GDPR GENERAL GUIDANCE FOR CONGREGATIONS

Contents

INTRODUCTION

The Council of the European Union has said that "*the processing of personal data should be designed to serve mankind*". Whilst there is some scope for disagreement as to whether this laudable aim has been achieved, the law governing the handling of personal information will change with the coming into force of the General Data Protection Regulation (GDPR) across the EU on 25 May 2018. Brexit will have no impact on that, because the UK Government has said that it will legislate to implement the essential terms of the GDPR in UK law and has already produced a draft Data Protection Bill to do this. There is as yet no indication of when it is likely to be passed, and come into force, but the new law will apply as from 25 May regardless of whether its source is the GDPR or UK legislation.

This Guidance Note aims to provide an overview of the main provisions of the GDPR. Further guidance, a set of FAQs and styles relating to specific areas where policies or procedures are required under the new law, are also available for use by congregations and Presbyteries.

THE KEY DEFINITIONS

Before looking at the principles underpinning the new regulatory regime it is worth reviewing the key definitions in the GDPR. These are:-

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

Personal data

The GDPR defines personal data as:

"*any information relating to an identified or identifiable natural person (called a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or societal identity of that natural person*."

As under the current law, the definition relates to living individuals and to data held electronically or on paper records/in manual filing systems. The explicit inclusion of location data, online identifiers and genetic data is new, and may result in additional compliance obligations.

The definition includes 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.

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 basically 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 come 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 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.

How should data be handled for the purpose of the inspection of records?

When records are transported for an inspection by Presbytery they should be moved as securely as possible using, for example, a lockable document case. Consideration should be given to whether there is scope for records to be emailed to Presbytery or provided on an encrypted USB stick.

Other types of data processed by congregations will fall into this special category by implication. So, for example, in relation to membership lists, the personal information processed will come under this special category as by implication it relates to religious belief, but as the processing of such information for the purposes of maintaining an accurate membership roll is part of the church's "legitimate activities" it is permitted under the relevant exception above, with no explicit consent being required. However, before such data could be used for other purposes, such as sharing with any other party, the explicit consent of the individual would be required.

LEGITIMATE ACTIVITIES

It is important to remember that the "legitimate activities" exception to the prohibition on processing special category data is conditional on the data not being disclosed outwith the Church without obtaining the consent of the individual. So, for example, although the names of individuals on church rotas can be shared within the congregation, they should not appear on church websites unless the individuals concerned have given their specific written consent for that. Publishing any personal information (including photographs) on the internet is effectively making it available worldwide and should not be done without consent.

THE DATA PROTECTION PRINCIPLES

Just like the current Act, the GDPR sets out a list of data protection principles. These are very similar to the current principles. They are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Principle 1 - Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner. People have an increased right to be informed about how their personal data is being used, and you must be clear and transparent about how and why you are using personal information.

For data processing to be lawful, you must be able to rely on at least one of the following "legal bases" for processing, those highlighted being the legal bases most likely to be relevant for churches:-

(*Note: This is the starting point for processing personal data – for special category data additional rules apply, as referred to above*):

a) **the person has given consent to the processing of their personal data for one or more <u>specific</u> purposes** (*see below for further information on the use of consent as the legal basis for processing);*

b) **processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (**such as keeping and maintaining staff/payroll records**)**;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or another natural person (this really just relates to life and death situations);

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**

For most Presbytery or congregational processing, this last category will often be the legal basis on which you will want to rely. You should not rely on consent, other than as a last resort, not only because it is a laborious and thankless process to obtain consent for every single item of information which you are processing, but because consent can be withdrawn. If it is withdrawn, you are likely to have difficulty in continuing to process the information in question. Also, it is misleading to ask for consent if you are in fact going to process the information regardless of whether or not consent is given.

It is also essential that you can <u>demonstrate</u> that this basis of processing applies, and there is a 3-stage test for doing so. You have to:-

- identify a legitimate interest
- establish that your processing is in fact "necessary"
- conduct a balancing test

The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits. The processing must be necessary: if you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply. You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. On the other hand, the fact that individuals have a reasonable expectation that you will process their personal data makes it likely that processing on this basis will be lawful.

