Data Protection Guidance for Safeguarding Coordinators

The law governing the handling of personal information will change on 25 May 2018 when the General Data Protection Regulation (GDPR) comes into force across the EU. As the UK Government is legislating to implement the essential terms of the GDPR in UK law (having produced a draft Data Protection Bill) Brexit will have no impact on this latest update to data protection law.

These guidelines are intended to provide safeguarding coordinators with a snapshot of key elements of the updated legislation for consideration when handling "personal data" and safeguarding documentation and advice.

KEY DEFINITIONS

Key definitions under the GDPR are:-

- Personal data
- Processing
- Data controller
- Data processor
- Special category data (sensitive personal data).

Personal data

Personal data is information, held either electronically or physically, relating to living individuals who can be identified, directly or indirectly, by the information.

Examples include names, addresses, online identifiers and digital photographs and videos, where images are clear enough to enable individuals to be identified. Other examples of the sort of personal data commonly held by congregations are: staff/payroll records; membership lists; baptismal records; information relating to pastoral care; information regarding those attending holiday clubs or other activities; lists of children/young people attending Sunday schools, youth groups and creches; records of those for whom the congregation holds contact details for various reasons, including volunteers working with children and young people and others, those attending churches, making Gift Aid donations etc. These are examples only and there may be other types of personal data held.

The definition also includes Churches with websites with a facility to collect data, such as a "contact us" form should be aware that the information supplied by any enquirer is personal data and will have to be held by the church in accordance with data protection law. Further, if a church uses cookies on its website to monitor browsing, it will be collecting personal data of that individual.

Processing

Processing is anything at all you do with personal data – it includes collecting, editing, storing, holding, disclosing, sharing, viewing, recording, listening, erasing, deleting etc. Individuals responsible for processing personal information in churches may include the minister and other office bearers, treasurers, administrators, group leaders, safeguarding coordinators and others.

Data controller

The "controller" means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. In congregations there may be more than one controller. For some personal data it will be the Kirk Session, for others it will be the Congregational Board (the members of which are also the charity trustees), and for others it will be the minister. It will depend on the personal data in question. The "controller" also includes all staff and volunteers who work for the controller entity, and when staff or volunteers process personal information on behalf of the church, as part of their role, they will be doing so as a data controller. It is important that such staff/volunteers are adequately trained in respect of what is required of them under data protection law, as any data breach by them could lead to the congregation being liable. For example, staff/volunteers should not use any personal information being processed on behalf of the congregation for their personal use. Personal information must be used only for the *specific* purposes for which it has been *lawfully* obtained (see below for more on this).

Data processor

The "processor" means a natural or legal person, public authority, agency or any other body which processes personal data *on behalf of* the controller. This could be a third party who has been asked by the congregation to carry out processing on its behalf and the definition of "processor" would also apply to any staff/volunteers working for the processor in this role. An example would be an IT supplier engaged by a church to provide a new system on which personal information will be stored. The IT supplier's staff also comes within the definition of "processor".

Under the GDPR, data processors will be jointly and severally liable with data controllers for data breaches, to the extent for which they are responsible. This is a change from the current law. Any congregation using, or considering the use of, a data processor should have an appropriate written contract with that processor and should seek guidance from the Law Department as to the terms of that contract.

Special category data

It is important that congregations are aware of and understand this special category of personal information. It replaces, and is very similar to, the "sensitive personal data" category contained in the current Data Protection Act. It is personal data which are stated to be more sensitive than other types, and so require additional protection and safeguards. It is defined in Article 9 of the GDPR as:

"*personal data revealing a person's racial or ethnic origin, political opinions,* ***religious or philosophical beliefs****, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health or sex life and sexual orientation*".

Most of the personal data processed by congregations about individuals will come under the definition of special category data, either specifically or by implication, as the mere holding of any information about a person by a congregation is likely to be indicative of that person's religious beliefs.

How should special category data be handled?

Processing of such special category data is prohibited under the GDPR unless one of the listed exemptions applies. Two of these exemptions will be especially relevant and useful for congregations (although others may also apply):

- the individual has given **explicit consent** to the processing of those personal data for one or more specified purposes; OR
- processing is carried out in the course of its **legitimate activities** with **appropriate safeguards** by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing **relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes** and that the personal data are **not disclosed outside that body** without the consent of the data subjects.

This latter exception should cover much of the data processing carried out by the Church as a whole.

For some personal data processed by congregations (or by individual ministers/office bearers), such as in connection with pastoral care and/or **safeguarding matters** (note that special category data includes personal data relating to criminal offences and convictions), it will be obvious that it falls within the definition of special category personal data. So long as:

- the processing is carried out in the course of the congregation's legitimate activities;
- there are appropriate safeguards to keep information safe and secure;
- information relates either to members, former members, or individuals in regular contact with the church; and
- information is not disclosed to anyone else without the person's consent

then there is no need to get explicit consent, and the processing will come within the "legitimate activities" exemption.

