DATA PROTECTION REQUIREMENTS FOR CHURCHES AND CHRISTIAN ORGANISATIONS

A new, Europe-wide, regulation comes into force next year. The implications for churches which hold and process personal data are far reaching. As Christians, we should want to set an example in our performance in this area. **Neil Walker** provides an overview and a call to action. He is an IT educator by profession, was involved in IT training and processes in a large bank, and serves on the boards of Partnership and Church Growth Trust. He is a leader of Caldmore Evangelical Church, Walsall.

25 May 2018 is a key date for the diaries of all church leaders. This is the date chosen for the EU's General Data Protection Regulation[1] (GDPR) to come into force. GDPR is a comprehensive regulation, enacted in 2016, which will strengthen and unify data protection for individuals across Europe. Brexit will have no immediate effect on the applicability of GDPR in the United Kingdom. It will be in force until the UK enacts Brexit legislation repealing or replacing it or incorporating it into UK law at the point the UK leaves the EU, and, given the political sensitivity of the matter, it can be assumed that Brexit legislation will in fact substantially transpose GDPR into UK law.

GDPR in effect adds to or supersedes existing legislation on data protection, which up to this point has been provided by the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations 2003.

DPA is based around 8 principles of good information handling and will be fully replaced by GDPR next year. *Stewardship* produced an excellent guide to data protection law for churches in May 2009, and while this does not currently appear in their list of briefing papers, you may be able to google it to refresh your memory of its content[2].

The world has changed since 1998. Then, only 10% of households had internet connections; Facebook and other social media did not exist; the smart phone was a pipe dream; and the cloud was, almost literally, pie in the sky. GDPR represents a significant enhancement in regulation, designed to better protect us in an environment where personal information can be stored, moved, used and misused with increasing speed and facility.

GDPR extends the scope of the law, the need for accountability, and the transparency required when collecting and processing data on individuals. It applies to any organisation in Europe and extends the definition of personal data to include any data which could be used to identify an individual to whom it relates (the IP address of someone's computer, mobile phone, or other connected device, for example).

GDPR broadly subsumes the eight principles of DPA, but adds an accountability principle. Under GDPR, a requirement to show how an organisation is complying with data protection principles is introduced—for example, documenting how your organisation has arrived at a decision to process data, demonstrating that policies and training are in place, and showing that auditing of data processing is carried out. Organisations must determine and document the legal basis for processing personal data. Privacy must be built into the design of processes for holding and handling data—not

[1] EU legislation can be applied in a member state in one of two ways: (1) by a Regulation, which applies directly in all member states from the date it comes into force; or (2) indirectly, where the EU enacts a Directive, the requirements of which then have to be transposed, usually by a deadline specified in the Directive, into the domestic law of each member state so as to achieve the objectives specified by the Directive by means to varying extents at the choice of the member state. GDPR is a Regulation which applies directly.

[2] 2 https://www.stewardship.org.uk/downloads/briefingpapers/Guide%20to%20data%20protection%20law%20for%20churches.pdf

collecting anything that is not required, not holding it for longer than required for operational purposes, and ensuring that storage and transmission is secure.

GDPR strengthens the need for organisations to be transparent in their data processing. Privacy notices need to specify the legal basis for processing the data, data retention periods, and contact details for complaints. This is in addition to the existing rules which cover identity of the organisation and intended use of data. Each individual (referred to in the jargon as the 'data subject') needs to be appraised of their right to:

- see what data are held about them (subject access); this must be granted free of charge
- have inaccuracies in any data held about them corrected
- have information erased (and forgotten by the organisation)
- prevent direct marketing to them by the organisation
- data portability (to be provided with an electronic copy of the data relevant to them)

The legal basis for processing data is premised on one or more of six conditions:

- consent of the data subject
- performance of any contract with the data subject relating to it
- compliance with a legal obligation
- that the vital interests of the data subject are protected
- that the data acquired and held is needed for the performance of a task carried out by the organisation in the public interest
- that the legitimate interests of data subjects are protected

Where consent is used as the legal basis for data processing, this is not simply a general, or implied consent. It must be by an unambiguous positive indication of wish in a statement or by clear affirmative action. This means specific and explicit consent for each processing activity, evidenced and auditable, dynamic (not open-ended), and easy to withdraw. In practice, this means that, in every instance where you collect and process data electronically, there is a need to record the opt-in action of each data subject, not simply with a tick box, but with a record that indicates when the subject agreed, and what they were agreeing to. They must also be made aware of the process by which they can withdraw their consent on an ongoing basis.

GDPR introduces special protection for children's personal data. Broadly, for a child under 13 there will be a need to have consent from a parent or guardian in order to process any data lawfully.

GDPR mandates identification and notification of breaches of the regulation to the individual, and sometimes the national regulator (the Information Commissioner's Office, ICO) within 72 hours. The maximum fine for organisations which breach the regulation will be €20 million. Quite apart from anything else, this should give charity trustees pause for thought.

