# General Data Protection Regulations
# GDPR

**What is Data Protection?**
Simply stated, Data Protection is a set of regulations put in place to protect an individual's right to privacy, so that information given to an organisation is not misused, nor shared without the individual's consent, whether purposely or in error. Data protection helps to prevent financial and identity fraud, as well as protecting the individual from other forms of abuse connected with personal details being inappropriately shared. Adhering to data protection regulations is mandatory, and never optional.

**Data Protection Legislation**
The legislation governing how organisations must protect data given to them by an individual is known as the **General Data Protection Regulations (GDPR).** First instigated in 1998, and previously referred to as Data Protection ('DP'), the regulations were updated on 25th April 2018 and renamed to **GDPR**. The current regime places much tighter controls on organisations holding or processing customer or user data.

**The GDPR Regulator**
All matters relating to the safe-keeping and processing of an individual's data is regulated by the Information Commissioner's Office **(ICO**). Contact details are given at the end of this information sheet.

**The 'customer' or service user – The 'Subject'**
Throughout the regulations, the individual whose data is held by an organisation is referred to as the '**subject**'. In the case of a church this is taken to mean any person involved with the church whose personal information has been in some way recorded by the church, whether that person is an employee, elder, member, hirer or visitor.

**What is meant by Data Processing?**
Data processing can be taken to cover the collection and storage of any personal data pertaining to any subject the church comes into contact with. So, for example this would include membership details such as names and addresses, and contact details such as telephone numbers or email addresses. Other records, such as those of a Minister, or Lay Leader would by necessity contain far more personal data, such as bank details provided for payroll purposes, ethnicity (if collected) and **DBS** (Disclosure and Barring Service) information.

**GDPR – Some basics**
- GDPR regulations apply to all churches, and to Synod
- GDPR rules cover both the church's written and electronic records
- Commonly applying across the EU, the regulations will remain post 'Brexit'
- The regulations are designed to protect the individual's right to privacy
- They require all data collection to be fair and reasonable
- They establish legal grounds for processing a subject's data*****
- They place a requirement for transparency within an organisation, which means each church **must have** a 'Privacy Notice'*****

- It is good practice, although not mandatory, to have a Data Protection Policy*****
- Each church needs an appointed data 'Controller'*****
- There are 2 tiers of data – personal data and sensitive or 'special category' data*****
- Some data can be processed without specific consent from a subject*****
- Consent is always required before information can be shared*
- All subjects have a right to see what information is held about them*
- A subject can request that their information is deleted from church records*
- Some, but not all data breaches must be reported to the Information Commissioner's Office*

***See below for further information**

**What is a Data Controller and does our church need one?**
The Data Controller is the nominated person (or persons) appointed by the church to take on the role of ensuring compliance with GDPR. The term 'Data Officer' should not be used as this is a formal title which carries with it certain obligatory functions very unlikely to be necessary in respect of a church.

**What is classified as personal data?**
Personal data is any information about a living person which can be used to identify that individual. This includes names and addresses, and the GDPR rules cover all church users, whether employees, members, hirers, or visitors. Consent is not necessarily needed to process this data (see *Consent* below).

**What is sensitive or special category data?**
Both terms refer to the same list of data which is more tightly regulated as it is information which could place an individual ('subject') at personal risk if it were known to third parties. Processing sensitive data therefore requires specific consent, and includes any of the following:-

- Racial or ethnic origin
- Political beliefs or affiliations
- Religious or philosophical beliefs ******
- Trade Union membership
- Medical information
- Genetic or biometric data, for example fingerprints or bodily samples
- Details of sexual orientation
- Criminal record or information received through **DBS** requests

******The church will be able to rely on legal basis 5 below as a ground for securely holding *special category* data of religious belief without specific consent. The church can also usually rely on the fact that the individual's religious belief has been made manifestly public by the very act of church attendance for Christian worship (see *Consent* below)

**A Subject's rights under GDPR**
The 2018 regulations conferred additional rights to a subject as follows :-

- The right to access******or rectify their data if errors exist
- The right to have their data erased (unless the law requires such information to be retained)
- The right to be informed on how their data will be processed (see privacy statement below)
- The right to object to usage of data for certain purposes, such as marketing or (historic) research
- The right to restrict the extent of processing of their data

*** the 2018 regulations allow for a subject data request in any reasonable format without the previously required initial fee from the subject. For all such requests the church must reply within 30 days from receipt.*

**Consent**

Consent is one of several legitimate bases under GDPR for processing a subject's data. It is described as any freely given, specific or clear indication from a subject that they agree to their personal data being processed, or such data itself is/has been made manifestly public by the subject own statements or actions**.**

Best practice dictates that consent (where necessary) will usually be in writing and records kept of consents given by subjects. Contrary to common belief, consent is **not** required by a church for most simple general records such as the name, address and contact details for members, as there are 5 other legal bases which enable an organisation to process data without first having gained the consent of the subject. If the intention is to **share** information by way of a register or directory however, you will need consent to share.

