DIOCESE OF OXFORD

Data Protection

GDPR: a 20 Minute Guide for Churches

About this Document

This document gives churches a quick (around 20 minutes) introduction to the new data protection law known as GDPR (General Data Protection Regulation). It contains definitions, an explanation of the key concepts of GDPR, steps to gain compliance to GDPR and pointers to some useful reference sources for more detailed information. This will not give you an in-depth, complete understanding of how GDPR applies to your parish, benefice or deanery. However it should help you grasp the basics, to help you get going faster than if you started from scratch.

Contents

1 Introduction

On 25th May 2018 new, tighter, data protection regulation came into force across the EU. This is known as GDPR (General Data Protection Regulation), plus the DPA 2018 (Data Protection Act 2018) which is UK law. In this document we'll simply use 'GDPR' to describe the whole thing.

This document gives a high-level summary of the data protection law, as it applies to us now, with reference to parishes and deaneries in the Church of England.

In order to arrive at balanced, wise judgements on what GDPR compliance looks like for you in your parish/benefice/deanery, there is no substitute for investing some hours in finding out what GDPR is, plus reading a few good reference sources. Some have cut and pasted others' documents (and this can be a good start), but without some understanding of the new legal framework, you might just be copying someone else's mistakes without realising it. Through a lack of understanding, some have arrived at unreasonable or excessive conclusions (indeed, you might consider this to be a sign that your thinking has gone astray). Ultimately you need to interpret what is required for your parish/benefice/deanery. It will require some reading and research: hopefully this document will get you there faster.

2 What is the Point?

GDPR is, to many peoples' minds, a huge burden of unnecessary bureaucracy. It has emerged in response to large organisations, high-profile data scandals (like the Cambridge Analytica case) and to combat the risk of identity fraud. Churches and small charities are caught up in this as well, however there are some benefits to us:

- It encourages good practice in handling data. The church operates on high levels of trust, which is clearly a good thing, however we sometimes stray into high-risk situations without realising. GDPR makes everyone more aware of what good practice looks like when handling personal data.
- It keeps us in touch with the expectations of wider society. Those who have just occasional contact with us (such as baptism families and wedding couples) will expect to see that we work to high ethical standards and keep within the law.

The increased financial penalties for non-compliance with GDPR have been well-publicised, but are very unlikely to affect parishes and the ICO have stated it is not their aim to catch us out. Nevertheless we are not exempt from the law and we should not be complacent: at least one national Christian charity was fined a considerable sum for inadequate data protection practice recently.

The rest of this document contains:

- **Definitions**: a list of specific terms which are used in the area of data protection.
- **Explanation of GDPR**: a very brief (and therefore incomplete) summary, where I hope to give you the key information about GDPR which you need to know, to get you going.
- **Reference sources**: good places to go for more information.
- **Next steps**: a pointer to how to move forward.

3 Definitions

Here we define the key words and phrases associated with data protection.

3.1 ICO: Information Commissioner's Office

The ICO is the independent regulatory body which deals with data protection in the UK. They advise on compliance to data protection legislation, handle complaints and may undertake audits of organisations. In more serious cases the ICO can serve enforcement notices, financial penalties and prosecute where a criminal offence has occurred.

The most helpful thing the ICO provide is an online Guide to GDPR, which is long and detailed but well-indexed, searchable and a definitive source of information on GDPR.

3.2 Data Subject

The person which the data is about.

3.3 Personal data

Personal Data is any information about a living individual, which is capable of identifying that individual. Bear in mind the context in which the information appears:

- 'John Smith' in Oxfordshire doesn't identify a living individual (it identifies a few hundred probably)
- 'John Smith' in Reading identifies around 80 people (so again, not personal data)
- 'John Smith' in St George's church PCC is going to identify an individual person, so in this context it is Personal Data

This example also illustrates some of the difficulty in interpreting data protection law, because it is often context-dependent.

Don't forget, personal data can be:

- on paper *as well as* digital/electronic, and
- images *as well as* text (e.g. photos, CCTV).

3.4 Sensitive Information

This is any information relating to an individual's

- Racial or ethnic origin
- Sexual orientation
- **Religious**, political or trade union affiliation
- Genetic or biometric data

This is also known as **Special Category Information.**

Note that personal data of our congregations is considered as Special Category because Christian religious affiliation can be *inferred* because they are members of a Church. This means the data

should be handled more carefully and with greater security than 'normal' personal data (although unhelpfully, the law is not specific about *how much more* securely).

3.5 Data Controller

The legal entity that *decides how* the data is kept and used.

