data Protection Act 2018 which also came into effect on 25th May 2018.

Why is GDPR important for my Parish?

The canonical importance of processing, protecting and archiving biographical information is enshrined within the fabric of every Diocese and Parish. The Diocese recognises that the greatest of care must be taken when processing personal data and understands that this is not a purely administrative task. The records a Parish holds can have profound pastoral significance. Personal information is directly relatable to the dignity of human life and the respect that every individual deserves must extend to information held about that individual. GDPR respects and is not intended to prejudice the status of churches and religious associations. However it is vital that parish administration adapts to reflect the challenges posed by the information era. Compliance is a mandatory legal requirement. Auditing your data processing activities and ensuring that the highest possible standards are applied to the collection and storage of confidential information is an essential part of risk management. Failure to adhere to the requirements of GDPR could result in enforcement by the Information Commissioner's Office.

Who bears responsibility for compliance with GDPR within the Church?

Legal responsibility for all decisions regarding the purpose and means of processing personal data rests with the '**Data Controller'** under GDPR. The civil, corporate structure of the Diocese means that responsibility for setting policy and benchmarking data protection processes will be centralised and carried out by the Diocesan Office. The Diocese of Derry and more specifically, Derry Diocesan Trust is the Data Controller including when processing is carried out by its curial offices, Parishes and committees.

If you require any further information on data protection within the Parishes in the Diocese please contact:-

Executive Director

Diocesan Office, St Eugene's Cathedral, Francis Street, Derry BT48 9AP

Tel: 028 71262302 Email: office@derrydiocese.org

THE INFORMATION COMMISSIONER'S OFFICE (ICO)

What is the role of the Information Commissioner's Office (the ICO)?

The ICO is an independent authority set up to uphold information rights in the public interest in the UK. It has 4 key functions:-

- It operates an advice service to address general enquiries on data protection and freedom of information;
- Promotes good practice in information rights by raising awareness of organisational responsibilities across all sectors.
- Influences policy in related areas by working closely with the departments of the Northern Ireland civil service and the wider public sector;
- Acts as a regulator and enforcer in serious data breaches.

Is there an equivalent authority in the Republic of Ireland?

Yes, the equivalent authority in the Republic of Ireland is the Data Protection Commission. GDPR makes special provision for organisations that are engaged in cross-border processing activities. As the Diocesan Office is located in Derry, the UK Information Commissioner's Office will be the 'Lead Supervisory Authority' under European law even if processing is carried out in the Republic of Ireland. This position could change after Brexit.

Can the ICO impose a fine?

Yes, in extreme cases, the ICO has the power to monetary fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater.

Is my Parish required to register with the ICO?

No, individual parishes are not required to register with the ICO. As discussed above, the Diocese is a single entity in civil law and has registered with the ICO on behalf of all Parishes. Any previous registration entered on behalf of the Parish, under the previous legislation, should be cancelled when the time comes for renewal.

If you are unsure if your Parish has been registered with the ICO or believe that your registration has been renewed automatically, you can search the public register maintained by the ICO online.

https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

STATEMENT FROM THE ICO

Quote from the ICO's Head of Regions, Ken Macdonald:

"We don't want to be worrying about the breaches, because we want to prevent the breaches taking place. If they do happen, then we will be taking the appropriate action and serving the appropriate level of penalty for the breach. Unfortunately, despite all these stories that we have, from the cases that we have taken regulatory action, security is a big thing, and people are still forgetting about it. They forget about, in particular, the paper records. Too often, I see people in public, reading personal, sensitive information. Too often, we fine people and organisations because papers have been left in bags at the train station, on the bus, etc. It's not just about the digital world, it's not just about encryption, it's about handling everything - physical and electronic information."

As featured in 'Inside Business' on BBC Radio Ulster and published online on 3rd June 2018 https://www.bbc.co.uk/news/uk-northern-ireland-44332414

SCOPE OF THE REGULATION

What is 'Personal Data'?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law.

Personal data that has been rendered anonymous, in such a way that the individual is no longer identifiable, is not considered to be personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The law protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- an Internet Protocol (IP) address.

Are there any special categories of data?

The following special categories of personal data are deemed 'sensitive' and warrant specific protection under GDPR:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- processing of genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- health;
- sex life or sexual orientation.

SCOPE OF THE REGULATION

When does GDPR apply?

GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system, or intended to be part of such a system.

Processing covers a wide range of operations performed on personal data. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

Examples of processing: -

- staff management and payroll administration;
- maintaining a list or database of contacts;
- sending newsletters or bulletins;
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (CCTV).

Does GDPR always apply?

No, it doesn't apply to the processing of personal data of deceased persons or information about companies.

GDPR does not apply to data processed by an individual for purely personal reasons or for activities carried out in one's home, provided there is no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, then the data protection law has to be respected.

GDPR encourages organisations to anonymise personal data as much as possible to mitigate risk. GDPR does not apply to anonymised material.

Case Study: Differentiating between personal activities and parish work

A parish employee uses her own private address book to invite friends to her wedding which is taking place in the Parish. GDPR will not apply.

The same employee uses her facebook account to contact friends seeking donations to fundraise for the parish. GDPR will apply. All fundraising activities must be authorised by the Parish Priest. While individuals are welcome to raise awareness of fundraising campaigns, they should do so by sharing official posts from the Parish.

THE DATA PROTECTION PRINCIPLES

What issues should my Parish consider when processing data?

The Parish is required to adhere to 'the data protection principles' in all processing activities to comply with the requirements of GDPR. The principles are summarised as follows: -

- LAWFULNESS, FAIRNESS AND TRANSPARENCY
  All personal data must be processed lawfully, fairly and in a transparent manner

- PURPOSE LIMITATION
  Data must only be collected and processed for legitimate purposes which are specifically and explicitly stated. You cannot simply collect personal data for undefined purposes

- DATA MINIMISATION
  Only data which is relevant for the purpose should be collected and processed

- ACCURACY
  Reasonable steps should be taken to ensure that data remains accurate and is kept up to date

- STORAGE LIMITATION
  Data should not be kept for any longer than is necessary (unless it is being processed for archiving purposes in the public interest, for scientific purposes, or for statistical or historical purposes)

- INTEGRITY AND CONFIDENTIALITY
  Data must be kept securely and technical and organisational measures should be put in place to protect it from hackers etc

- ACCOUNTABILITY
  Data controllers must be able to demonstrate compliance with all the GDPR principles

Why does my Parish need a Privacy Notice?

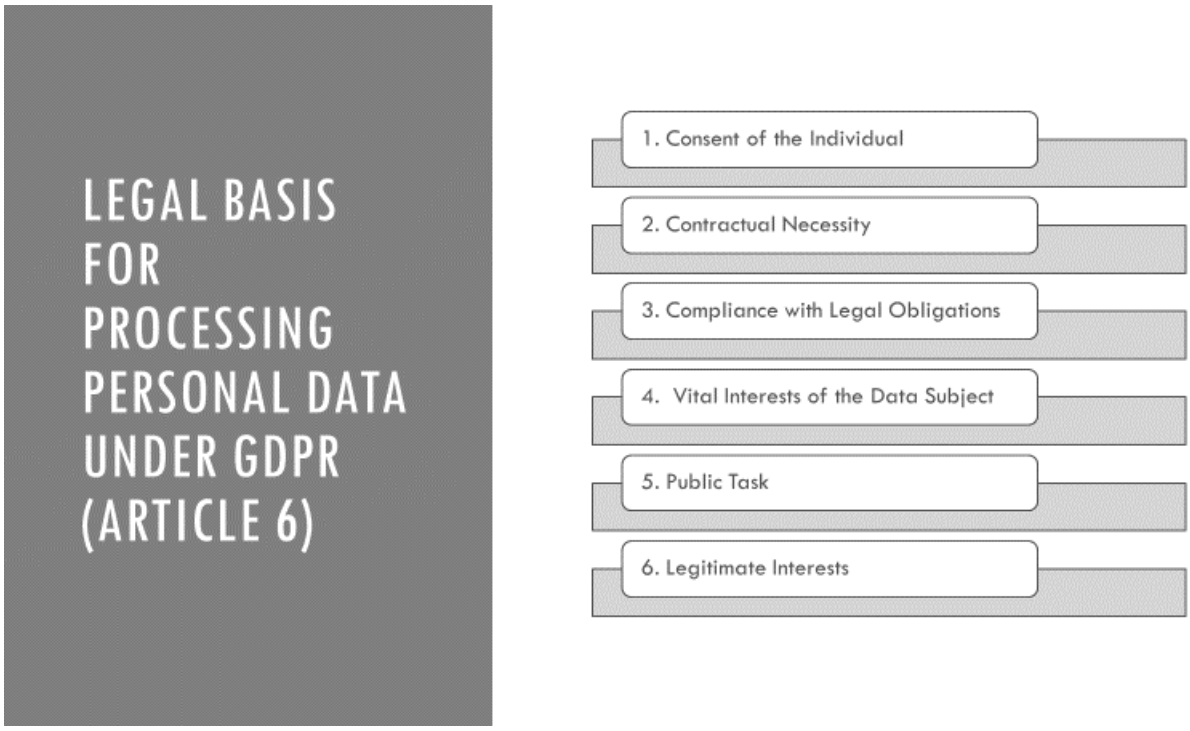
The data protection principles stress that all processing of personal data should be transparent so that individuals can understand what personal data concerning them is collected and used, and to what extent that personal data is, or will be, processed. A Privacy Notice is an essential requirement under GDPR and is an illustration of the principles of transparency and accountability in action. The principle of transparency in particular, requires any information and communication relating to the processing of personal data to be easily accessible and easy to understand. Clear and plain language must be used. A copy of the Privacy Notice which has been produced by the Diocese for use in every parish is enclosed at Appendix 1. Information contained within the notice includes: -

