CATHOLIC INSURANCE SERVICE LTD

THE GENERAL DATA PROTECTION REGULATION: A BRIEF GUIDE FOR CATHOLIC DIOCESES

BLAKE MORGAN

Foreword

In 1983 Pope St John Paul II promulgated the revised Code of Canon Law with the Apostolic Constitution *Sacrae Disciplinae Legis*. In the opening paragraph St John Paul II reminds us that, 'always maintaining fidelity to the Divine Founder' ecclesiastical laws are revised to be 'truly in accord with the salvific mission entrusted to the Church'.

Drawing on the teaching of the Second Vatican Ecumenical Council the revised Code of Canon Law expounds rights and obligations of members of the Christian faithful, in all their variety, which are to serve the mission of the Church.

While the Church's system of law enunciates many rights and obligations, the community of the faithful, and the associations and structures upon which it draws, is also subject to various civil laws in each of the territories in which the universal Church finds expression. These civil laws often give greater particularity to principles found in the Church's own body of law. One such area is that of privacy and the protection of personal data. Necessarily, civil laws in this area may be revised and adapted more readily, in line with technological and cultural developments, than may ecclesiastical laws.

Recent years have seen an explosive growth in what is now possible with modern information technology, a growth that could hardly have been imagined in 1983, let alone in 1962-65, the years of the Council.

In the United Kingdom, in 1998 the Data Protection Act, implementing the first European Union Data Protection Directive of 1995, established a 'provision for the regulation of processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information'. Now, more than 20 years after the 1995 Directive, the European Union has issued the new General Data Protection Regulation 2016 which applies from 25th May 2018. The Regulation replaces the 1995 Directive and will be supplemented by a new UK specific Data Protection Act which, at the time of writing, is still making its way through Parliament. The new UK Data Protection Act extends the scope of the Regulation within the UK and also provides for UK specific derogations from the Regulation where this is permitted under the Regulation in certain circumstances.

The guidance contained in what follows is intended to provide some assistance to the application of these important changes within the lived experience of the Catholic Faith Community; particularly as encountered within the parish and diocesan setting. I am grateful to all those who have helped in the preparation of this guide which will assist the Catholic Church in this country fulfil the mission of salvation entrusted to her.

+ Vincent Nichols

Cardinal Vincent Nichols
President of the Catholic Bishops' Conference of England and Wales

CATHOLIC INSURANCE SERVICE LTD

BLAKE MORGAN

Index

1. Introduction

This Guide and the attached sample documents are intended to provide information and general guidance on data protection for Catholic Dioceses. These materials are addressed to diocesan Bishops and those who assist them in managing data protection throughout the diocese and in discharging the responsibilities of the diocesan Trustees as Data Controller. As a form of introductory guidance, the primary objective of this document is to explain the general principles which are intended to regulate the conduct of data processing.

We hope you will find the Guide helpful, but it should not be used as a substitute for obtaining legal advice to address specific circumstances and issues, nor should it supplant the detailed guidance notes issued by the Information Commissioner's Office. We recommend that you seek independent legal advice at an appropriate stage to ensure your Diocese has in place all the necessary policies and procedures to comply with the GDPR, and that those policies and procedures are sufficiently robust and consistent with your existing internal operational structures and policies.

The GDPR makes clear that those involved in the processing of personal data must be able to demonstrate compliance with their legal obligations. Whilst the production of policies is an initial step towards compliance, each Diocese must communicate those policies to all those who handle personal data in the Diocese, including staff, clergy and many volunteers, and ensure that they understand their responsibilities in terms of data protection. Measures should also be put in place to audit practice and compliance with the policies, and regular training should be delivered.

We consulted widely in the preparation of this Guide to try to ensure it is relevant and helpful to Dioceses and we would like to thank, in particular:

Dr E. Morgan	Barrister and Visiting Professor, Faculty of Canon Law, Leuven
Fr Christopher Dawson	Diocese of Salford
Sarah Williams	Diocese of Shrewsbury
Clare O'Brien	Diocese of Birmingham
Brin Dunsire	Diocese of Northampton
Clare Losty	Diocese of Brentwood
Tim Redding	Diocese of Northampton
Paolo Camoletto	Diocese of Westminster

This Guide will be available to Dioceses via the Catholic Insurance Service website. Any Dioceses who are happy to share documents and resources which they have prepared in relation to GDPR, (e.g. completed data audits and Privacy Notices), are welcome to send copies to CIS so that they can also be uploaded onto the website to create a resource area for Dioceses.

Kathy Perrin
Chief Executive Officer
Catholic Insurance Service

Sheilah Mackie
Partner
Blake Morgan

2. Data Protection and the "General Data Protection Regulation" 2016 ('GDPR')

It may surprise some to know that there have been data protection laws in the UK since 1984. These laws regulate how organisations, including charities such as Dioceses, collect and use information about living people. Data protection laws are designed to protect people's privacy by:

- ensuring organisations protect individuals' rights and their personal information; and
- allowing individuals access to the information which organisations hold about them.

During the course of your activities Dioceses collect, store, use and otherwise process personal information about the people with whom you interact. This may include information about parishioners, clergy, volunteers, employees, contractors, suppliers and other third parties.

This means that Dioceses, in the same way as other charities and organisations, must comply with data protection laws. Ensuring that personal information is properly and securely managed is also an important part of achieving trust and confidence between Dioceses and with those with whom you interact.