You must record which basis of processing you are choosing for your different processing activities, and your reasons for doing so. This is best done by means of a Legitimate Interests Assessment (LIA), which documents your decision-making process and will help you to demonstrate compliance with the law. A style LIA is being produced by the Law Department and will be on the website very shortly.

You must include details of your legitimate interests in your privacy notice.

<u>Consent as a legal basis for processing personal information</u>

Some detailed information is necessary on the use of consent as a legal basis for processing personal data. It is crucial for congregations to be clear as to which of the

above listed legal bases for processing apply to their processing of personal information, so as to ensure compliance with the new law. In particular, under the GDPR the legal basis of "consent" gives individuals much more control over their data and its uses than they have under the current Act.

One of the themes of the GDPR is to move away from "consent" as the condition of first choice for processing personal data, although there will still be many situations where it is required. The GDPR sets a high standard for consent. But often congregations won't need consent. For example, congregations should often be able to rely on either "legitimate interests" (or "legitimate activities" where the personal information is special category data) as the legal basis for processing personal information. However, there will be situations where consent is the appropriate legal basis for processing personal information, e.g. when a congregation wants to include personal information in a congregational directory for circulation; or to include personal information on a website (*see under "Special category data" above*). In such situations it will be vital to ensure that correct procedures are followed.

Consent of an individual means any freely given, specific (this may often lead to more than one consent being required from the same individual for different uses of their data), informed and unambiguous indication of the person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Pre-ticked boxes do not demonstrate "clear affirmative action", and nor does any other method of default consent.

Consent must also be easily withdrawn (so individuals must be informed at the time of giving consent as to how they can withdraw it, and the procedure for withdrawing consent must be as simple as that for granting it in the first place); it must be clearly distinguishable; and the congregation must be able to prove compliance. It is important to be particularly careful about compliance if a congregation is relying on consent *alone* as the legal basis for processing (it is an option to get the consent of the individual *in addition to* another legal basis for processing personal information). If the data subject is a child, consent should be obtained in addition to relying on legitimate interests.

A sample consent form is available here http://www.churchofscotland.org.uk/__data/assets/word_doc/0008/49229/GDPR_Consent_form.docx. You should keep signed forms to evidence that consent has been properly given. Consent can be given orally rather than in writing and in such circumstances you should record in writing that consent has been given in this way.

The ICO has provided useful checklists (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) for asking for consent, recording consent and managing consent.

Principle 2 - Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. It is therefore important (a) to be clear about the reasons why you are collecting personal information from individuals and (b) ensure that the information is only used for that purpose.

Principle 3 – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. You should not be holding information for which you cannot demonstrate a need.

Principle 4 – Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Particular care should be taken when you are collating and/or transmitting information for central record purposes, since a mistake in – for example – the address of a manse which may have been sold and replaced could easily result in a data security breach if confidential information such as a payslip is subsequently sent to the wrong address.

Principle 5 – Storage limitation

Personal data must be:

- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed. It is therefore important to be clear as to what the purposes are from the outset. It also means that data which has been anonymised can be retained; and
- subject to appropriate security measures, data may be kept longer for public interest archiving, scientific and historical research and statistical purposes.

You should review what information you are holding and consider whether it might be time to let go of anything that is no longer required. You should carry out a data audit with the aim of establishing exactly what personal information is held, along with a number of other essential details such as:

- The purpose for which information is held
- The type of information

- How it is collected
- How it is accessed, where and by whom
- How relevant it is
- What steps are taken to ensure it is kept up to date
- How long it is retained
- What security measures are in place
- Any third parties to whom it is disclosed
- Whether it is transferred outside the UK

Once you know what information you are holding, it will be much easier to take steps to comply with the new legislation. It will also aid a "clear out" of redundant personal data and result in a more streamlined information management system.

You should not hold information that you reasonably believe to be out of date, including names on a Communion Roll or Supplementary Roll, unless you have a clear purpose in doing so which passes the 3-step "legitimate interests test" referred to on page 8. Regular reviews of Supplementary Rolls should be carried out to determine why information is being held and whether it may be appropriate to remove it. It may, for example, be appropriate to retain personal details so that if someone who has moved out of the parish should ask for their lines there will be a record of their membership.