- The identity of the controller;
- The purposes of processing personal data within the Parish;
- The safeguards and rights which apply in relation to the processing of personal data;
- Contact information for data protection queries.

The Privacy Notice must be provided at the time data is collected when creating or updating a record. When processing relates to existing records, the Notice should be printed in hardcopy and made available from the parish office. For ease of reference, parishioners should also be able to download it electronically from the Parish website.

LAWFUL PROCESSING

For processing to be lawful under the GDPR, you need to identify a legal basis before you can process personal data. There are six legal grounds or reasons identified in the regulation.



As a general rule, processing of the 'Special Category Data' is prohibited unless a company or organisation can demonstrate that the processing activities fulfil a further condition under the legislation. Given the context in which processing occurs within the Parish, it is inevitable that a high percentage of the data that is processed will either explicitly or implicitly include an individual's religion which is 'special category' data. When this is the case, the Diocese relies upon the fact that processing is carried out in the course of its legitimate activities as a non-profit-making organisation with a religious aim. Fulfilling this condition requires the Diocese to demonstrate that appropriate safeguards are in place, that processing relates solely to the members or to former members of the Parish and that personal data is not disclosed externally without an individual's consent.

Further conditions which may apply to the 'Special Category Data' within the work of the Parish include:-

- Data is manifestly made public by the data subject; (for example, the individual actively participates in a public act of worship);
- It is necessary for handling legal claims;
- There is a substantial public interest for processing in accordance with the law;
- Archiving is in the public interest/necessary for research & statistics;
- The individual has given their explicit consent.

PARISH RECORDS

How are the Data Protection Principles reflected in the Diocese's approach to data protection?

Understanding what data is processed, and why is pivotal to applying the provisions of GDPR in practice. In preparation for the introduction of the GDPR, the Diocese carried out an impact assessment to identify the various categories of data collected and stored within a Parish and consider the legal basis for processing.

