Edward Connor Solicitors

General Data Protection Regulation

The changes in data protection law and what this means for your church.

Contents

The information in this booklet reflects Edward Connor Solicitors' understanding as at 12th January 2018. It is produced for the purpose of knowledge sharing and does not constitute legal advice.

Growing digital technology means the world is a different place to what it was when the Data Protection Act 1998 ("DPA") came into force. Record keeping has shifted from paper to electronics, the methods for manipulating personal information have become more powerful and identity theft has become a significant problem. People want greater choice and control over how their *personal data* is used.

The EU General Data Protection Regulation ("GDPR") extends the data rights of individuals, making transparency as a right, and increases the obligations on organisations to have clear policies and procedures in place to protect *personal data* and to adopt appropriate technical and organisational measures.

Although the GDPR has been described as a game changer for data protection and privacy law, requiring substantial forward planning for every organisation, if organisations are already complying with the Data Protection Act, they may need to simply make tweaks to their current procedures. However, if organisations have not been used to giving much thought to data protection, they need to be aware that the GDPR increases the consequences for non-compliance (including by providing for Information Commissioner's Office penalties of up to £17 million or 4% of global turnover).

Of course, as churches, we will be motivated not simply by wanting to avoid financial penalties but by a desire to obey scripture by obeying the authorities. If your church is transparent in this area, it will also build trust and confidence with its membership and the community at large. The purpose of this paper is to set out the key themes of the GDPR and what you can do now to prepare for it.

The GDPR will come into force on 25 May 2018. As a regulation, it will come into force automatically across the European Union, without member states needing to pass additional laws. Brexit will not make any difference to the UK as the new Data Protection Bill will repeal the Data Protection Act 1998 and incorporate the GDPR into UK law.

"This is a terrible time to be bad at Data Protection. The stakes - in terms of reputation and enforcement - have never been higher"- Tim Turner, *Fundraising and Data Protection*

How does the GDPR apply to us as churches?

Every organisation in the EU will need to comply with GDPR and that includes churches. You will need to review the impact of the Regulation on your operations, as soon as possible, and determine what changes have to be made to ensure compliance. There are no significant charity exemptions in the GDPR.

A local church comes within the definition of *data controller* in the legislation, as a 'body, which...determines the purposes and means of the *processing* of *personal data'*.

Processing means 'obtaining, recording, or holding information or data or carrying out any operation on the information or data...' *Personal data* is 'information relating to a living individual who can be identified from that data (*data subject*)'.

In storing information relating to members and other individuals, a local church will be '*processing*' (i.e. obtaining, storing, using, disclosing, destroying) '*personal data*' such as the names, addresses, photographs, email addresses and telephone numbers of church members/contacts and employees. A church may also be *processing* '*sensitive personal data/special categories of data'* if it keeps information about a person's religious beliefs or sexual orientation.

GDPR in detail

The GDPR outlines 6 principles that should be applied to any collection or *processing* of *personal data*. Fundamentally, if you can demonstrate that you're meeting these requirements, it is likely that you're in a good position to meet your GDPR compliance requirements. Note that the GDPR places greater emphasis on the documentation that *data controllers* must keep in order to demonstrate compliance with all of the principles.

1. *PERSONAL DATA* MUST BE PROCESSED LAWFULLY, FAIRLY AND TRANSPARENTLY

Registration with the ICO

To process data ***lawfully***, under the Data Protection Act 1998 (DPA), all *data controllers* are currently required to register with the Information Commissioner's Office (ICO) in order to be included within the ICO's public register of *data controllers* (available on the ICO website), unless an exemption applies. It is a simple process carried out by completing an online form at:

www.ico.org.uk/for-organisations/register

Currently the registration has to be maintained on an annual basis and there is an annual fee. This fee structure is likely to change when the new GDPR comes into force and the requirement to register is likely to go but may be replaced with an alternative regime under the ICO.

Conditions for *processing*

In order for *processing* to be **lawful** under the GDPR, you need to identify a lawful basis before you can process *personal data*, referred to in the GDPR as '*conditions for processing'*. The legal basis identified has an effect on individuals' rights (see Appendix 2 - *The right to be informed*), e.g. relying on consent to process data means the individual will generally have stronger rights, e.g. to have data deleted.

You don't need consent for every use of *personal data*, but if you don't have consent, you need to know what other legal justification you have that allows you to use the data.

It is important that you determine your lawful basis for *processing* data and document this.

