Data Protection Guidance for Safeguarding Coordinators

The law governing the handling of personal information changed on 25 May 2018 when the General Data Protection Regulation (GDPR) came into force across the EU and the Data Protection Act 2018 came into force in the UK.

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/criminal convictions information

The 2018 Act makes specific – and slightly different - provision for information about criminal convictions (i.e personal data relating to convictions and offences, or related security measures) and "special category data" relating to the safeguarding of children and individuals at risk.

Substantial public interest

Looking first at the processing of "special category personal data" (which in this context will involve information about someone's health or sex life), the Act permits this on the basis that doing so is in the substantial public interest, but sets out some conditions. Data controllers undertaking such processing must have both a **lawful basis** under Article 9 of the GDPR and **either legal authority or official authority for the processing** under Article 10. There must also be an appropriate **policy** document in place before doing any processing and a **record** of the processing must be maintained. What does this mean in practice?

(i) The first thing is to decide your condition for **lawful processing** of such data in terms of Article 9. The appropriate ground for processing safeguarding data will be that doing so is "for reasons of substantial public interest". This is qualified to the extent that suitable measures must be in place to protect the rights of the data subject.

(i) You must then be clear that you have **legal authority** before you undertake the processing. The Data Protection Act 2018 provides such a ground in section 10 (3), which says that personal data can be processed for reasons of substantial public interest if the processing meets one of the conditions in Part 2 of Schedule 1 of the Act.

One of these conditions relates to safeguarding of children and individuals at risk. It provides for a lawful ground for the processing of special category personal data – without consent if the circumstances justify it – where it is in the substantial public interest, and necessary for the purpose of: (a) protecting an individual from neglect or physical, mental or emotional harm; or

(b) protecting the physical, mental or emotional well-being of an individual, where that individual is either aged under 18 or is aged 18 or over and is “at risk” (having needs for care and support, experiencing or at risk of neglect or any type of harm, and unable to protect themselves).

The Act still expects the possibility of obtaining consent from an individual to be considered (and in these circumstances it would have to be explicit). However, if in the circumstances the consent cannot be given, or the data controller cannot reasonably be expected to obtain it – notably because obtaining it would prejudice the safeguarding purpose (i.e. the protection of the individual) – then the ground applies. It is a question of whether the use of the personal data is proportionate to the lawful aim.

There is also another provision in the Act which allows processing in the "substantial public interest", where processing is necessary for the purposes of complying with (or assisting compliance with) *"a regulatory requirement*" which involves "*taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct*" – and where consent cannot reasonably be obtained.

The Government has made it clear that the Act intends to make it easier for organisations to carry out "*legitimate safeguarding activities that are in the substantial public interest*" in full confidence, and to ensure the law is "*fit for purpose*" and will "*cover the safeguarding activities expected of organisations responsible*” for individuals at risk.

It seems fair to conclude that the Act’s provisions are intended to go beyond one-off information sharing and reactive or urgent steps and will instead provide a framework within which churches and other organisations can operate reasonable and proportionate safeguarding practices and policies. This includes policies on monitoring, reporting, retention and record-keeping, so as to ensure that all the information that might be relevant to questions of early intervention or prevention is captured. In turn, this will allow churches to be safer by design, in part through how they record and share personal data, and not simply be reactive to incidents that meet a reporting threshold under the criminal law.

(ii) To qualify for the protection afforded by the Act, Part 4 of Schedule 1 to the Act requires that a data controller must have an appropriate **policy** document in place, which explains the controller’s procedures for complying with the data protection principles and explains the controller’s policies regarding the retention of personal data processed in reliance on the relevant condition. A

suitable style data protection policy has been drafted by the Law Department and is available on the Church's website.

(iii) Finally, to qualify for this protection a data controller must also maintain a **record of the processing**, in terms of Article 30 of the GDPR. This must say what condition is relied on, how the processing meets the lawfulness requirement and whether the information is retained in accordance with the policy document. A suitable style record of processing, which will cover all of the different types of processing carried out by congregations, including safeguarding information, is in the course of preparation by the Law Department and will be published very shortly on the Church's website.

Criminal convictions data

The Data Protection Act deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it, although there is no requirement to have a written policy in place or to maintain a record of the processing in order to benefit from the protections which relate to criminal offence data.

GDPR Article 10 says: "*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*." The Data Protection Act 2018 provides such a ground in section 10 (4), which says that personal data can be processed for reasons of substantial public interest if the processing meets one of the conditions in Parts 1, 2 or 3 of Schedule 1 of the Act.

This means that in addition to the safeguarding of children and individuals at risk (which is a condition in Part 2, as referred to above) congregations can also rely on the additional condition in paragraph 31 of Part 3 of Schedule 1. This reflects the general "not for profit" processing exemption for special category data which is contained in Article 9 of the GDPR and says that the condition is met if the processing is carried out "*in the course of its legitimate activities with appropriate safeguards, by a…not-for-profit body with a…religious…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 the data is not disclosed outside that body without the consent of the data subject"*.

Accordingly, if criminal convictions data is to be shared beyond the Church, without the consent of the individual concerned, it would not be possible to rely on this condition but it would be possible to rely on the provision regarding safeguarding of children and individuals at risk to enable this to be done.

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 both controllers and processors of special category data and criminal convictions data, processing information on the basis of either (a) this being in the course of its legitimate activities as a not-for-profit body with a religious aim or (b) for reasons of substantial public interest, with the Presbytery acting as the joint data controller.

- The collection and use of personal information (including criminal convictions) for safeguarding purposes is allowed under GDPR and **you do not need consent in order to do this**. You must, however, have suitable data protection and records of processing activities in place.

- 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 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 referred to on page 5.