Subject Matter	Examples	Legal Basis for Processing
Sacramental Records	Baptism, Marriage, First Holy Communion & Confirmation Registers	When we collect personal data relating to the celebration of a sacrament and maintain records on parish activities, we do so in the legitimate interests of our Church and its members. Collecting information pertaining to the celebration of our faith is an essential part of the fulfilment of our spiritual and charitable purpose to advance the Catholic religion. We also process information in compliance with our legal obligations and as part of a wider task in the public interest, for example when officiating at a wedding.
Records pertaining to the celebration and participation in Mass, events, pilgrimages and services	List of Eucharistic Ministers, Readers, Choir & Musicians, contact information and requests relating to visits to the housebound, information for the Parish newsletter, audio and visual recordings & photographs, Death Registers	The congregation plays an integral role in all religious services. It is important for us to be able to communicate with you in relation to news about activities and events taking place within the Church and local community including seeking feedback and informing you of any changes to our pastoral plans or ministry. Processing this data is necessary to fulfil our legitimate interests as a Church and to fulfil our spiritual and charitable purpose.
Pastoral Care, Safeguarding, Health & Safety	CCTV/webcam, Accident Log, volunteer information, training records, Access NI or National Vetting Bureau applications/clearance, record of complaints	This information is of pivotal importance for legal and pastoral reasons and is processed in accordance with our legal obligations, our public tasks and our legitimate interests in contributing to the advancement of our faith in the local community.
Finance & Governance including Fundraising & Donations	Gift Aid declarations, parish envelopes, minutes of committee meetings, tender documents, use of facilities, parish draws	The Diocese is a registered charity and we are required to hold information on finance and governance to comply with our legal obligations under charity and tax law.
General church administration including information on our employees	Parish diary and telephone directory, routine correspondence, visitation papers, contracts, timesheets, personnel files, miscellaneous information obtained relating to the operation of our website including cookies	This category of data is varied, and processing is based on both contractual necessity and our legitimate interest in achieving our charitable objects of advancing and maintaining the Catholic religion.
Statistical and historical information	Parish census and surveys	Processing information of a wider statistical and historical nature is consistent with the performance of a task in the public interest.

KEEPING DATA SECURE

GDPR requires every organisation to have "appropriate technological and organisational measures" in place in order to process data securely. This requirement is aimed at addressing the security of paper documents and devices as well as managing the risks associated with online activity and computer processing.

Within the Parish, it is vital to physically secure Church premises and to be mindful that data is a valuable commodity which is at risk of theft or corruption. Optimising the use of existing security features such as using locked cabinets, CCTV and security alarms is crucial. The risks of a potential data breach are heightened when systems are in place but are not utilised properly.

Example: -

Under the previous legislation, in 2013, Glasgow City Council was fined £150,000.00 for a data breach arising from theft of two laptops from its premises which were insecure as they were were being refurbished. One laptop had been locked away in its storage drawer and the key placed in the drawer where the second laptop was kept, but the second drawer was subsequently left unlocked overnight, allowing the thief access to both laptops which were unencrypted. One of the laptops stolen contained the council's creditor payment history file, listing the personal information of 20,143 people, including the bank account details of 6,069 individuals. This breach could have been avoided if basic security measures had been taken.

Extra care must be taken when using portable devices and transporting paper files or diaries. Always consider whether it is necessary to take the records with you. If it is necessary, do you require the entire file or can you select the key information that you require to minimise risk. When in public, always ensure that the records are in your presence and are not left unattended. Before removing the file, make sure that information is not visible from coversheets, labels or loose pages.

Common threats to data security when handling paper records

- Multiple photocopies
- Copies left on printers
- Unauthorised removal of documents from the office
- Storing records in communal, shared or public spaces
- Failing to use locked cabinets or storage
- Insecure disposal

Tips for counteracting these threats

- Display ICO posters (Appendix 2) or reminders in the Parish Office to promote awareness of data protection within the parish office so that all clergy, staff and volunteers within the Parish;
- Limit the number of copies that can be made of documents containing personal information;
- As a general rule, do not permit parish records to be removed from the parish office;
- Assign responsibility to a staff member to ensure that all print trays are clear at the end of each day;
- Scan confidential paper documents so that they can be password protected and encrypted;
- Never dispose of personal data within general waste. Always ensure that documents containing personal information are shredded and/or disposed of securely by an accredited confidential waste company.

What is cyber security?

Cyber security is the practice of protecting systems, networks, and programs from online or digital attacks. These attacks are usually aimed at extorting money from users or accessing, or destroying sensitive information.

There are many different types of cyber security threats including malicious software known as malware and ransomware which are designed to damage or gain unauthorised access to a computer. Viruses are a form of malware. Ransomware blocks access to files on the computer system until a ransom is paid. A further threat is known as phishing. Phishing is the term used to describe the practice of sending fraudulent emails that resemble emails from reputable sources seeking personal information such as banking and credit card details, and passwords.

What steps can my Parish take to improve cyber security within the Parish?

Managing cyber security can be daunting and it is difficult to keep track of the latest technology but there are lots of helpful resources available. A one page summary on cyber-security issued by the National Cyber Security Centre is reproduced at Appendix 3 for your information.

If in doubt, seek advice from your system administrator on additional measures in cyber security to prevent corruption of data by viruses or hacking.

