

General Data Protection Regulation 2018

The **Data Protection Act 1998 (DPA)** has governed the use of personal data for the last twenty years. However, the European Union's **General Data Protection Regulation (GDPR)** is now in force and the deadline for compliance is 25th May 2018. Additionally, a Data Protection Bill is making its way through Parliament with the intention of filling in certain gaps that have been left to the discretion of Member States, and of imposing the requirements of the **GDPR** into British Law once the United Kingdom has left the EU.

Overview

Data Protection, and the **GDPR** specifically, should be regarded as protecting the privacy of the individual.

Data means information relating to a *data subject* (i.e. a living person) who can be directly or indirectly identified from that data; whether the information is kept in paper records or on electronic devices such as a computer or smart phone.

Data Protection is a requirement placed on *Data Controllers* who process (see below) information about data subjects. Churches, in this context, are *Data Controllers*.

Process means to obtain, record, or hold data, or carry out any operation on the data.

Classification of Data

Data falls into two categories – **Sensitive Personal Data** and **Personal Data**:

- **Sensitive Personal Data** is any data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data (e.g. fingerprints), physical or mental health, sex life and/or sexual orientation.
- **Personal Data** is any other information relating to an identified or identifiable living person, such as their postal address.

The Principles

The principles of the **GDPR** are similar to that of the **DPA**, with added detail at certain points and a new *accountability* requirement. The principles are that personal data:

- 1) Shall be processed *lawfully, fairly, and in a transparent manner in relation to individuals (**lawfully*: the conditions for processing data have been met; *fairly*: the connection between the *use* for which the data was collected and the *use* to which it is put; *transparent*: the data subject is fully aware of how their data is being or will be used – this last should be in a church's **Privacy Policy**, see section below);
- 2) Shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- 3) Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 4) Shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- 5) Shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- 6) 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 organisation measures.

Furthermore:

- 7) The Data Controller shall be responsible for, and be able to demonstrate, compliance with these principles.

This last is the *accountability* principle, which requires Data Controllers to demonstrate *how* they comply with the principles – for example by documenting the decisions taken during the process of acquiring and storing data.

Conditions for processing Data

A Data Controller needs to have legitimate grounds for processing information:

- For **Personal Data** there are a number of conditions specified – at least one of which needs to be satisfied. Churches, when processing data, would most likely exercise one or more of the following:
 - They have the explicit consent of the data subject;
 - It is necessary for compliance with a legal obligation;
 - It is necessary to protect the vital interests of a data subject, or another person where the data subject is incapable of giving consent;
 - It is necessary for the purposes of the legitimate interests of the Data Controller or third party, except where overridden by interests or fundamental rights and freedoms of the data subject.
- For processing **Sensitive Personal Data**, there are likewise a number of conditions specified – again at least one of which needs to be satisfied. Churches, when processing data, would most likely exercise one or more of the following:
 - They have the explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
 - It is necessary for the carrying out of obligations under employment;
 - It is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent;
 - The data is manifestly made public by the data subject.

Furthermore, for the purposes of *employment*, when processing **Sensitive Personal Data**, the church must have a policy stating how this will be managed, taking into consideration the above conditions. The same requirement applies when processing information from the Disclosure and Barring Service (DBS), and therefore a policy also needs to be in place.

As stated, data may only be processed if at least one of the above conditions are satisfied. When relying on *consent* this must be *explicit* i.e. active agreement. Churches should keep systematic records of how and when an individual gave consent to process their personal data: be it verbally, electronically or by letter.

Rights of the Data Subject

Individuals have the right to withdraw their consent at a later time. When this happens, unless the data is required to be kept by statute, churches must permanently *erase* the individual's details, and not only, for instance, from a members' list. The data must be eradicated from all files, be it paper or electronic. The **GDPR** essentially gives individuals the right to be forgotten.

In addition, individuals have a number of other rights, the most likely ones applying to churches being ...

- the right to be informed (i.e. that their data *is* being held, and for *what* purpose);
- the right of access to one's personal information (see **Subject Access Request** below);
- the right to rectification (i.e. correction of inaccurate data);
- the right to restrict processing;
- the right to data portability (i.e. allows individuals to obtain and reuse their personal data for their own purposes across different services); and
- the right to object.

Church Responsibilities

Through appropriate management and strict application of criteria and controls, churches must:

- Observe fully the conditions regarding the fair collection and use of information;
- Meet legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil the church's operational needs or to comply with any legal requirements;
- Ensure the quality of information used (i.e. that it is *accurate*);
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Treat people justly and fairly when dealing with requests for information (see **Subject Access Request**); and
- Set out clear procedures for responding to requests for information (see **Subject Access Request**).

Most personal data that is held will relate to individuals who can be categorised. For instance church members, regular donors, staff, contractors (e.g. plumber), as well as those who attend activities such as Sunday School, youth and toddler groups.

In order to ensure compliance with the **GDPR**, it is necessary that churches identify the following in respect of each category:

- *What* data is held?
- *Why* is it held?
- *How* was it obtained?
- What will it be *used* for?
- How *long* will it be needed?
- *Where* is it held?