Dioceses are responsible for ensuring that all personal data used by staff, clergy, volunteers and others on behalf of the Diocese – whether they are using Diocesan equipment and systems or personal devices - is processed in a way which is compliant with data protection legislation.

On 25th May 2018, the Data Protection Act 1998 will be superseded by the General Data Protection Regulation 2016 ('GDPR'). The GDPR places great emphasis on transparency when dealing with personal data, puts more onerous obligations on organisations handling personal data and includes much higher penalties for those who fail to comply with the legal requirements in respect of the security and handling of personal data. This Guide is intended to assist Dioceses in understanding the new legal duties and to put in place policies and procedures which will help them to comply with the new legislation.

3. Terminology

Data includes information processed wholly or partly by automated means e.g. via computers and other technology, and on paper if it is, or is intended to be, held in an organised filing system (e.g. paper files organised in alphabetical (or any other kind of) order).

Personal Data is information about a living individual, who can be identified from that data or from that data and other data in your possession. It includes facts and opinions.
Personal data therefore includes information about a living individual held in paper files or on a PC/laptop/tablet computer, portable storage media (e.g. memory sticks and external hard drives) or smartphones. The data could be contained in Word documents, Excel spreadsheets, emails, databases, text messages or voicemail recordings.

Personal data also includes images of living people who can be identified, so CCTV images, photographs and video images, telephone calls (recorded or live streamed) are included.

Special Categories of Personal Data (formerly Sensitive Personal Data) includes information about an individual's racial or ethnic origin; religious, political or philosophical beliefs; sexual life or orientation; biometric data and health conditions.
Dioceses process a lot of Special Category personal data, including data revealing individuals' religious beliefs (e.g. baptism registers), information about health conditions of parishioners or employees and safeguarding records.
Information concerning an individual's criminal convictions and offences are now treated separately and are subject to even more stringent rules than Special Categories of data.

Processing is anything that you do with or to the data, including viewing; editing; organising; combining; sharing; storing and deleting it.

The **Data Subject** is the individual to whom the data relates. So, if you hold a personnel file for a parish secretary, the parish secretary will be the Data Subject in respect of that information. Data Subjects must be living individuals and the GDPR, like the Data Protection Act 1998 before it, does not apply to deceased individuals.

A **Data Controller** is a legal person who determines the purposes for which and the manner in which data is to be processed. For Dioceses, this will usually be the Diocesan Trustees, but it will depend on the legal structure of the Diocese. It is vital that the Trustees are trained in their data protection responsibilities.

Data Processors are third parties who process data on behalf of the Data Controller, (e.g. a payroll provider which processes the diocesan payroll or a cloud-based IT service which is used to store personal data). If you use any Data Processors, which is almost certainly going to be the case for most Dioceses, please read the relevant section below.

4. The Six Data Protection Principles

Underpinning the GDPR are six principles with which organisations must comply. These provide that personal data must be:

1. Processed fairly, lawfully and in a transparent manner.

You must identify the legal basis on which you are relying to process each category of personal data and you must inform Data Subjects what you are doing with their personal data by giving them a 'Privacy Notice'.

2. Collected for the specific purposes about which you have informed the data subject and not used for any other purposes.

For example, if you collect personal data about a job applicant, you cannot then use that data to send them news about the Diocese and its activities. You can, however, use data for further purposes if those further purposes are not incompatible with the initial purposes notified to the individual. For example, if another job vacancy arises, it would be acceptable to notify unsuccessful applicants of the new vacancy. Retention of data for archiving or historical purposes is also acceptable.

3. Adequate, relevant and limited to what is necessary to achieve your stated purposes.

Ensure the data you collect is really needed for the purpose for which it is collected, e.g., you do not need details of a parishioner's medical history, GP or next of kin to send them a newsletter, but you may if they are going on the Diocesan pilgrimage to Lourdes.

4. Accurate and, where necessary, kept up to date.

Procedures should be put in place to ensure that all personal data is be checked at appropriate intervals to ensure it is still required for the purpose for which it was obtained and that it remains accurate. Any data which is out of date or inaccurate should be corrected promptly and data which is no longer required should be securely deleted or destroyed. Please note this does not require historical archives to be corrected or overwritten.

5. Kept in a form which permits identification of data subjects for no longer than is necessary to achieve your stated purposes.

The GDPR does not specify for how long different categories of personal data should be kept. The Diocese should determine its own retention periods for all categories of personal data and ensure records are securely destroyed when they are no longer required. However, even before its destruction date, data may be able to be anonymised or have identifying details minimised, which will help to protect individuals' privacy.

6. Kept safe and secure. This includes protecting the data against unauthorised processing and against accidental loss, destruction or damage.

Security of data is imperative. As so much personal data is stored electronically, you need to ensure your IT systems are secure against malicious attacks and that you have appropriate IT security systems and procedures in place to guard against accidental loss or disclosure, but don't forget physical security measures such as locking away paper files too and ensuring that offices where data is stored are kept locked when not occupied or in use.

Dioceses must put adequate policies and procedures in place, covering such matters as:

- Restricting access to personal data to those with a 'need to know';
- IT Security, Acceptable Usage and Password policies;
- Adopting a 'clean desk' policy and ensuring paper records are stored in locked cabinets;
- Ensuring that paper documents are securely shredded and electronic data is securely deleted;
- Remote working and use of personal and portable electronic devices to ensure that personal data accessed away from curial or parish offices is subject to appropriate security measures, including keeping paper files away from public visibility, the use of passwords/passcodes, encryption and secure storage (e.g. not left in the boot of a car).
- Ensuring staff and others are trained not give out personal data over the telephone unless in very limited circumstances where they know or can verify the caller's identity and their entitlement to receive the information requested;
- Ensuring personal data is securely packaged and sent by the most appropriate means (e.g. special delivery, courier or hand delivery).