The conditions for *processing* that may be relevant to the church's *processing* of *personal data* are:

i) Consent of the *data subject* (see Appendix 1)

ii) The *processing* is necessary for the performance of a contract (e.g. for staff details – the contract of employment)

iii) The *processing* is necessary for the purposes of legitimate interests pursued by the church (including commercial benefit) unless this is outweighed by harm to the individual's rights and interests.

We would expect most of a church's *processing* of *personal data* relating to church contacts to fall under this condition of *processing*, as the data is necessary for a church to carry out its functions on behalf of members and other contacts.

Fair and transparent *processing*

Even if you have a legal basis other than consent for sharing data, you still need to tell people what you are doing with their data in order for your *processing* to be fair and transparent (unless there is an exemption from this in data protection legislation).

When you collect *personal data* you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you need to tell people including, your lawful basis for *processing* the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The information must be provided in concise, easy to understand and clear language.

2. *PERSONAL DATA* CAN ONLY BE COLLECTED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

(See below Appendix 2)

3. *PERSONAL DATA* MUST BE ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY FOR *PROCESSING*

This requires data minimisation – collecting only what is necessary for the particular job and retaining a minimum amount of data.

4. *PERSONAL DATA* MUST BE ACCURATE AND KEPT UP TO DATE

The church must have a method for ensuring details (such as addresses) are kept up-to-date. You should request evidence (e.g. a marriage certificate for change of name) before changing details on your systems to prevent fraud.

5. *PERSONAL DATA* MUST BE KEPT IN A FORM SUCH THAT THE *DATA SUBJECT* CAN BE IDENTIFIED ONLY AS LONG AS IS NECESSARY FOR *PROCESSING*

It is important to consider what retention policy is suitable for the *personal data* you process. Consider how electronically stored *personal data* will be deleted as well as hardcopies.

6. *PERSONAL DATA* MUST BE PROCESSED IN A MANNER THAT ENSURES ITS SECURITY

Internal Safeguards

The GDPR specifies protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Any measures taken to secure data should be taken on the basis of a thorough risk assessment identifying any threats or vulnerabilities in the organisation. It is important to have an Information Security Policy and to carry out regular testing, assessing and reviewing of the effectiveness of measures taken.

Examples of technical measures are: anti-virus software on computers, back-up, firewalls, password protection, encryption, steps taken to stop cybercrime, hacking and other security compromises, robust IT systems etc.

Examples of organisational measures are: policies and procedures; training for staff and volunteers; home working policy; telephone and email policy; laptop policy and procedure; social media policy; all coupled with staff discipline if there is a breach.

Outsourcing

It is also important to ensure service level agreements/ outsourcing arrangements are reviewed in line with the requirements of the GDPR. As a *data controller,* you will be equally liable for any breaches that occur as a result of a supplier's failure to preserve data protection. This means having robust information security practices in place for supplier contracts where the responsibilities and liabilities between the controller and processor are stipulated. It is important to audit processors (e.g. shredding company/ outsourced payroll) to ensure they can guarantee *processing* will be in line with the GDPR.

Appendix 1 - Action Plan for Churches

The following pages offer you some steps you could follow to implement GDPR in your church.

First, there is a summary of the major differences between the old legislation and the new GDPR– please note the information in this table is not comprehensive, so please do read through the rest of the appendices.

Then, there are 8 steps for you to work through to assess how to implement this legislation.

To help you implement these changes, we have produced a pack of model documents which are available for you to buy.

This pack includes:

- Data protection policy and guidance
- Information security policy
- Draft privacy notice
- Retention of records policy
- Complaints process
- Audit checklist for compliance
- Breach procedure

Prices: £100 + VAT for FIEC churches / £150 + VAT for non-FIEC churches.

We hope this pack helps you to serve your congregations and communities in a God-honouring way as we navigate our way through these changes.

Appendix 1 cont. Main changes between DPA (1998)

Area of change	Data Protection Act	GDPR
Scope	Only covered people in UK	Any organisation that holds or processes personal data of EU citizens
Security Breaches	Limited reporting requirement	Reporting extended to cover any breach where there is likely to be a risk to an individuals rights and freedoms
Opt-in (for consent)	A negative was required i.e. untick a box	A positive opt-in is required
Data Requests	Can charge and no automatic right to correction or deletion of data	Generally no charge (unless repetitive or excessive) and the right to have information corrected or deleted
Need for a Data Protection Officer	Not required	Required only where large scale processing of data subjects is a core activity (see Step 6, p.16 below)
Impact Assessment	Not required	Privacy Impact Assessments required for new projects where there is risk to individual
Fines	Up to £500,000	Up to 20million euros or 4% of global turnover, whichever is higher