A separate guidance note on data retention is available here http://www.churchofscotland.org.uk/__data/assets/pdf_file/0018/49230/Data_Retention_Policy_Congregations.pdf. A data audit template is available here http://www.churchofscotland.org.uk/__data/assets/word_doc/0019/49231/Data_Audit.docx.

Principle 6 – Integrity and confidentiality

Personal data must be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This is the same as under the current law. So, data should be kept on secure computer systems and/or in secure manual filing systems. In particular:

- passwords should be kept secure, should be strong, changed regularly and not shared. If computers are in shared areas the user should lock or log off when away from his or her desk.
- 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.
- use the "bcc" rather than "cc" or "to" fields when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group

- confidential paper waste should be disposed of securely by shredding.
- emails containing personal information should not be sent to anyone's work email address (other than "@churchofscotland.org" addresses), as this might be accessed by third parties
- to prevent virus attacks care should be taken when opening emails and attachments or visiting new websites.
- hard copy personal information should be securely stored and not visible when not being used.
- visitors should be signed in and out of premises or accompanied in areas normally restricted to "staff".
- personal data being taken off the premises should be encrypted if it would cause damage or distress if lost or stolen.
- back-ups of data should be kept.
- when congregational information is processed using home computers it should be password protected and encrypted for transport using an encryption system such as BitLocker.

When records are transported for the purpose of inspection by Presbytery, they should be handled as securely as possible, for example by using a lockable document case.

Cradle rolls should only include the name of the child and the date of baptism. Explicit consent must be obtained from the child's parent(s) if the cradle rolls are on public display.

The Church must respect the individual's right to confidentiality. Care must be taken to ensure that third parties cannot access information without the permission of the individual concerned and that data about individuals is not disclosed – to third parties or others – without their consent, unless the Church is allowed or obliged to disclose the data by law.

Care should be taken in dealing with any request for personal information over the telephone. The amount of information given out over the telephone should be limited and in any event identity checks should be carried out if giving information out over the telephone, whether by way of an incoming or an outgoing call, to ensure that the person requesting the information is either the individual concerned, or someone properly authorised to act on their behalf.

Most breaches of the Data Protection Act relate to a breach of this principle, and arise from data being sent by email, post or fax to the wrong person. The best thing you can do to protect yourself against this is to be careful when handling personal information, particularly when sending it by email.

Principle 7 – Accountability

This is a new concept introduced by the GDPR. It means that the data controller must be able to **demonstrate compliance** with the first 6 principles. So you have to be able to

evidence that you are compliant. To be able to do this, congregations should, for example, document the decisions they take about their various types of data processing, provide and record staff and volunteer training, review policies and audit processing methods and activities. There is a lot of material on the Church website to help with this:

- a data audit template (found here http://www.churchofscotland.org.uk/__data/assets/word_doc/0019/49231/Data_Audit.docx)
- privacy notice templates (found here http://www.churchofscotland.org.uk/__data/assets/word_doc/0003/49233/Privacy_Notice_Congregation.docx)
- a security breach management procedure (found here http://www.churchofscotland.org.uk/__data/assets/word_doc/0004/49234/Data_security_breach_management_policy_Presbyteries.docx)
- a subject access request policy
- a data retention policy (found here http://www.churchofscotland.org.uk/__data/assets/pdf_file/0018/49230/Data_Retention_Policy_Congregations.pdf)
- a legitimate interests assessment form

SOME RIGHTS OF INDIVIDUALS (DATA SUBJECTS) UNDER THE GDPR

The right to be informed

Individuals have the right to be informed, by being given "fair processing information" about how organisations will use their personal data, so congregations must be transparent about how and why they are using personal information. This should normally be done through a data processing notice or privacy notice, although it can also be done orally, for example when taking personal information over the telephone or in person. It is a good idea to document it in writing if this information is given orally.