5. Accountability

As mentioned above, the Diocesan Trustees will usually be the Data Controller for a Diocese (this depends on your legal structure). The GDPR introduces the concept of 'accountability' in data protection and states that the Data Controller "*shall be responsible for, and be able to demonstrate, compliance with*" the data protection principles.

This means that all Diocesan Trustees should be trained in their data protection responsibilities and should implement a programme of training for those who handle personal data throughout the Diocese; they should approve the Diocesan policies and procedures and audit compliance, and they should ensure adequate resources are allocated to data protection management. Each of these steps should be recorded in order to demonstrate compliance, as required by the GDPR.

Although under the GDPR there will no longer be a requirement for Data Controllers to register with the Information Commissioner's Office ('ICO'), a new annual data protection fee will be introduced which Data Controllers will have to pay. At the time of writing the final model has not been approved by Parliament.

6. Data Protection Officer ('DPO')

Under the GDPR, in certain circumstances, organisations are required to appoint a DPO. This includes where special category personal data is processed on a 'large scale'. Although it is not absolutely clear that Dioceses must appoint a DPO under the legislation, on balance, we consider that Dioceses are best advised to appoint a DPO because they process a lot of information which reveals individuals' religious beliefs (e.g. parish registers).

The duties of a DPO include:

- To inform and advise the Diocese about its obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training clergy/staff and conducting internal audits; and
- To be the first point of contact for the ICO and for individuals whose data is processed (clergy, employees, volunteers, parishioners etc.).

Where a DPO is appointed, the Diocese must ensure that:

- The DPO reports to board level, (i.e. directly to the Trustees);
- The DPO operates independently and is not dismissed or penalised for performing their task;
- Adequate resources are provided to enable the DPO to meet their GDPR obligations; and
- The individual acting as DPO is not dismissed from that role due to carrying out their duties under the GDPR.

Whilst the GDPR does not specify the precise qualifications a DPO is expected to have, it does require that they should have expertise in data protection law and an in-depth understanding of the GDPR. Knowledge of the Catholic Church and of the structures and activities of Dioceses will also be crucial.

The role of DPO can be allocated to an existing employee provided the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. This is likely to mean that no member of senior staff who is responsible for determining the purpose and means of any data processing can take on the role of the DPO (e.g. Financial Secretary, Chancellor, Head of IT or HR). You can also contract out the role of DPO externally.

If you decide not to appoint a DPO, the Diocese must document its reasons for not doing so and should consider appointing a Data Compliance Manager or at least allocating responsibility for data protection compliance to a specific person.

7. Lawful Bases for Processing Personal Data

Before collecting any personal data, you must always identify what lawful basis you have for processing the data and the purpose for which it is to be processed. Both should be recorded on your Data Processing Record against the data in question (see below).

There are six lawful bases for processing and which basis is most appropriate in each case will depend on your purpose and your relationship with the data subject. Remember that, if you can reasonably achieve your purpose without collecting any personal data, you will not lawfully be able to collect the personal data.

The lawful bases for processing are set out in Article 6 of the GDPR:

(a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose.

The GDPR sets a high standard for consent. It must be freely given, specific, informed, active, explicit and able to be withdrawn. For example, individuals should be asked to tick a box and sign to confirm their consent to particular actions. If you rely on consent, you must keep a record of when and how the consent was given.

It is preferable not to rely on consent where possible because it is difficult to achieve the standard of consent which the GDPR demands and consent can be withdrawn at any time, which can cause difficulties. We have provided sample consent forms suitable for use in certain situations where you do need to process data based on consent (e.g. to share news of parish events and fundraising activities).

(b) Contract: the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract.

An example of this would be obtaining an employee's bank account details in order to make their salary payments, which you have to do under their contract of employment.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

In some circumstances, for example, you may be under a legal obligation to report certain personal data to the statutory authorities or to HMRC.

(d) Vital interests: the processing is necessary to protect someone's life.

Note that this only applies in 'life or death' situations, (e.g. you could inform paramedics of an individual's medical condition if they are unable to do so).

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
This would include maintaining marriage records.

(f) Legitimate interests: the processing is necessary for the Data Controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
Dioceses are likely to rely on this lawful basis for much of their personal data processing, including the processing of personal data about parishioners and volunteers by parishes, so that volunteer rotas can be compiled and information about the parish can be provided to parishioners. However, Dioceses must be aware that when communicating unsolicited "direct marketing"[1] materials to parishioners, separate rules relating to marketing must be complied with if the method chosen to do so is electronic (e.g. email newsletters or appeals for fundraising).

Once you have identified the lawful basis for collecting a particular category of personal data, you should record it and include it in the Privacy Notice you issue to the data subject.

8. Processing Special Category Personal Data

Dioceses will process special category data (e.g. data revealing a person's religious beliefs, medical conditions and safeguarding information). For such data, you need to identify both a lawful basis for processing (set out above) **and** an additional condition under Article 9 for processing this type of data. The most relevant condition will be that you have the explicit consent of the data subject or because the processing is required to establish, exercise or defend legal claims or under the substantial public interest ground (the latter ground being expanded in detail in the UK Data Protection Bill).