A 'legal entity' can be a company, a charity, a PCC, an incumbent or a Bishop. The Church of England, because of the way it is structured and instituted, has a great many 'legal entities'.

3.6 Data Processor

A different legal entity to the data controller, who is actually processing the data, *on instructions from the data controller.*

Note that:

- A data controller can also process data
- You can have joint data controllers (two legal entities which share the data)

Data processing for personal use not connected with a legal entity is not considered as personal data under GDPR.

3.7 Processing

Almost anything you can imagine doing with data counts as 'processing': recording, disseminating, adapting, obtaining, destroying, organising, erasing, transmitting, retrieving, combining, altering, holding – all these activities count as 'processing' of data.

3.8 Eights Rights of Individuals

Under GDPR, individuals have eight rights, summarised below:

1. Data subjects have a **right to be Informed** about the collection and use of their personal data (transparency).
2. Any data subject has a **right to access** the data which a data controller holds about them, to satisfy themselves it is being processed lawfully. This is known as a Subject Access Request: it may be submitted verbally or in writing; data controllers have one calendar month to provide a copy of the data; and there is no fee for doing this.
3. If you believe a data controller holds incorrect data about you, you have a **right to rectification**: the controller must correct inaccurate data.
4. A data subject may ask you to delete/destroy all data you hold about them: known as the **right to erasure** (often also called the right to be forgotten). Note this is not an absolute right as the data controller may have a legal or contractual requirement to process the data (for example an employer needs an employee's personal data in order to pay the employee, as per their contract of employment).
5. **Right to restrict/suppress processing:** In certain circumstances, a data subject may request their personal data can be stored but not used.
6. **Right to Data Portability:** Ease of movement between IT environments (unlikely to be relevant for parishes).

7. **Right to Object:** Absolute right to request suppression of direct marketing communications.
8. **Rights in relation to automated decision-making and profiling** (unlikely to be relevant for parishes).

4 Explanation of GDPR

4.1 General principles

These are seven principles at the heart of GDPR:

1. **Lawfulness, fairness and transparency**. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose Limitation**. Data must be collected for specified, explicit and legitimate purposes, with no further processing that is incompatible with those purposes.
3. **Data minimisation**. The data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy**. Data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
5. **Storage limitation**. Data shall be kept for no longer than is necessary to achieve the purpose for which it was collected.
6. **Integrity and confidentiality**. Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
7. **Accountability**. The data controller shall be responsible for, and be able to demonstrate compliance with the above principles.

This is a summary, the ICO Guide to GDPR contains the full version.

4.2 Lawful processing of data

There are **six 'lawful bases'** for processing personal data, listed below. You should be familiar with these:

1. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
2. Legal obligation: the processing is necessary for you to comply with other laws, such as church representation laws, faculty law, tax law, health and safety, safeguarding of vulnerable persons.
3. Legitimate interests: the processing is **necessary** for your legitimate interests or the legitimate interests of a third party, provided your interests do not outweigh those of the third party. For example, a PCC has a legitimate interest to process personal data of elected office-holders (the PCC members, churchwardens, treasurer, etc.) in order to circulate information about meetings and other church business so they can carry out their role responsibilities effectively.

Note with legitimate interest there is a **balance/exchange**: in this case people offer to hold office, in exchange the personal data is processed to help them to perform that office effectively (and the interests are reasonably balanced).

4. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
5. Vital interests: the processing is necessary to protect someone's life. This should not be necessary in church contexts, where consent is probably more appropriate.
6. 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.

It is unlikely that 5 and 6 will apply in the parish/benefice/deanery context.

Wherever you process personal data, you need to decide what is the *most appropriate* lawful basis for the processing. In church contexts it is important you understand **legitimate interest**: it is very flexible and can apply in a range of circumstances; the disadvantage is that you take on more responsibility for considering other peoples' rights and interests. **Consent** is a safe option because it places the control with data subjects, however it is often used where legitimate interest is more appropriate (at which point it becomes restrictive and counter-productive if people do not consent).

4.3 Transparency

Under GDPR, you have a responsibility for **transparency**: that is, being clear to data subjects what you are doing/will do with the data you hold about them. A good rule of thumb is that 'there should be **no surprises**' for people. In practice this means publishing a document known as a 'Privacy Notice' (which explains what you do with their data) and publish it in places where the data subjects will see it (such as send it by email, publish on your website or display in a public place). Privacy Notice statements may also form part of the Consent-giving process (see later).

