Anthony Collins solicitors

DATA PROTECTION AND THE GDPR: WHAT DO YOU NEED TO KNOW?

We appreciate that there is a lot of news about changes to the regulations on data protection (the General Data Protection Regulation or 'GDPR') that are required from May 2018 and we receive an increasing number of queries on data protection and the GDPR. In response, we have prepared this brief note on the key issues for church charities grappling with data protection law.

Much of the news you will have seen is focused on the need for changes to be made by any organisation holding personal data; churches included. We also appreciate that churches are focused on missional objectives and do not go out of their way to misuse data. This fact sheet is not intended to provide a comprehensive guide to the regulations but to help churches understand the key elements of change and the aspects that are most likely to require action. It is intended to be read alongside the Information Commissioner's own guidance, and we provide links to some key guidance below.

In writing this fact sheet, we have been very grateful for the input from Stewardship and especially their experience of the needs of churches across the country. Stephen Mathews, who is responsible for the Stewardship 'Consultancy Helpline', comments:

> "*Different churches have very different use of data and consequent needs in respect of the new GDPR requirements. We hope that smaller churches and those only holding data on individuals for very limited reasons (e.g. Gift Aid and membership contact lists) will not feel the need to take expensive professional advice. Some, even with limited data, may still want that for peace of mind, which is both legitimate and right as we see the ever-increasing professionalism that is expected of churches both by regulators and by the general public; including church members.*
>
> *We recommend that larger churches or those holding sensitive data work through the issues carefully with one or more of their trustees taking responsibility for the project and expect to take focused advice from specialists where there are areas on which they are still unclear*."

The GDPR has focused the minds of many in the sector – and it is a critical issue – but organisations should start by complying with existing law. The following non-exhaustive list will get you started.

Are you sure:

- What personal data (information *relating to* living persons, including opinions about them and expressions of intention) you hold, how you collect it, and for what purposes?

  Some typical categories of data for churches are listed in the appendix to this guidance note, together with some common risk areas for volunteer-run churches.

  Focus on potential areas of 'risky' processing, e.g. where sensitive personal data such as data about the health of a congregation member or other pastoral issues are involved.

- How you communicate with people ('data subjects'), how you will process any personal information you hold about them (**fairness**): do your 'privacy notices' cover all the information required by the GDPR?

  For smaller churches, this may involve little more than making clear when you will be putting church members on a mailing list and how often you will be sending them your newsletter or Sunday morning

email bulletin. If you hold more personal data because, for example, you run a nursery or other community provision from your church, you will need to consider this issue further (see below).

- You have **legal grounds** for processing all the data you use.

  Seeking consent is usually the simplest way to ensure that you may lawfully use data about a person but it is not the only legal ground. In fact, it is one of the weakest grounds – it can be withdrawn at any time, and it must be easy for people ('data subjects') to withdraw consent. Other grounds include the necessity for the performance of a contract with the individual concerned and necessity for achieving the 'legitimate interests' of the organisation.

- Where consent is your justification for using data:
  - the consent obtained meets the requirements of the GDPR, such as being freely given, specific, informed and unambiguous, whether or not given before the GDPR takes effect;
  - the consent is recent enough;
  - you could prove that you received consent if challenged.

  It may be useful to refer to the ICO's draft guidance on 'GDPR consent'.

- You only send electronic marketing (email and SMS), which includes a wide range of promotions and not just goods and services, to people who have given GDPR compliant 'opt-in' consent.

  You should be aware that simply sending people information about church services could be treated as 'marketing' for this purpose.

  The ICO's guidance on 'Direct marketing' is helpful but be aware that while this guidance suggests that alternatives to 'opt-in' mechanisms may be acceptable in some limited cases, the more recent draft guidance on GDPR consent excludes this possibility completely.

- All your contracts with '*data processors*' are GDPR compliant.

  If you pay a local IT professional – even if s/he is the child of a church member – to keep the computer in the church office running, you probably have a '*data processor*' and you should have a contract in place to make sure that s/he does not misuse the data held by the church.

  You will need to consider whether each organisation or person you deal with is a 'data processor' – only using data as you tell them to and on your behalf – or a '*data controller*' – using the information for purposes that they decide. The distinction is not always easy to make but the ICO's guidance on 'Data controllers and data processors' can help you make it.