GDPR may require the appointment of a Data Protection Officer in some circumstances, but in all circumstances there will be a need to ensure that someone in the organisation has been designated as responsible for data protection, and that they have the necessary knowledge, support and authority to ensure that the organisation is applying the regulation effectively.

All of this protection should be comforting to us as data subjects—in principle, we can look forward to freedom from unsolicited begging letters, from unwanted direct mailing, from web sites capturing our data for unknown purposes. But the regulation brings additional responsibilities on us as church leaders, and the nature of our response before a watching world is important.

In the past, some of us may have taken mental cover from the requirements of the DPA, by saying to ourselves that we are too small an organisation for the authorities to be worried about, or perhaps that we don't really process any data—we just have an address book, an attendees list, a prayer list. Indeed, there was an exemption from registration with ICO for churches which solely held and processed:

- Church membership list (where individuals have provided their details themselves)
- Gift Aid records
- Accounting records
- Payroll records

Under GDPR, this is not a sustainable response and, in any case, churches and other organisations may well have been breaching the current legislation. ICO has already signalled that it intends to enforce the law, having already fined 13 charities, some relatively small, for improper use of data so far this year. Elizabeth Denham, the Commissioner, has been quoted as saying: 'These fines draw a line under what has been a complex investigation into the way some charities have handled personal information. While we will continue to educate and support charities, we have been clear that what we now want, and expect, is for charities to follow the law.' The regulation demands that, even for small churches, our electronic collection and use of personal data is thought about, managed, and tested in advance.

Let's take the case of the organisation of a Children's Holiday Club. Consents will be required for children to attend, lists generated for group leaders, and contact details stored and made available as necessary. Sensitive data, including medical conditions, allergies, parental access restrictions, etc., will be required to ensure that helpers can make properly informed decisions during club activities. In the past, these are organisational details that church Leaders would just cope with—perhaps drop in a box file and pull out again next summer?

From May 2018, there will be a mandated need to plan in advance the basis on which this data is to be collected, stored, processed and retained. Will leaders be sent group details on their personal smart phones? If so, how will access be controlled? What will be the retention policy for that data? How will the parent/guardian verify what is being held? How will they make contact to demand removal of data? How can they be provided with electronic copy for data portability? This is the way of the world in which we are called to be witnesses and we must respond in a way which is generous, open hearted, and at the very least abides by the new law.

Other common scenarios come to mind—addresses and birth dates of those who have attended ladies meetings, 'down the shed' clubs and other neighbourhood outreach are often held to enable us to send birthday cards, invitations, newsletters, calendars. This is data storage and processing and is subject to GDPR. Simply storing membership and prayer lists in electronic form brings these items under regulation. Just a couple of minutes spent mentally reviewing the activities of your church will probably generate a number of instances for your particular situation.

In relation to direct marketing, which both the existing law and GDPR also regulates, it is tempting to rely on the idea that this only applies where someone is selling something, or soliciting money. Church leaders need to be aware that in law this term applies more broadly, and covers the promotion of aims and ideals as well as any advertising or marketing communication (whether trying to sell a product or promoting an organisation) that is directed to particular individuals. Think about the impact for texts and emails containing invitations to events, promotion of camps, church weekends, requests for support of needy causes, etc., or indeed simply church newsletters. Specific consent needs to have been sought and obtained from each recipient, even from existing contacts and supporters, before such texts and emails are issued by an organisation.

One short article in Perspectives is not going to provide a solution, but we have 9 months now in which to prepare, and a number of organisations are providing advice and guidance. ICO (ico.org.uk) has a web site section specifically for small charities, with readable guides and downloadable tools to support your preparation. ICOs top five tips for you are:

Tell people what you are doing with their data.
People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice), so it is important you are open and honest with people about how their data will be used.

Make sure your staff/volunteers are adequately trained
New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff and volunteers.

Use strong passwords
There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves. Passwords should not be disclosed to others, even within the organisation.

Encrypt all portable devices
Make sure all portable devices—such as memory sticks and laptops— used to store personal information are encrypted.

Only keep people's information for as long as necessary
Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Microsoft has committed to supporting its customers by ensuring that Windows 10, Office 365, and its Cloud services are completely GDPR compliant by May 2018. *Dropbox* is committed to the security and the protection of users' data in line with legal requirements and best practices at all times. It is also committed to enhancing its systems as further guidance emerges, so that it meets or exceeds legal requirements going forward.

The tools we use to handle data in the modern age will be ready. We must be too.
We would encourage you to make best use of the preparation time using four simple steps:

1. Discover
Identify what personal data you have and where it resides
2. Manage
Govern how personal data is used and accessed, in line with the legal requirements
3. Protect
Establish security controls to prevent, detect and respond to vulnerabilities and data breaches
4. Report
Keep required documentation, manage data requests and breach notifications

The Apostle Paul, in his letter to Titus, urges him to remind God's people to be subject to rulers and authorities, to be considerate, to be ever ready to do what is good. Let's glorify God as we make preparations for May 2018.