Under the last, data could be “held” in paper documents, on a church member’s home computer, or in the IT system of a third party’s physical or virtual server space (see **Outsourcing** below).

The **GDPR** principles also relate to data held on children. For churches, this would mainly occur in the context of Sunday School, youth or toddler group records. A child under the age of 16* cannot give consent for their data to be processed (*at the time of writing, the Data Protection Bill proposes the age of 13). Consent can only be given from a person holding ‘parental responsibility’. Thus there must be a verifiable paper-trail of authorisation from the responsible adult confirming consent for the church to hold data on said child.

Data that is collected to compile a church membership list cannot be used by a member or third party to advertise their business. Furthermore, each individual on said list must have given explicit consent for their details to be shared with the other members. Likewise, it might be advisable to include a confidentiality statement instructing members not to share the details with non-members. Here again the *accountability* principle is in play.

Data Breaches

A *data breach* is any personal data seen by anyone not entitled to do so. A breach can be one member disclosing to a non-member the contact details, obtained from a members list, of another member. A breach can also be considered to have occurred where data is misplaced or lost.

In the unfortunate event of a breach, the church must immediately determine what the resulting risk and severity is to the rights and freedoms of those involved. If there is deemed to be a risk, the church must inform the Information Commissioner’s Office (ICO) of the full details within 72 hours. (If the risk is considered unlikely, then the church does not have to report it; however they *do need* to be able to justify this decision and should therefore document it). Reporting the breach could result in an investigation by the ICO and occasion a fine. Hence the need to ensure that there are adequate controls in place. Additionally, it is necessary to have a policy for managing data breaches should they occur.

It is essential that all church members are made aware that any information they have access to as members must be kept confidential; not only because it should be, but because failure to do so could result in an ICO investigation.

Subject Access Request (SAR)

Individuals have a right of access to any information held on them, and can make what is known as a Subject Access Request (SAR). SAR’s must be handled appropriately and within 30 days of receipt of the request. Under the **GDPR**, requests are nominally free. However a reasonable fee may be charged if the request is disproportionate, groundless or recurring; and if further copies of the same information are requested.

The ICO has produced a ‘checklist’ to help in handling such a request, which can be done online (<https://ico.org.uk/for-organisations/subject-access-request-checklist/>). Whilst this checklist is geared towards businesses, the underlying principles are relevant to churches. In the event of a church receiving a request, church officers may approach the Corporation for guidance as to how they should proceed.

Privacy Policy

Churches, like all organisations, are required to have a **Privacy Policy** which must be easily accessible (e.g. on the church website), and include the following:

- The identity and contact details of the Data Controller i.e. the church.
- The purposes for which the church collects the data.

(...list continues on following page)

- The legal grounds for use of said data, which could be:
 - the data subject's explicit consent, which they can withdraw at any time;
 - legitimate interests, detailed accordingly;
 - a statutory requirement or contract.
- The length of time data will be retained, and the criteria used to determine it.
- The data subject's right to access the information, rectify inaccuracies, request erasure, and object to processing. In addition, their right to data portability, and to complain to the ICO.

For a **practical outworking** of these principles, **churches are welcome to use for a template the Corporation's Privacy Policy**; see: www.gbtc.org.uk/2PrivacyPolicy.html or contact the office.

Websites & Cookies

A church should indicate on their website whether or not it uses 'cookies'. This is a small text file that is automatically downloaded onto a computer or smartphone when someone accesses a website. Cookies allow the website to recognise that person's device and store data about their preferences or past actions. The use to which such information is used should be included in the church's **Privacy Policy** (see above).

Outsourcing

It is the responsibility of the Data Controller to ensure that adequate controls are in place to protect information that might become accessible to third parties. For instance, photocopier or computer companies that service the church's equipment. Written agreements must be in place stating explicitly how those organisations will protect the church's data, dealing specifically with how confidentiality is maintained, and how the data will be dealt with at the end of the agreement. At the very least the agreement must ensure that any third party handling the data is compliant with the **GDPR**.

Data Deletion

Principle 5 of the **GDPR** states that personal data, "Shall be kept in a form which permits identification of data subjects *for no longer than is necessary for the purposes for which the personal data is processed*".

Churches must decide for themselves when it is no longer necessary to keep an individual's information on record. There might be any number of reasons for retaining data. However, whatever the church's reason for retaining said data, they must be able to substantiate it. This must be recorded in a policy statement.

Further Reading

In conclusion, it is crucial to stress that the **GDPR** is more comprehensive than has been portrayed here. However, we felt it necessary to summarise the areas of particular relevance to churches.

The ICO has issued guidance for businesses including charities – under which churches fall – on how to prepare for the **GDPR**. These can be accessed at the following links:

- *Preparing for the GDPR: 12 steps to take now*: <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
- *An Overview of the GDPR*: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>

Further information and advice may be obtained from:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 0303 123 1113 or 01625 545745

Email: registration@ico.org.uk Website: <https://ico.org.uk/>

FS\GDPR\07\18

Disclaimer: *This Fact Sheet has been prepared carefully from the information available; however GBTC accepts no responsibility for its complete accuracy, and would encourage the consultation of professional advisors. All rights to the resource material are reserved. The material is not to be published in other media or mirrored on websites without written permission.*