Further information and tips can be found on the Cyber Aware website which is a part of a UK cross-government awareness scheme**:** - https://www.cyberaware.gov.uk/

DATA RETENTION

What does GDPR say about data retention?

Any personal data which is retained should be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Personal data should not be kept longer than necessary in accordance with the principle of 'Storage Limitation', (page 7). Time limits should, therefore, be established by the controller for erasure or for a periodic review of all records containing personal data.

Every reasonable step should be taken to ensure that personal data which is inaccurate is rectified or deleted.

How is this applied in practice by the Diocese?

The subject matter of the record will determine how long the information is retained within the Diocese. Some of the personal data processed by the Diocese will be of wider historical or genealogical significance, which justifies retaining it for longer periods than would typically be associated with business transactions. There may also be instances where the sensitive or legal nature of the record itself requires the Diocese to store the information for an extended period. For example, all records pertaining to safeguarding are maintained for 100 years. The table below provides a quick reference for each subject matter, but if you require specific information on a retention period please contact the Diocesan office.

Subject Matter	**Retention Period**
Sacramental Records	Permanently
Records pertaining to the celebration and participation in Mass, events, pilgrimages and services	Routine information such as rotas and contact details will be checked intermittently and by the Parish Office on an informal basis and formally reviewed every 5 years to ensure that the data remains relevant/accurate and that processing is still necessary.
Safeguarding	This information is sensitive and is held for 100 years.
Finance & Governance including Fundraising & Donations	Determined by Company, Charity & Tax Law Specifically, we retain Gift Aid declarations and associated paperwork for up to seven years after the year to which they relate.
General church administration including information on our employees	Determined by Employment Law otherwise routine information such as diaries and timesheets will be checked intermittently by the Parish Office on an informal basis and formally reviewed every 5 years to ensure that the data remains relevant/accurate and that processing is still necessary.
Statistical and historical information	Permanently

THE RIGHTS OF THE INDIVIDUAL

What rights has GDPR established?

An individual has the right to:

- information about the processing of his/her personal data;
- obtain access to the personal data held about them;
- ask for incorrect, inaccurate or incomplete personal data to be corrected;
- request that personal data be erased when it's no longer needed or if processing it is unlawful;
- object or ask to restrict the processing of their personal data in specific cases;
- receive personal data in a machine-readable format and send it to another controller ('data portability').

Additional rights apply in relation to processing related to direct marketing and decisions based on automated processing but these are unlikely to arise in the activities carried out by your Parish.

Are these rights absolute?

The right to the protection of personal data is not an absolute right. Recital (4) of GDPR explains that it *"must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles… in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity".*

How does an individual exercise these rights?

An individual wishing to exercise these rights must contact the Data Controller, in this instance the Diocese via the Diocesan Office. The Diocese is required to consider the request and to provide a response within one month. If the Diocese is unable to satisfy the request, the individual will be provided with a written explanation for the decision and advised of their right to make a complaint to the Information Commissioner's Office.

Further information on how to manage a request to access parish records can be found later in this guide.

ACCESSING PARISH RECORDS

Parish Staff, Clergy, Volunteers

The Parish office is a hub of data processing activity. It is important that all staff, clergy and volunteers are aware of the importance of data protection within the Parish. Do not assume that all records should be accessible to all personnel. If documents are considered to be particularly sensitive, access should be limited to the Parish Priest or directly relevant person.

Practical tips for office administration

- Implement a clear desk policy;
- Ensure that records are not stored in waiting areas, communal spaces or meeting rooms or any place that a parishioner or member of the public could be unattended;
- Limit any personal data which is openly displayed on notice boards to essential information;
- Ensure that computers are password protected and that passwords are not automatically saved or handwritten and affixed to the desk/computer as a memory aide.
- Position ICO posters near computer stations, printing areas or bins/shredders as a regular reminder of good practice.

Parishioners (including former Parishioners)

It is important to remember that the entire focus of GDPR is personal data. An individual is only entitled to data that relates exclusively to them. Requests can be made verbally in person or by telephone, or in writing by email or letter.

1. ***Request to access or copy a specific record***
   Requests for copies of sacramental records, such as a baptismal certificates for couples preparing for marriage, are very common. However if the request involves an unusual element for example, the individual asks to see the original entry on the baptismal register, there are number of important practical considerations that should be taken into account when handling such a request.