Other lawful bases for processing Safeguarding information

In some cases Safeguarding Panels might need to process information that does not relate to members or those in contact with the Church. For example, it may be necessary for a safeguarding coordinator to pass on child or adult protection concerns about someone not connected with the Church to the police or a welfare agency. For obvious reasons, it will not be realistic or practicable to obtain the consent of the data subject (the person who is the focus of the concern) to this processing.

This is an area that, as at April 2018, is being developed by the UK Government and it is not yet certain how the new UK Data Protection Act will deal with sharing safeguarding information. Until that is clarified, safeguarding panels should continue to share information with appropriate third parties, without seeking consent, where this is necessary to protect a child or vulnerable adult from neglect or physical, mental or emotional harm or to protect their physical, mental or emotional wellbeing; and/or sharing the information is necessary for reasons of substantial public interest.

Data retention

Data protection legislation specifies that personal data must be accurate and up to date and not retained for any longer than necessary. Determining when information is no longer necessary can pose a challenge to safeguarding coordinators and the following bullet points should assist. Where there are any doubts, or questions, guidance can be obtained by contacting the Safeguarding Service via email at: Safeguarding@churchofscotland.org.uk

- Safeguarding Panels should not retain PVG applications (even a copy). The most that congregations should keep is the PVG application number.

- Job application forms should be retained for as long as the appointment lasts plus 6 years and then destroyed securely.

- Covenants of responsibilities should be retained for 100 years for those convicted of a sexual offence.

- Records of concerns relating to potential/actual sexual offending should be retained for 100 years.

- Records relating to child protection concerns should be retained for 50 years.
- Records relating to adult protection concerns should be retained for 50 years.
- Advice from the Safeguarding Service should be retained for 3 years (unless it falls under one of the previous categories, in which case it should be dealt with as set out above).
- A Data Retention Schedule for congregations is available from the Church of Scotland website, here: http://www.churchofscotland.org.uk/resources/law_circulars#data_protection
- All safeguarding information should be securely retained. If it is held electronically, it should be stored on encrypted devices in password protected files. If it is held physically it should be in a locked cabinet or other secure storage.

Data breaches

A data breach can occur when information is intentionally collected without a proper basis or when information is unintentionally lost, altered or sent to the wrong recipient.

The updated data protection legislation includes penalties for intentional and unintentional mishandling of information and, additionally, penalties where an individual has inappropriate access to information.

If there has been a data breach **the Presbytery Clerk must be notified** as soon as possible, as reportable breaches must be intimated to the Information Commissioner's Office **within 72 hours** of the data controller becoming aware of the breach. If you receive information that you should not have, you should contact the sender and take steps to return it. You should not retain any information that has inadvertently been shared with you.

Guidance on data breach procedure is available from the Church of Scotland website here: http://www.churchofscotland.org.uk/resources/law_circulars#data_protection

Summary

What do safeguarding coordinators need to know about GDPR?

For the purposes of the legislation, Safeguarding Panels will (usually) be processors of special category data, processing information on the basis of either (a) having a legitimate interest to do so or (b) for reasons of substantial public interest, with the Presbytery acting as the overarching data controller.

- The collection and use of personal information for safeguarding purposes is allowed under GDPR and **you do not need consent in order to do this**. The law as it will come into force in terms of the new Data Protection Act in the UK is not yet finalised but as at April 2018 it does not appear that the person who is the subject of the information will need to be told about the processing, provided that the information is used only for safeguarding purposes.

- Security of information is a crucial element of data protection and all safeguarding information must be securely stored and processed. Lockable filing cabinets and password protected files are essential. Also:

  - ✓ passwords should be kept secure, should be strong, changed regularly and not shared
  - ✓ if you are sharing a computer or tablet with anyone else, you must ensure that all personal data relating to other people is password-protected
  - ✓ emails containing personal information should not be sent to anyone's work email address, as this might be accessed by third parties
  - ✓ confidential paper waste should be disposed of securely by shredding
  - ✓ to prevent virus attacks, care should be taken when opening emails and attachments or visiting new websites

- Safeguarding information can be shared with those advising a safeguarding panel but cannot be shared with any parties not directly involved with a safeguarding matter.

- Although the general principle under GDPR is that all data must be accurate and up to date there are legitimate interests in retaining some safeguarding information, for example in order to respond to any concerns about historic abuse. You should however review the information you are currently holding and consider whether it is time to let go of anything that is no longer needed, in accordance with the data retention schedule available from the Church of Scotland website.