**Children under 16**

Importantly, consent is always required from a parent for data collected for children under 16 years of age.

**The 5 Legal Bases for processing data without specific consent**

1. The subject's personal data is required to enter into a contract (such as employment)

2. Data collected is required to meet the church's legal obligations

3. Or is required to protect the vital interest of the subject or other person

4. Processing is necessary for the church to perform a public interest task or official function

5. Processing is necessary for the church to pursue its legitimate activities, which are specifically of a religious nature and are restricted solely to current or former members of this and personal data is not disclosed outside that organisation without specific consent. (This category also applies to organisations whose foundation is based on political, philosophical or trade union aims)

**Hiring and Data Protection**

If the church hires out its premises it will need to process all booking or hirer's data in line with GDPR regulations. In 2018 a new annual return of hiring was implemented by Synod which requires churches to provide a simple summary of hirers using the premises each year. Given that this does not contain any special category data, and that hiring is carried out by local churches through Synod delegated authority, consent is not required pass this information to Synod. You may wish however to incorporate a statement concerning passing hirer's data to Synod within your hiring booking paperwork, or include this in your privacy Notice.

**Privacy Notice – an absolute 'must-have' under GDPR**

Under GDPR there is increased responsibility for each organisation to demonstrate transparency in the way subject data is gathered, processed and otherwise used or shared. Such information is made public via a Privacy Notice, which is a mandatory requirement.

**What your Privacy Notice needs to Contain**

Most organisations make their Privacy Notice available through their website. The Notice needs to contain the following information:-

- Who will be the Data Controller
- What subject data is gathered
- Why this information is needed
- How subject data will processed
- What exact purposes the data will be used for
- If, and how subject data will be shared, and with whom
- The retention period for various types of data
- The subject's rights
- How a subject can contact you

**NB there is a sample Privacy Notice in the GDPR section of Church House website which can be downloaded and adapted to the individual circumstances of your particular church.**

**Does our church need a Data Protection Policy?**

Under the 2018 GDPR regulations it is not compulsory to have a specific data protection policy. However it is definitely good practice to have one, even if only a simple policy and this is particularly recommended for larger churches with significant hiring of church buildings (and therefore an increased amount of subject data on record. Include in your policy statements on:-

- Compliance with GDPR regulations
- Who will take the role of Data Controller
- Who else may gather or process data
- How data will be used and/or shared
- Who will have access to data
- How data will be protected
- Retention periods for various types of data
- Making data available to subjects
- Reporting responsibilities in the event of any data breach

**What to do if data breaches occur**

It is a common misunderstanding that all data breaches need to be reported to the ICO, for example where devices containing information have been lost, stolen or even hacked into. This in fact is not the case. A data breach only needs to be reported if it presents a risk to the rights and freedoms of the data subject. In this instance full and frank disclosure of the breach must be reported to the ICO within 72 hours of the breach occurring.

If it is considered that the data breach represents a serious risk to the individual's rights and freedom then it must also be reported to the subject whose data has been compromised.

**In Summary: What the church needs to do to satisfy GDPR**

Appoint a Data Controller
Have absolute clarity on what data is held by the church ***
Collect only data which is necessary
Keep records of all data processing carried out
Keep data safe and secure
Limit data access to only those who need it
Gain specific written consent for sharing date or gathering data for children under 16

Comply with subject access or other legitimate data requests
Review held data regularly, at least annually
Report any breaches placing subjects at risk
Carry out an impact assessment on any new activities requiring data processing (for example if starting hiring out premises)

***** A good starting point in terms of understanding what data is held and processed by the church, any weak data processes, and to provide a useful tool for reviewing data processing is an audit/mapping form. You can find this as Property Information sheet 16.1 on the Synod Website.**

**In Summary: What the church needs to have to satisfy GDPR**
A Privacy Notice (mandatory) – on website and a paper copy
Consider having a Data Protection Policy (obligatory)

**Suggested further advice, reading and information**
In addition to contacting the Synod Office you will find useful further information and documents on the following websites :-

**Church House website** GDPR section where you will find a GDPR **'Toolkit'** containing Sample Privacy notice, Data Protection Good Practice checklist, Hints and Tips, and a Consent template.
https://www.urc.org.uk/

**Information Commissioner's website.** Has a useful blog on GDPR issues as well as lots of general information.
www.ico.org.uk

**GDPR for Churches.** An information-packed website with information specifically targeted towards churches. They also run very reasonably priced training events.
http://gdprforchurches.org.uk/

**Stewardship**
You can download a Guide to Data Protection for churches
www.stewardship.org.uk

Contact the Synod Property team at:-

**Synod Office**
Taunton URC
18 Paul Street
Taunton
Somerset TA1 3PF

01823 275470
synodoffice@urcsouthwest.org.uk
www.urcsouthwest.org.uk