  Contracts with data processors must contain the clauses specified in the GDPR that are described in the ICO's draft guidance on 'Contracts and liabilities between controllers and processors'. You should adopt a risk-based approach: start by reviewing contracts involving sensitive personal data.

- All your policies and procedures for the church are up to date.

  Do you keep records of how personal data is being processed and why? Is there a clear framework of accountability? The GDPR requires you to show you comply with the law, and for all but the smallest churches, this is likely to involve having some basic documents recording how you will collect data about congregation members and others – and what you will do with that data.

- You have a clear policy on reporting '*data breaches*'.

  Under the current law, there is, strictly speaking, no legal requirement to report breaches to the ICO, but the GDPR will require self-reporting within 72 hours in cases which pose a risk to individuals. In cases of high risk, the individual would also need to be notified. Charity trustees should also consider whether the Charity Commission needs to be notified.

  See the Commission's guidance including the examples of incidents to report. The threshold for reporting may not be the same for the Charity Commission and the ICO.

- You have a clear procedure for responding if a member of the congregation or someone else asks for a copy of all the data you hold about them (a 'subject access request') and the leadership team are all familiar with it.

  Under the existing law, you must provide individuals who request it with access to the data you hold about them within 40 days. This will be reduced to one month – do you know who should deal with any such requests and how they will do so?

- You have a Data Protection Officer ('DPO') if you need one.

  The EU's 'Guidelines on Data Protection Officers' may help you decide whether or not you require a DPO (see page 5 onwards). Most smaller churches will not be obliged to have a DPO because their core activities do not involve monitoring individuals or processing sensitive data on a large scale.

- You do not keep data longer than is necessary – and you tell people how long you will retain data about them.

  Old data is unlikely to be accurate; it increases the volume of data that needs to be kept secure (increasing the risk of breach), and people may ask for copies of it.

- You provide data protection training to ensure that employees, volunteers and others involved in handling personal data for your organisation are familiar with their obligations.
- You are registered with the ICO, and your entry is accurate.

  Some churches are unsure whether they are registered as data controllers with the ICO. Until the GDPR comes in force (when this requirement will end), all data controllers must be registered with the ICO. The exemptions to this – including the 'charity' exemption – are narrow and will rarely apply.
- Reviewing the steps above should give you a clear sense of where you need to focus attention to achieve compliance with data protection law and the GDPR. If you need help to complete that journey before 25 May 2018, the answers to the questions above will help you seek informed advice from an appropriate professional.

For general guidance on steps you might take and pointers to the guidance mentioned above, you may find the ICO helpline for smaller organisations useful at https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/ or 0303 123 1113

Anthony Collins solicitors

For further information

Please contact Edwina Turner or our Data Protection and Information team if you require any further information.

APPENDIX

A. COMMON CATEGORIES OF PERSONAL DATA HELD BY SMALLER CHURCHES

1. Church contact list
2. Church mid-week membership/attendance lists
3. Training events (including Alpha and internal courses)
4. Gift Aid records
5. Payroll and volunteer management details
6. Pastoral notes (including sensitive data on health and 'issues')
7. Organisational contact lists (e.g. mums and parents etc.)
8. Family/parent records associated with youth and children – including food allergies/medical conditions and details of other special needs.

B. COMMON RISK AREAS FOR VOLUNTEER-RUN CHURCHES

(These issues are as relevant now as to the GDPR)

- If volunteers take pastoral notes or other data away from the church building, how do you ensure the data is secure? How do you guard against the loss of data?
- Where you use mobile phones, computers or other electronic devices, do you have secure passwords – and appropriate procedures to ensure that passwords are not shared?
- Does everyone use the same password for church business or do you have different access rights so that you only access the data you need to see?
- Do you have lockable filing cabinets and other physical security mechanisms to protect confidential data stored in shared working areas?
- Do you ensure that congregation records and other confidential data is professionally shredded or otherwise securely destroyed?
- Do you have agreed procedures to ensure that where confidential information and/or sensitive personal data needs to be shared between members of a pastoral team, that data is stored systematically and appropriate steps are taken to record the legal justification for using the data?