However, there is a 'charities' condition which means that consent is not required where special category data is being processed:

- in the course of the Diocese's legitimate activities;
- with appropriate safeguards;
- relating solely to the members or former members of the Diocese or to persons who have regular contact with the Diocese in connection with its purposes; and
- the personal data are not disclosed outside the Diocese without the consent of the data subjects.

[1] 'Direct Marketing' means the communication of advertising or marketing material to individuals. It is not just about selling goods and services, but includes promoting the aims and ideals of not-for-profit organisations. Where Dioceses and parishes undertake direct marketing, they must ensure that the required consent has been obtained and the direct marketing rules are adhered to. For example, particular care must be taken when communicating by text or email. It is beyond the scope of this guidance to address the direct marketing rules and dioceses are referred to the ICO guidance on the Privacy and Electronic Communications Regulations ('PECR'), which govern direct marketing by electronic means.

Where all the above conditions apply, the data may be processed without consent provided there is a lawful basis for doing so under Article 6 (see above).

Consider the example of a list of parishioners held by a parish and used to inform the parishioners about Mass times and parish events. This data should be considered to be special category data because it (at least arguably) reveals the religious beliefs of the data subjects. The lawful basis for processing this data is that it is necessary for the legitimate interests of the Diocese in advancing and maintaining the Roman Catholic faith. Although it is special category data, the data subjects' consent should not be required provided the list relates solely to members of the parish, will not be disclosed outside the diocese and is kept safe and secure. However, if the parish wanted to share this list with others, (e.g. a fundraising company or the Bishops' Conference), or if the parish intended to use the list to send the individuals 'direct marketing' information via email or text message, each data subject's consent would be required.

Another example would be information kept by a parish priest in paper files or on computer about parishioners and their pastoral needs. This information may include details about parishioners' health conditions and notes made by the priest containing his personal views of the parishioners' needs. This is personal data which the priest needs to hold in order to fulfil his duties as a priest. It is therefore in the Diocese's 'legitimate interests' to hold this data, but as it includes special category data an additional ground for processing needs to be met. Provided the priest:

- ensures that the information is kept securely (e.g. in a locked or password protected file),
- the information relates to parishioners who have regular contact with the parish, and
- the information is not disclosed to any third parties outside the diocese without the explicit consent of the parishioners

the priest can rely on the 'charities' ground above and will not require parishioners' explicit consent to keep these records.

9. Processing Data about Criminal Convictions and Offences

The processing of data about an individual's criminal convictions and actual or alleged offences is dealt with separately from special categories of personal data. The GDPR prohibits any processing of this data unless it is specifically authorised by the UK (or other relevant Member States') law and that law provides appropriate safeguards for the rights and freedoms of data subjects.

The new UK Data Protection Bill that is currently making its way through Parliament will set out various grounds on which criminal conviction and offences information can be processed. This is likely to include in relation to employment, the prevention or detecting of unlawful or dishonest acts, the provision of counselling, insurance and pension issues, processing by not for profit bodies, defending legal claims or to protect an individual's vital interests.

10. Data Subjects' Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Whilst all Dioceses must be able to demonstrate a clear commitment to the rights of data subjects, it is important to bear in mind that Dioceses will, on occasion, come into possession of personal data pursuant to data sharing arrangements with statutory authorities and agencies (e.g. in connection with safeguarding matters and DBS applications). When engaging with the rights of data subjects, and particularly requests from data subjects, care should be taken to ensure that any ongoing statutory obligations are complied with and guidance may need to be sought from the relevant authorities.

Children have the right to exercise all of the rights given to data subjects under the GDPR. While in England there is no strict rule as to what age a child must be in order to exercise their rights, children from 12 years upwards are generally taken as being able to make their own decisions (although consideration must be given to the child's level of understanding and capacity). This means that parents, guardians or other family members cannot make requests for children from 12 years upwards in most cases unless the child does not have capacity or the child has given their express permission for someone else to make a request on their behalf.

We provide some guidance on the right to be informed and the right of access below, as these are rights that will be exercised most commonly by data subjects. It is beyond the scope of this guide to set out information about each of the other rights, but Dioceses can refer to the ICO's guidance and must ensure their DPO has the necessary knowledge and expertise to deal with requests from data subjects.

10.1 The Right to be Informed & Privacy Notices

As under the Data Protection Act, the GDPR requires data controllers to give data subjects “fair processing information”. This is part of the requirement for organisations to be transparent when processing personal data and it is usually dealt with by issuing data subjects a "Privacy Notice when collecting their personal data. It is also good practice to make your general Privacy Notice available via your website so that it is readily accessible to all individuals you interact with.

The GDPR sets out the information that you should provide and when individuals should be informed. This depends on whether or not you obtained the personal data directly from individuals. Privacy Notices must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The ICO have prepared a helpful table which summarises the information you should supply to individuals and at what stage. Please see:

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

Short form Privacy Notices should be used to make clear what information is being collected in each individual circumstance with reference made to Diocese's full Privacy Notice; this is to ensure that data subjects are not overloaded with information but are given a summary of, for example, for what purposes the information they are providing will be used by the Diocese.

For example, Privacy Notices should be used when asking individuals to complete a parish census or a Gift Aid form, or when they provide information to participate in a Diocesan pilgrimage. It is a good idea to review all the forms Dioceses use to collect personal data from individuals to ensure they have appropriate Privacy Notice s on them and to destroy old copies of the forms to ensure they are no longer used. Asking parishes to use common forms supplied by the Diocese will assist in ensuring compliance. A sample full Privacy Notice as well as short form Privacy Notices which can be adapted for different purposes are provided.