Documentation to demonstrate transparency

Under GDPR, it is not sufficient to be compliant with this law, you should be able to *show* how you are compliant. This means having internal documentation which states the standards to which you are working. This will include much of the same information as the Privacy Notice, but may need more details: this requirement may be best served by a data protection policy; in some cases procedure documentation (or similar), where particular details of your local practice are formally held, stating such things as the sort of personal data you process, the lawful basis on which you hold it, typical retention times for documents containing personal data and who is responsible for data processing.

4.4 Consent

If you seek consent from data subjects to process their personal data, you must note:

- Consent must be **explicit**: you cannot assume data subjects consent by default
- Consent must be **freely given**
- The wording of the consent must be in **clear language**. It is good practice to offer data subjects options (for example to offer separate tick-boxes for receiving the prayer diary, for service information and for general parish communications)

- It must be as easy for data subjects to subsequently **withdraw consent** as it was to give consent in the first place.
- The data controller must retain **proof of consent being given - and withdrawn** - for at least as long as you continue to use the data.
- While not common practice, it is lawful to gain consent orally, but you must be very careful to document this immediately and accurately (your responsibility to be transparent with data subjects becomes important here)

4.5 Data Sharing

GDPR places additional requirements when a data controller shares data with another legal entity. It is the responsibility of the data controller to ensure that, whoever they pass personal data to, the third party will handle the data lawfully. The obvious way to do this is through some written statement(s) issued by the data controller which place obligations on the third party, and by the third party acknowledging their responsibility.

4.6 Interactions with Data Subjects

From the eight rights of individuals, as a data controller, you will note that data controllers have a responsibility to those whose data you hold. You must be prepared to respond to the following sorts of requests:

- To correct data about a person that is incorrect
- To delete all information you hold about a data subject (right to erasure)
- Right to object: removal of consent (previously given)
- Subject Access request: to provide a copy of all data you hold about a data subject

This includes ensuring that the person making these requests is the person they say they are, and that you only action the request for the data subject concerned.

Right to be informed: you should inform all data subjects affected by any change to the way you process their data (e.g. reissue your Privacy Notice).

4.7 Risk Management and Data Breaches

You should, as a matter of course, be regularly assessing the risks associated with your processing of personal data, seeking to identify those areas of activity which represent the highest risk (a combination of *likelihood* of something going wrong and the *impact* if it should go wrong).

Our working practices, technology use and the people involved will change over time – this can contribute to risks emerging. You should consider changing the way you process data in order to minimise the risk of data being accidentally disclosed, corrupted or lost: a 'continuous improvement' mindset is invaluable here.

A 'data breach' is an event where data is lost, damaged or inappropriately disclosed. You should keep a record of all data breaches, however small, and review them on a regular basis: in this way you have evidence of where the greater risks might lie, which can lead to action to avoid larger risks in the future.

The PCC should review its data protection measures regularly (suggest at least every three years and initially more frequently).

4.8 Registering with ICO?

The ICO maintains a register of Data Controllers, although many charities and not-for-profit organisations are exempt from registering. Those who do need to register will also pay a fee (paid annually), although again there are exceptions for small charities.

In general, churches fall into the exempt category, unless they operate CCTV for the purposes of crime prevention (in which case registration is mandatory). The ICO has online questionnaires to help you work out if you need to register and pay a fee:

- Do I need to register? https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/
- What fee should I pay? https://ico.org.uk/for-organisations/how-much-will-i-need-to-pay/

The rules change from time to time, so it is worth checking.

5 Reference Sources

There will be many different sources of information, but some of the better ones we've found are listed here:

- The **ICO's Guide to GDPR**: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- The **Diocese of Oxford** has a page of useful resources including training materials and standard forms we have used, which is located in the Support Services section: https://www.oxford.anglican.org/support-services/general-data-protection-regulation-parishes/
- The **Church of England** publishes a document "Keep or Bin – The Care of Church Records", which you can download from this page: https://www.churchofengland.org/more/libraries-and-archives/records-management-guides
- The **Diocese of Rochester** has produced a helpful GDPR Toolkit which can be downloaded here: https://www.rochester.anglican.org/resources/gdpr/

6 Next Steps

The Parish Resources website has a simple GDPR checklist, which is available from this page: https://www.parishresources.org.uk/gdpr/ This site also contains some standard template privacy notices and other guidance on writing privacy notices.

Further help with carrying out a GDPR data audit (usually the first step) is also available: https://www.parishresources.org.uk/gdpr/dataaudit/

A more detailed Action Plan is published by Rochester Diocese in Appendix 2 (page 25) of their Toolkit document: www.rochester.anglican.org/content/pages/documents/1519894032.pdf