   - Providing a copy of a specific document is preferable to permitting a general inspection.
   - If the individual is not known to you and has arrived unexpectedly you should confirm his/her identity by asking to see photographic ID such as a driving licence or passport.
   - The individual should be accompanied at all times when inspecting the document.
   - You should obscure any references to other third parties that have no bearing on the request, for example, covering the entries above and below.
   - As a general rule, photographs should be prohibited unless the document/record has been sufficiently redacted to ensure that only the individual's information is available.

   Please note that you are not under any legal obligation to provide immediate access to original records or provide an instant photocopy. All requests made under GDPR must be processed within one month. If in doubt, please contact the Diocesan office.

Can a friend or relative collect a Baptismal Certificate on a Parishioner's behalf?

Yes, provided that the friend or relative can provide confirmation that they are doing so at the request of the parishioner and with his/her consent.

2. ***A general request for information on the personal data held within the Parish***
   If a parishioner attends the parish office or approaches a member of clergy seeking access to all records held by the parish about them, this enquiry should be re-directed to the Diocesan office so that it can be processed as a 'Subject Access Request'. The Parishioner should be provided with a copy of the Parish's Privacy Notice, (see Appendix 1), which contains the necessary contact information and essential details on an individual's rights in relation to such requests.

Keep multiple hard copies of the Privacy Notice in the Parish Office so that it is readily available and can be easily disseminated to Parishioners

The general public

Church records are not public documents. GDPR is limited to personal data and does not facilitate open access to confidential documents. If an individual is not a member of your congregation and has no known links to your Parish, they have no entitlement to access any church records. On a case by case basis, you may consider permitting access to historical information.

It is important to note that individuals accompanying parishioners may fall within this category. Caution should be exercised in permitting any person accompanying a parishioner to access church records.

Example scenario: -

An unknown individual attends the parish office. She is visiting Northern Ireland on holiday from Australia. She has Irish relatives in the area and she wants to know more about her family tree. She asks if she can inspect the marriage and baptismal records.

Recommended approach

Unrestricted access is prohibited. It is permissible for you to carry out a search against the records to assist with the request so that you can consider what information is available, however, it will not be possible for you to provide any information on any living relative and your search should be confined to historical information.

Other Third Parties

This category could include: -

- *Police/Law Enforcement or Government Agencies*
- *Solicitors or other agents, advisors or representatives*
- *Historians/Researchers*
- *The Media*

All requests of this nature should be re-directed to the Diocesan Office irrespective of Parishioner consent. These requests may require legal advice to be obtained before any disclosure or comment is made.

SHARING DATA

Sharing Personal Data within the Diocese

As the entire diocese is a single entity for the purposes of GDPR, it is permissible to share data within the Diocese for example, when a Parish sends information to the Diocesan Office as part of the payroll process.

Sharing Personal Data with external third parties such as schools and service providers

The Diocese will only share personal information with external third parties if it is necessary and consistent with its legitimate interests.

Sometimes sharing information is necessary for pastoral reasons for example, if a school requires information to assist in preparation for the celebration of a sacrament. It is clearly in the legitimate interest of the parish to engage with local schools however, the Parish should be mindful of the principle of 'data minimisation', (page 7) and should only share essential and relevant information. In most situations, the number of children baptised in a particular year will suffice rather than providing names and addresses from the baptismal register. Alternatively, the school should provide a list of the children enrolled in their school so that the Parish can provide a tailored response. Information or circumstances may have changed since the entry was made in the register and the Parish is, therefore, unable to verify the ongoing accuracy of the contents for use by the school.

On other occasions, the Diocese will consult with third parties such as IT consultants or payroll consultants to assist in administrative tasks, or professional advisers to advise on legal or technical matters. Before sharing any personal data, the Diocese is required to ensure that satisfactory controls are in place to allow the information to be transmitted safely and to seek confirmation from third party service providers so that it can be satisfied that the third parties are duly accredited within their respective industry or trade and that they comply with data protection laws.

There are also instances when there will be a specific legal requirement to share information, for example in order to perform essential safeguarding tasks such as checks against criminal records from Access NI/National Vetting Bureau, liaison with the Police and other law enforcement agencies, insurers or tax, charity or immigration authorities.