10.2 The Right of Access

Under the GDPR individuals have the right to access their personal data being processed by a Diocese. These are known as Subject Access Requests ('SARs'). When supplying individuals with their personal data, the Diocese also has to provide supplementary information (the information that is generally supplied in a Privacy Notice). The purpose of the right of access is to enable data subjects to check the accuracy of the data and the lawfulness of the Diocese's use of the data.

It is important that everyone dealing with personal data in the Diocese is aware of the right of access and can recognise a SAR, but we suggest the Diocesan policy provides that the DPO will deal with all SARs so that all clergy and staff need to do is to recognise an SAR and refer it immediately to the DPO. SARs must be made in writing, but please note this includes email and social media. Requests do not need to be addressed to the DPO, they can be made of any representative of the diocese, nor do they need to refer to "subject access" or the GDPR.

Once a request is received, it should be acknowledged promptly. The first step is to check and verify the identity of the person making the request. This is particularly important because you can only give an individual their own personal data, you cannot disclose to them personal data about another person. Often you will know the data subject who makes the request but, where you don't, you may also need to ask them to identify what data they think the Diocese holds about them (e.g. they trained for the priesthood a number of years ago but weren't ordained, so the Diocese may still hold a file about them).

Remember that, as the Diocese is the data controller, technically a subject access request covers all the data held by the Diocese. In some cases, this could amount to a huge amount of data, for example, if a person has lived in the Diocese their whole life, has been actively involved in several parishes and perhaps even employed by the Diocese. Their request would cover all the information held in the Diocesan curial office as well as the parishes. Normally, when a subject access request is received, the data subject wants a particular set of data. Where a lot of information is involved, you can ask the data subject to identify and so limit the data they want, but they are not required to do so.

Once you have confirmed the data subject's identity and know what data you are looking for, the time for complying with the request will begin. Information must be provided 'without delay' and at the latest within one month after the date of receipt of the request. You cannot charge a fee (except in limited circumstances). The length of the month varies depending in which month you received a request. For example, a request received on 20 March would have until 21 April to be complied with. If the 21 April falls on a weekend, the deadline is extended to the next working day.

As you cannot provide personal data about anyone else to the data subject, you must be careful to ensure that, when preparing the data to disclose to the data subject, you have the consent of any third parties to give their personal data to the data subject. If not, you will need to consider whether it is reasonable in all the circumstances to give that personal data to the data subject (e.g. it is information already known to the data subject).

There are also exemptions which apply to SARs in some circumstances, including data which is subject to legal privilege or would be likely to prejudice a criminal if disclosed. Dealing with SARs can be complex and legal advice may be required in many cases.

11. Data Processors

Data controllers must only appoint data processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. Processors must only act on the documented instructions of a controller, but they will also have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply with those direct responsibilities.

Where Dioceses use third parties to process personal data held by the Diocese (e.g. an external payroll provider), a written contract must be put in place so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract and we have provided a checklist as well as a sample Data Processing Agreement. In the future, standard contract clauses may be provided by the European Commission or the ICO and may form part of certification schemes. However, at the time of writing no standard clauses have been drafted.

12. Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include where someone unauthorised gains access to personal data, such as a ransomware attack; sending an email containing personal data to the wrong person and electronic devices or paper files containing personal data being lost or stolen. It also includes data becoming unavailable, for example, someone losing the key to a filing cabinet with personal data in it or a password for a database being unavailable because the only person who knew it has left the Diocese without passing it on.

The ICO advises that there will be a personal data breach whenever any personal data is lost, corrupted or mistakenly destroyed or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this **within 72 hours** of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individual data subjects (e.g. the breach could result in financial loss, breach of confidentiality or any other significant economic or other disadvantage), you must also inform those individuals without undue delay. We have prepared a data breach flowchart to help you identify what breaches need to be reported to the ICO and to data subjects.

You should ensure you have robust breach procedures in place so that everyone knows what to do if they suspect there has been a data breach. You are also required to keep a register of any personal data breaches, regardless of whether you are required to notify the ICO about them. Again, sample documents are provided.

Failure to comply with the breach notification procedures is a breach of the GDPR in its own right and can attract separate fines from those that may be imposed for the initial data breach.

13. 10 Key Steps towards Compliance

This step by step guide is intended to assist Dioceses in understating their new legal duties and to put in place policies and procedures which help them to comply with the new legislation.

1	**Decide who will be responsible for data protection**	The Diocesan Trustees will in most cases have overall responsibility for data protection compliance within the Diocese, so they should receive training and formulate a compliance plan. The next step should be allocating responsibilities. Someone independent should take responsibility for compliance with data protection legislation and should have the knowledge and authority to do this effectively (see above on Data Protection Officers). This individual can be internal or external and can be helped by a wider team. For example, you may want to consider whether specific individuals in different departments should be allocated some data protection responsibility (e.g. the Head of HR could be responsible for compliance within the HR department, and someone in each parish could be nominated to be in charge of data protection in the parish). A structure chart could be prepared to clearly show responsibilities and reporting lines.
2	**Update your Policies & Notices Policies**	Have clear, practical policies and procedures on information governance for staff to follow. It is not enough to circulate policies, you must also monitor their application to ensure they are being followed in practice. A GDPR compliant data protection policy and privacy notice is the first step. Adapt our samples for your diocese or update your existing versions. This will need to be supplemented by other policies, for example, an IT Security & Password Policy, a Bring Your Own Device Policy and so on. We have provided some samples to help you.
3	**Raise awareness & arrange training**	With the introduction of GDPR it is crucial that everyone has an awareness of their data protection responsibilities. We would not suggest trying to make everyone who handles data in the diocese an expert in data protection. The DPO must have an appropriate level of knowledge and training. Clergy, staff, volunteers and other key data users in all areas of the Diocese need to know enough to recognise any data protection issues (e.g. a data breach or subject access request); to make good decisions about