Appendix 1 cont. Steps to take to prepare for GDPR

Step 1 **Awareness** (ICO 1)	Complete initial employee/ trustee briefing 1. Ensure key decision makers in the church (trustees and staff) are aware about data protection and the changes coming with GDPR. 2. Discuss with insurers protection for some of the risks consequential upon a data breach. 3. Add data protection compliance to the church's risk register.
Step 2 **Information Held** (ICO 2)	Carry out a data audit 1.What personal data do you hold and where did it come from? 2.Why is it collected? 3.How is data stored (electronic/paper?) and where does it reside physically? (e.g. if you use Cloud solution, where is the Cloud supplier based?) 4.Who has access to data, have they been specifically authorised and what skills, training and clearance do they have? 5.How sensitive is the data? (i.e. does it include health/religious beliefs?) 6.How long is data held for and what is the reason for that time period? 7.What 3rd parties have access to data, how is it transferred? What agreements and contracts are there? *See Data Protection Audit Form and Data Protection Compliance Questionnaire in Edward Connor Solicitors Data Protection Pack*

Appendix 1 cont.

Step 3 **Legal Basis for Processing** (ICO 6,7,8)	Identify and document the lawful basis for processing personal data 1.Document the lawful basis for each processing of personal data 2.If relying on consent, review how you seek, record and manage consents 3.Ensure consent is freely given, specific, informed and unambiguous 4.Do you need systems in place to verify individuals' ages and to obtain parental/guardian consent? *See Data Protection Compliance Questionnaire in Edward Connor Solicitors Data Protection Pack*
Step 4 **Communicating Privacy Information** (ICO 3)	Policy review 1.Review your current privacy notices and put a plan in place to make any changes required by GDPR 2.Do you explain to church members/employees the different ways data will be used, what you will and will not do with the data, how you will ensure security, information about peoples' access to their data and how to make a complaint? *See Privacy Notice in Edward Connor Solicitors Data Protection Pack*

ICO numbers correspond to the Information Commissioner's Office 12 step guidance on how to prepare for the GDPR

Appendix 1 cont.

Step 5

Individual's Rights

(ICO 4)

Implement New Policies and Procedures

1. Consider all of the individual rights set out in the GDPR and how you would ensure these can be met.

2. How would you delete personal data?

3. How would you deal with a subject access request?

Consider testing the system with dummy requests

See Data Protection Policy and Retention of Records Policy in Edward Connor Solicitors Data Protection Pack

Step 6

Person Responsible for Data Protection

(ICO 11)

1.Identify single point of responsibility and accountability for GDPR in the church

NB. It is best not to use the term 'data protection officer' as this carries with it statutory responsibilities and there is unlikely to be a legal requirement for the church to have a data protection officer (DPO)

GDPR says the appointment of a DPO by a controller or processor is mandatory where :

- The processing is carried out by a ***public authority***;
- The core activities of the controller or processor consist of processing operations which require ***regular and systematic processing*** of data subjects on a ***large scale***; or
- The core activities of the controller or processor consist of processing on a ***large scale of sensitive data*** (Article 9) or data relating to ***criminal convictions / offences*** (Article 10).

Appendix 1 cont.

Step 7 **Implement Breach Reporting** (ICO 9)	1. Put in place procedures to detect, report and investigate a personal data breach 2. Test policy with dummy breaches *See Data Breach Procedure and Complaints Process in Edward Connor Solicitors Data Protection Pack*
Step 8 **Review of Data Security**	1. Do adequate firewalls and virus protections exist? 2. Is there an enforced password policy? 3. What steps have been taken to stop cybercrime, hacking and other security compromises? 4. Is there a procedure in place for data breach management? 5. Do all employees understand the procedure? 6. What is the process for investigating cause of a breach? 7. What happens to data not being used? 8. Review storage and data elimination/ destruction policy. 9. Consider having a telephone/email/social media policy for church staff. *See Information Security Policy in Edward Connor Solicitors Data Protection Pack*

ICO numbers correspond to the Information Commissioner's Office 12 step guidance on how to prepare for the GDPR

Appendix 2 - Consent under GDPR

The GDPR sets a high standard for consent. You need to ensure you have *clear and unambiguous consent*.

- Consent should be in a separate form/document and the consent document should be laid out in simple terms.