Protecting Sacramental Records

Sacramental records must be treated with the greatest of care. Processing personal data contained within a sacramental record can involve contacting the individual, to which the record pertains, regarding ancillary matters related to the celebration of the sacrament. For example, the Parish Priest wishes to invite the parents of recently baptised children, those preparing for Holy Communion or Confirmation, newly married couples or recently bereaved families to a special mass or event. This practice is permissible for a limited period of time for activities directly related to the sacrament; however, it must be borne in mind that a sacramental record is created for a specific religious purpose and it is not intended to be amended or updated. It should not therefore be relied upon for more general purposes, or as an ongoing source of contact information for any longer than a year after the date the sacrament is celebrated.

If more regular contact with Parishioners is envisaged, (for example, to send weekly bulletins, raising awareness of fundraising activities or issuing notices about annual events), a separate database of contacts, or a mailing list for Parishioners should be created. The rationale for this recommendation is twofold: -

1. It maintains the integrity and spiritual purpose of the sacramental record;
2. It allows contact information to be maintained and managed in a more responsive, targeted and efficient way. A list or database can be computerised to aid day-to-day administration and can be readily and regularly reviewed in accordance with the needs and rights of Parishioners.

PRACTICAL TIPS

Top five tips from the Information Commissioner's Office for small and medium sized charities and third sector organisations:

1. ***Tell people what you are doing with their data***

People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important that you are open and honest with people about how their data will be used.

2. ***Make sure your staff, clergy and volunteers are adequately trained***

New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff, clergy and volunteers.

3. ***Use strong passwords***

There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

4. ***Encrypt all portable devices***

Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

5. ***Only keep people's information for as long as necessary***

Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

DATA BREACH

What qualifies as a data breach?

A personal data breach occurs when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data processed.

What does the GDPR say about data breaches?

Self-reporting is an important feature of GDPR and is underpinned by the accountability principle. Data controllers must assess and record all data breaches. Breaches must be reported to the Information Commissioner's Office where the breach is likely to result in a risk to the rights and freedoms of an individual. Notifications must be made without undue delay and, where feasible, not later than 72 hours after the Data Controller becomes aware of the breach. In serious cases, it may also be necessary to notify the individuals concerned that the breach has occurred.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

What should I do if there is a data breach in my Parish?

All data breaches should be reported to the Diocesan Office immediately even if the breach is accidental or seems fairly innocuous. The Diocesan Office is required to keep a record of breaches as part of its legal obligations as a Data Controller.

In addition to the legal requirements, there are a number of benefits which stem from a shared experience of data protection. Reporting breaches or concerns that have arisen in your Parish will provide important learning opportunities and will enable the Diocese to develop further training, hone its policies or recommend updates to technology or security systems.

What will the Diocese do if a Parish reports a breach?

The Diocese will assess the need to report the breach to the Information Commissioner's Officer and/or notify the Parishioners involved by considering the following key factors:

- The likelihood and severity of any risk to people's rights and freedoms arising from the breach;

  Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal

  Medium Risk: The breach may have an impact on individuals, but the impact is unlikely to be substantial

  High Risk: The breach may have a considerable impact on affected individuals

  Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.

- Were appropriate technical measures or organisational protections in place at the time of the breach e.g. encryption

Legal advice may be sought to help the Diocese carrying out the necessary risk assessment.

FURTHER INFORMATION

To find a copy of the Regulation: -

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

For further guidance: -

https://ico.org.uk/

To contact the Information Commissioner's Office:-

The Information Commissioner's Office – Northern Ireland:

3rd Floor, 14 Cromac Place, Belfast BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114

Email: ni@ico.org.uk

The equivalent authority in the Republic of Ireland is the Data Protection Commission:

Canal House, Station Road, Portarlington R32 AP23 Co. Laois

Telephone: +353 (0761) 104 800

Email: info@dataprotection.ie

Please note this guide has been prepared as part of training materials for your parish on data protection. It should however, only be taken as general guidance and should not be used as a substitute for obtaining legal advice if a contentious issue does arise.

UPDATES FOR THIS GUIDE

This is not a 'one-off' publication and monitoring the day-to-day outworking of the legislation will be continuous.

VERSION NO.	DRAFTED BY	APPROVED BY	DATE PRODUCED	PURPOSE/CHANGE
1	NAPIER & SONS SOLICITORS	EXECUTIVE DIRECTOR	FEBRUARY 2019	COMPILED AS A GUIDE FOR TRAINING PURPOSES