		what they need to do to be compliant in their area (e.g. keeping records secure and using strong passwords), and where to turn for advice. Ensure everyone undergoes training appropriate to their role and that records of all training are kept.
4a	**Undertake a Data Audit**	Each 'department' within the Diocese (e.g. HR, Finance, parishes) should complete a data audit. A sample form is attached to help you with this process. This will help the Diocese to identify what personal data is held where in the Diocese, and for what purpose. (We do not recommend asking all parishes to complete a data audit, a selection of parishes should be sufficient unless you are of the view that each will hold very different types of information). Once you know what data you collect and process, you can then ensure you deal with it properly. The audit can be used to check whether all records are held securely, to set appropriate retention periods (and then to securely delete/destroy data no longer required) and to identify where agreements with third party data processors need to be checked and/or privacy notices need to be issued. You should document your findings because the GDPR requires data controllers to keep records of their processing activities. You should also record if you share data with any third parties.
4b	**Identify and document your 'lawful basis' for processing data**	To legally process data under the GDPR you must have a 'lawful basis' to do so. Please see above for more detail. Don't forget that you also need an additional condition where you process special category personal data. You must understand and document your lawful basis for processing each category of personal data when you undertake your data audit. If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under the GDPR, consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent, instead people must positively opt-in. Remember that marketing rules apply additionally where you want to contact individuals for fundraising or promotional purposes. Generally, you should only rely on one processing ground per purpose and you should not change this after you have collected the personal data, e.g., if you opt to process on the basis of consent but then encounter problems with demonstrating GDPR compliant consent you cannot simply

		switch to relying on legitimate interests. If you're not sure that your existing ground will hold up under the GDPR, there is a one-off opportunity to change to another lawful ground before 25th May 2018.
5	**Review your security systems**	Your data audit will highlight any concerns regarding the security of the personal data which you hold. These may be as simple as ensuring paper records are stored in locked cabinets or passwords are not shared. You may also wish to undertake an IT security review to ensure that your IT systems and processes are keeping data as securely as possible to minimise the likelihood of a data breach. Simple steps such as putting up posters reminding people to log off PCs, keep passwords secure and not to leave paper documents unattended on desks may help to develop a culture of data security within the diocese. Some steps you can ask parishes to take are: 1. Ensure the operating system on parish PCs is up to date; 2. Check they are using reputable anti-virus software; 3. Ensure they regularly check for and download updates; 4. Consider encrypting mobile devices; 5. Set strong passwords, change them regularly and don't share them with anyone.
6	**Set Retention Periods**	Under the GDPR, you must not keep data for longer than you need it for the purpose for which it was originally obtained. We recommend that you set a retention period for each category of personal data that you process and ensure those retention periods are applied consistently throughout the Diocese. A sample basic retention schedule is provided.
7a	**Privacy Notices**	When you collect personal data, you must always tell people in a concise, easy to understand way how you intend to use their data. Privacy notices are the most common way to do this and your data audit will identify when you need to issue an appropriate privacy notice. Under the GDPR, privacy notices must give detailed information such as how long you will keep data for and what lawful basis you have to process data. Generally, you will need to put a short privacy notice on all documents which you use to collect personal data, and these should refer to the Diocese's full Privacy Notice, which should be put on the Diocesan website (with links from parish

		websites). For more information, please see our sample privacy notices.
7b	**Build in extra protection for children**	Privacy notices should be written in language that children can understand if you are collecting information from them. Remember that children from 12 years upwards are generally seen as being able to understand their rights and exercise them rather than by way of a parent or guardian.
8	**Put in place agreements with Data Processors**	A list of third parties who process personal data on behalf of the diocese (data processors) should be compiled and the contracts in place should be updated to ensure compliance with the GDPR. This may include, for example, payroll and occupational health providers. You must make data processors process the data you provide them with securely. Firstly, consider how you select suppliers and carry out appropriate due diligence. Then, ensure your contracts are updated to include the GDPR required clauses or put in place a separate Data Processing Agreement, and consider an audit programme to supervise them. For more information please see our Data Processor Checklist and sample Data Processor Agreement.
9	**Personal Data Breaches**	You need to be able to demonstrate that you have appropriate technical and organisational measures in place to protect against a data breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned, so you will also need to have the right procedures in place to detect, investigate and report a breach. The Data Protection Officer needs to be recognised by data users as the person to whom any breaches should be reported. They therefore need to be briefed on the procedure for dealing with data breaches. All data users should be briefed on personal data breach avoidance, and on what to do if a breach occurs. For more information please see our sample Data Breach Procedure and associated forms.

10	**Build data protection into your new projects**	The GDPR introduces the concept of "Privacy by Design", which means building data protection into all your new projects and services. It has always been good practice, but the GDPR makes privacy by design an express legal requirement. To achieve this, Data Protection Impact Assessments (DPIAs) should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or Special Categories of data will be processed on a large scale. Agree who will be responsible for carrying out DPIAs, when you will use them and how to record them. See the ICO website for further guidance.