- Pre-ticked opt-in boxes are specifically banned.

- Consent must be given to each separate *processing* activity (e.g. if you wish to carry out 6 different actions, the *data subject* must consent to all of them)

- Consent must not be "bundled", meaning that the consent given for each processing activity must be separate.

- You must keep clear records to demonstrate consent (who consented, when, what they were told at the time, how they have consented and whether they have withdrawn consent)

- The *data subject* should be informed of their right to withdraw consent and it should be easy for them to do this.

Appendix 2 cont

- Children aged 13-16 may give their own consent, provided they have capacity and fully understand the nature of the processing. This will depend on the child and processing in question, but it may be simpler to rely on parental consent as a default for under 16s.

- You must name your organisation and any third parties who will be relying on the consent (e.g. outsourced payroll or outsourced shredder company that disposes of confidential waste etc)

- There should be no imbalance of power in the relationship between the individual and the organisation (so it is better to rely on an alternative *lawful condition for processing* for employment matters)

- The GDPR makes clear that organisations can rely on existing consents given and there will be no need to seek fresh consent **but** the consent requests must already meet the GDPR standard and be properly documented.

- If your existing consents do not meet the GDPR high standards or are poorly documented you will need to (a) seek fresh GDPR compliant consent, or (b) identify a different *lawful condition for processing* or (c) stop the *processing*. Option (b) is only permissible as a one-off in this period of transition to GDPR, controllers will not be able to swap between lawful conditions under GDPR.

Appendix 3 - Individual Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act. The GDPR provides the following rights for individuals:

1. The Right to be Informed

The right to be informed encompasses your obligation to provide 'fair *processing* information', usually through a privacy notice.

The GDPR sets out the information you should supply and when individuals should be informed. The information you provide is determined by whether or not you obtained the *personal data* directly from individuals. The information must be concise, transparent, intelligible and easily accessible. It should be written in clear and precise language and be free of charge.

2. The Right of Access (Subject Access Requests)

Individuals will have a right to obtain confirmation that their data is being processed and access to their data under the GDPR. These are similar to existing subject access requests under the DPA but there is less time to comply (without delay and within 30 days). In addition no charge can be made for complying with the request.

Appendix 3 cont.

3. The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete *personal data* rectified and if you have disclosed the *personal data* to any third parties, you must also inform them of the rectification where possible. You must respond to a request for rectification within one month.

4. The Right to Erasure/ The Right to be Forgotten

This is to enable individuals to request the deletion or *personal data* where there is no compelling reason for its continued *processing* but is only available in limited circumstances and is not an absolute right. There are extra requirements for the erasure of children's *personal data*.

5. The Right to Restrict *Processing*

When individuals exercise this right, you are allowed to store *personal data* but not to further process it.

6. The Right to Data Portability

This is unlikely to ever apply to a local church. It is designed to enable easy transfer of data for consumers.

Appendix 3 cont.

7. The Right to Object

Individuals have a right to object to *processing* based on legitimate interests. You must stop *processing* in these circumstances unless you can demonstrate compelling legitimate grounds for *processing* which override the interests, rights and freedoms of the individual or the *processing* is in relation to legal claims.

It is important to inform individuals of their right to object "at the point of first communication" and in your ***privacy notice***.

8. Rights in Relation to Automated Decision Making and Profiling.

This is unlikely to ever apply to a local church. It is designed to be a safeguard against potentially damaging decisions being taken without human intervention.

Appendix 4 - Data Breaches

A *personal data* breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to *personal data*.

The GDPR mandates informing both the ICO and the *data subject* themselves in relevant circumstances. This is only where there is a high risk to the rights and freedoms of the individual **or** a large-scale breach affecting many people. However, it is better to be over cautious than to be accused of negligence, and the ICO will not penalise you for reporting a breach that they do not deem to be serious. Also, in the interest of transparency (see appendix 3, p.20) it is never a bad idea to inform the individual(s) of any breaches that may occur.

You need to have processes in place to make these notifications in event of a breach. Data breach reports must be made within 72 hours of the *data controller* becoming aware of the breach. The notification must be in a specific format and should include a description of the measures taken to address the breach and mitigate its possible side effects. It is also advisable to keep a register of breaches, but content of the breaches should be kept deliberately vague so as not to become a breach in and of itself.

Edward Connor Solicitors

39 The Point
Market Harborough
LE16 7QU

info@edwardconnor.com
01858 411569
www.edwardconnor.com

Updated March 2018