General Data Protection Regulation 2018

On 25th May 2018, subject to Royal Assent, the General Data Protection Regulation (**GDPR**) will replace the Data Protection Act 1998 (**DPA**).

Data Protection: 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 (e.g. computer, smart phone etc.).

Data *Protection* is a requirement placed on *Data Controllers* who process 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, physical or mental health, sex life and/or sexual orientation.
- **Personal Data** is any other information relating to an identified or identifiable living person.

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;
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.

Grace Baptist Trust Corporation • 19 Croydon Road, Caterham, Surrey CR3 6PA
Tel: 01883 345488 • Fax: 01883 345129 • Email: info@gbtc.org.uk • Website: www.gbtc.org.uk

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 *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 legitimate interests.

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.

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.

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

- Observe fully 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; and
- Set out clear procedures for responding to requests for information.

Churches should review all personal data held, taking into account:

- *What* is held?
- *Why* is it held?
- *Who* has access to it?
- *How* is it secured?
- *Where* is it held?

Under the last, data could, for example, be held 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 attendance records. A child under the age of 16 cannot give consent for their data to be processed. It 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.

Furthermore, if a church produces a contact list for members, each individual on said list must have given their permission for their details to be shared with the other members. Likewise, the list should include a confidentiality statement instructing members not to share the details with non-members. Here again the *accountability* principle is in play.

Grace Baptist Trust Corporation • 19 Croydon Road, Caterham, Surrey CR3 6PA
Tel: 01883 345488 • Fax: 01883 345129 • Email: info@gbtc.org.uk • Website: www.gbtc.org.uk

Rights of the Data Subject
Individuals have the right to withdraw their consent at a later time. When this happens, churches must permanently erase the individual's details, and not only, for example, 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 the following rights:

- 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).
- the right to object; and
- the right in relation to automated decision making and profiling (see **Websites: Cookies & Privacy Statement** below).

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 one month 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 Information Commissioner's Office (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.

Websites: Cookies & Privacy Statement
If a church hosts a website, they must indicate 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. It allows the website to recognise that person's device and store information about their preferences or past actions.

A church website should also have a privacy statement, particularly if individuals can contact the church via a "contact page" option. The following example covers such a scenario, along with if cookies are *not* used:

"[e.g. …… Church] is committed to protecting the privacy of all users of its website, and to acting in accordance with the General Data Protection Regulation. This website does not use cookies. Neither does it collect personal information from site users, except where users choose to communicate through the Contact page. If users choose to do so, they are required only to provide their name and email address. Furthermore, [e.g. …… Church] will contact users only in response to their initial enquiry. The personal details of users will not be stored, or used to contact them at other times, unless that is their stated request."

In addition, if a church website has links to other churches or organisations, it would be sensible to indicate so. For example:

"This website lists various links to other websites. Users should be aware that these websites will have their own privacy policies, and [e.g. …… Church] does not accept any responsibility or liability for said polices."

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. Ideally, agreements should be in place stating explicitly how those organisations will protect the church's data, and at the very least that they are able to confirm that they comply with the **GDPR.**

Data Breaches
A *data breach* is any personal data seen by anyone not entitled to do so. A breach can also be considered to have occurred where data is misplaced or lost. In the unfortunate event of a breach, churches must inform the ICO of the full details within 72 hours. This could result in an investigation by the ICO which could result in a fine. Hence the need to ensure that there are adequate controls in place.

Grace Baptist Trust Corporation • 19 Croydon Road, Caterham, Surrey CR3 6PA
Tel: 01883 345488 • Fax: 01883 345129 • Email: info@gbtc.org.uk • Website: www.gbtc.org.uk

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.

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 the ICO:

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

Telephone: 0303 123 1113 or 01625 545745; Fax: 01625 524510;
Email: registration@ico.org.uk
Website: https://ico.org.uk/

FS\GDPR\11\17

Grace Baptist Trust Corporation • 19 Croydon Road, Caterham, Surrey CR3 6PA
Tel: 01883 345488 • Fax: 01883 345129 • Email: info@gbtc.org.uk • Website: www.gbtc.org.uk