14. Top 10 Frequently Asked Questions

1. Can we continue to keep Parish Registers, and can we allow people to access them, e.g. to research their family history?

Parishes will maintain Registers of baptisms, marriages and deaths. These records should continue to be kept in the same way as always. If an individual asks for, e.g., a copy of their baptism certificate, this is not a Subject Access Request and should be responded to in the usual way. However, please note that individuals are not entitled to see information in Registers which does not relate to them, so you should not allow individuals to see any pages in a Register as this will contain multiple entries and so information about numerous people. For convenience and to minimise risk, it is suggested that those researching their family history should be directed to publicly available sources of information where possible.

2. What about fundraising?

It is recognised that within a Diocese or parish, activities may be undertaken which involve the processing of personal data for purposes which are complementary to Church participation and membership and that, from time to time, these may involve direct marketing (e.g. fundraising appeals or information about events). Any use of personal data for marketing (including fundraising) purposes must comply with both Data Protection legislation and the Privacy and Electronic Communications Regulations ("PECR") (and any replacement legislation) which govern marketing by electronic means, such as text or email.

The ICO has issued specific guidance in this area: “Guide to the Privacy and Electronic Communications Regulations.” In particular, the PECR requires that the Diocese has the prior consent of recipients in certain circumstances before it sends any unsolicited electronic messages for the purposes of fundraising, or for other marketing activities (e.g. events).

Individuals have a right to object to their personal data being used for direct marketing purposes and/or for profiling (including wealth screening). Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or fundraising communications must be sent to them and/or no further profiling or wealth screening must be carried out.
Fundraising and the PECR are outside the scope of this guidance, please seek separate advice on these issues.

3. What should we do when we conduct a Parish Census?

Many parishes send out census forms periodically seeking information about parishioners. If the census asks for the religious beliefs of those completing the form, it will be special category data and you will need the explicit consent of those completing the forms to process their personal data unless the parish will only use the information to contact the individuals about the parish by post and will not disclose their personal data to anyone outside the parish. The sample Privacy Notice on the Parish Census form we have provided can be used in these circumstances.

Even if the form does not ask for religious beliefs (or other special category personal data), if the information provided is to be used to send direct marketing to individuals by email or text message, explicit consent will still be required as a result of the PECR. Detailed guidance on the PECR is outside the scope of this guidance, please seek advice as necessary.

If you do rely on consent to process this information, you must tell people how they can withdraw their consent each time you communicate with them and, if they ask to be removed from the list, you must delete all their details promptly. This includes each individual whose details are collected on the form and not just the parishioner who completes the form.

If you are relying on consent to use information already collected from your parishioners, you will need to make sure that the consent given will meet the GDPR requirements for consent (i.e. freely given, specific, informed, active, explicit and able to be withdrawn). If it does not meet this threshold, you will either need to change to another processing ground or refresh your consents prior to 25th May 2018 by contacting those whose data is already held and asking them to confirm their consent to processing.

4. What do we need to do about Gift Aid forms?

We do not consider standard Gift Aid data to be special category data because lots of people donate to specific projects or appeals by Catholic Dioceses, but that does not necessarily mean they are Catholic and the data provided does not include their religious beliefs. Therefore, you can rely on 'legitimate interests' to process this data and will not need donors' consent provided:

Either

-you only communicate with the donors by post to confirm how much they have donated

Or

-you only communicate with the donors by post to confirm how much they have donated, to seek additional donations or to inform them about further events and/or appeals; **and**

- with each communication you give them an opportunity to 'opt out' of receiving further communications from the Diocese.

If at any stage you want to communicate with the donors by email, text message or other means covered by the PECR, you must have the donors' explicit consent before you do so. Note that you cannot contact an individual by email or text message in order to gain their consent to send further direct marketing emails or texts to them about fundraising activities – that in itself would be a breach of PECR.

5. Should Tribunals have a data protection policy?

The Christian Faithful participate within the life of the Church through membership. Admitted through the sacrament of baptism, each member of the Church is called to maintain bonds of communion. This communion is expressed through professions of faith, the sacraments and ecclesiastical governance: *Lumen Gentium* n4 and canon 205 of the Code of Canon Law. As with other denominations, the Church has established and maintained its own canonical Tribunals to determine, in accordance with its own laws, those issues which concern the freedom, eligibility and entitlement of members of the faithful to participate in the life of the Church, including but not limited to the reception of the sacraments and/or the exercise of forms of ministry. Each such Tribunal should formulate and adopt its own discrete data protection policy which should address and safeguard the rights of data subjects and the retention, safeguarding and retention of personal data. In formulating any such policy, particular care should be given to the demands of proportionality and transparency.

6. How does the GDPR interact with Canon Law?

The universal and particular Church enjoy rights of autonomy and self-determination which are recognised in civil law (e.g. Art 9 of the European Convention on Human Rights and Fundamental Freedoms). This autonomy finds primary expression in the Code of Canon Law 1983. The Code of Canon Law contains detailed provisions regarding the creation and retention of records, particularly in connection with reception of the sacraments. Whilst addressing issues of eligibility and membership, the Code also incorporates a number of means by which ecclesiastical governance is to be exercised. Specific mention is made of the right to privacy and duties of confidentiality. The provisions of the GDPR require that all and any personal data processed in accordance with governance procedures are processed in line with the principles set out earlier in this document. This will require each chancellery, Judicial Vicar or other canonical appointed delegate to ensure that such data are processed in line with those principles with particular care being given to the additional measures of protection applicable to special categories of data, the adoption of necessary data sharing protocols and

the obtaining of appropriate assurances from those exercising canonical jurisdiction as to the systems, measures, safeguards and protection applied to such data.

7. Do we need to worry about personal data held by schools?

Schools, including Voluntary Aided schools and Academies, are data controllers in their own right and will need to comply with the GDPR in respect of the personal data they collect and process. However, Dioceses may hold personal data about individuals connected to schools (e.g. personal data about prospective foundation governors or headteachers), and personal data may be shared between Dioceses and schools for various reasons. Dioceses must ensure that they carefully consider in what capacity (i.e. Data Controller/Joint Data Controller/Data Processor) they process such personal data and share it with schools. Any such personal data held by Dioceses should be included in the Diocese's data audit and addressed as appropriate in their Privacy Notices.

8. How are CCTV, photographs and live streaming affected?

If you wish to use, or to continue to use, CCTV, you should undertake and document a risk assessment to assess whether its use is necessary and proportionate. Ensure the cameras do not intrude on anyone's privacy (e.g. overlook a back garden), that the footage is kept securely and cannot be accessed by anyone who is not authorised to view it and review the retention period for the footage. Also, ensure correct signage is displayed warning of the use of CCTV and stating who the data controller is, with contact details. Both the ICO and the Security Camera Commissioner have issued codes of practice on the use of CCTV, which should be complied with where a Diocese uses or intends to install CCTV cameras.

In you take photographs or live stream services or events, you should bring people's attention to this beforehand. Display a sign in the parish advising that, on occasions, there may be photographers present at church services and, by attending those services, individuals give their permission for use of any general crowd shots they appear in for parish or Diocesan printed publications and websites. Display specific signs prominently on days when photographs are being taken or live streaming is taking place. Alternatively, make people aware of where they can be seated to avoid or minimise the risk of them being included in any footage or photographs if they so wish.

You should not use individual or small group shots of people without asking for consent first.

9. Can I send personal data abroad?

The GDPR provides that personal data should not be transferred outside of the European Economic Area ('EEA') unless the country to which it is being transferred provides an adequate level of protection for the processing of individuals' personal data.

This means that data can freely be sent to countries in the EEA, which include countries within the EU plus Norway, Liechtenstein and Iceland. In addition, a number of countries have been 'whitelisted' on the basis that they also offer an adequate level of protection for data subjects' rights. At the time of writing, the European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

Should you need to send personal data to other countries, you must take additional steps and you are likely to require the data subject's explicit consent. Where a Chancellor needs to send information to another Diocese about a couple wishing to marry abroad, for example, he will need to ask the couple to sign to confirm they consent to the data being transferred to the country in question in the knowledge that it is not regarded by the EU as having adequate safeguards in place to protect personal data. The Chancellor should also explain to the couple what steps he will take to protect the personal data being sent.

Another example may be where a Diocese uses a cloud-based IT provider. The Diocese must undertake due diligence on the provider including ascertaining whether any personal data will be transferred or stored outside the EEA and must ensure that the provider can demonstrate compliance with the GDPR. The IT provider is likely to be a Data Processor and so the diocese should also follow the guidance in relation to data processors set out above.

10. What do we need to do about processing employees' personal data?

In recent years, the term 'employment' and the question of who is in fact an employee has undergone particular change. A person may be treated as an employee for some legal purposes and not for others, whilst the very notion of employment varies dependent upon context. For the purposes of this guidance, the term should be taken to mean not only those who are actually employed by the Church, but also volunteers, workers and office-holders (e.g. clergy).

As with many other faith communities, the Dioceses rely heavily upon the invaluable contribution provided by each of these categories of individual, whether as an unpaid volunteer or on a paid basis. The processing of personal data about such individuals is likely

to require careful regulation across a range of organisational policies (e.g. recruitment and selection, DBS clearance, Sickness Absence, Safeguarding, Disciplinary, Data Protection and Occupational Health etc.). Dioceses must ensure that, in each case, a clear record of the legal basis for processing the relevant data (and the purpose for which it is processed) is recorded. These operational policies will require revision along with any Employee or Volunteer Handbook to ensure that the standards required, and the obligation imposed upon the data controller to demonstrate compliance, are evidenced. In addition, consideration will need to be given to the revision of any disciplinary codes, electronic communications and IT policies, to ensure that the potential for data breach (and its consequences) are addressed, particularly in the context of 'remote working' and the use of personal and portable electronic devices. Please see our sample IT Security and Bring Your Own Device policies for assistance.

It should be noted, in particular, that it will not be possible to rely on consent in relation to most employee data processing given the need for consent to be freely given, which is largely impossible in the employment context due to the clear imbalance in the employer-employee relationship. Consequently, employment contracts will need to be reviewed and a separate privacy notice for employees and volunteers should be prepared. It is recognised that the Dioceses have their own forms of contracts and associated HR documentation in place, and so and we suggest you work with your legal/HR advisors to produce a data protection policy and privacy notice for employees (and for job applicants), to review your employment contracts, and update your policies as necessary.

15. For Further Guidance

General guidance on the GDPR:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Guidance on fundraising and direct marketing:

https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

https://www.institute-of-fundraising.org.uk/about-us/news/institute-of-fundraising-launches-new-gdpr-guide-and-training/

Please also see our Resources folder for materials kindly shared by other dioceses.