These notices should include the identity of the congregation, how it is intended the information will be used, the legal basis for processing the information, how long the information will be retained for, and that individuals have a right to complain to the ICO if they are not happy with how their personal information is being processed. They must be transparent, concise, intelligible and easily accessible. They should be made available using the most appropriate mechanism, which could be in in printed media, through signage (e.g a poster) or electronically (on a website or in emails).

When should this be done? Congregations need to understand the level of knowledge people have about how their data is collected and what is done with it. If an individual would not reasonably expect what an organisation will do with their information, privacy information must be actively provided rather than simply making it available for them to look for themselves, for example on a website. If it is reasonable for someone to expect that their information will be used for an intended purpose, it is less likely that there will be a need to actively explain it to them. In most cases, it is anticipated that all use of personal data by congregations will be within the reasonable expectation of those providing it, so that it will be legitimate to make privacy information available if they look for it, rather than actively giving it to them.

A sample privacy notice for use by congregations can be found here http://www.churchofscotland.org.uk/__data/assets/word_doc/0003/49233/Privacy_Notice_Congregation.docx.

Note: privacy notices and consent forms are not the same thing. Privacy notices tell individuals how their data will be processed. They are required whatever the legal basis for processing is, whether consent or another basis (e.g. legitimate interests). Consent forms are for use only where consent is being used as the legal basis for processing information. However, it can sometimes be possible to include a consent statement within a privacy notice instead of having two separate documents.

The right of access

As under the current law, individuals have the right to obtain a copy of their personal data from the data controller, by way of a "subject access request". They are now entitled to receive this free of charge (although a reasonable fee can be charged if the data subject requests further copies), and within 30 days (shorter than the current 40-day period allowed). You can refuse manifestly unreasonable requests. If a subject access request is made in connection with a safeguarding matter that should be referred to the Safeguarding Service in the Church Office without delay.

The right to rectification/correction

Individuals have the right to have incorrect data rectified if it is inaccurate or incomplete.

The right to erasure - "right to be forgotten"

This is not an absolute right. Individuals have a right to have personal data erased by the data controller without undue delay in any of the following circumstances:

- the personal data are no longer necessary in relation to the purpose for which they were originally collected/processed.
- the individual withdraws consent.
- the individual objects to the processing and there is no

overriding legitimate interest for continuing the processing.

- the personal data are unlawfully processed (i.e. otherwise in breach of the GDPR).
- the personal data must be erased in order to comply with a legal obligation.
- the personal data are processed in relation to the offer of information society subjects to a child.

This means that congregations must erase data when an individual revokes their consent; when the purpose for which the data was collected is complete; or when compelled by law. However, it does not mean that an individual is necessarily entitled to have data erased on request. If the purposes for which it was collected still exist then the data should not be deleted, *unless* the legal basis for processing the data was consent – in that event the data will have to be deleted if consent is withdrawn.

The right to restriction of processing

In certain circumstances, such as if an individual considers that their personal data are inaccurate, or if they object to the processing, they may have the right to restrict processing of their personal data. In such an event the data can continue to be stored but not used/processed in any other way.

The right to object

Individuals have the right to object to processing if they are not satisfied that you have a legal basis for doing so. Any objection must be on "grounds relating to his or her particular situation". You must stop processing the personal data unless: it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

Individuals must be informed of their right to object "at the point of first communication" and in privacy notices. This must be explicitly brought to the attention of the individual and presented clearly and separately from any other information.

IF A DATA SECURITY BREACH HAS OCCURRED

A data security breach occurs where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It's not just losing data; it includes disclosure to the wrong person. Under the current law it is not mandatory to report a data breach to the ICO, although it is good practice to do so.

What breaches must be reported to the ICO?

Under the GDPR, when a personal data breach has occurred, the data controller must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then it must be notified to the ICO; if it is unlikely then it need not be reported. If it is decided not to report the breach, this decision should be documented so that it can if necessary be justified at a later date.

Reportable breaches **must be notified to the ICO within 72 hours** of the data controller becoming aware of the breach. A data processor is required to notify the controller without undue delay after becoming aware of a personal data breach.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals the controller must communicate the personal breach to the data subject without undue delay. This is not required if the data is encrypted.

In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals. This will include any loss of control over personal data, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality or any other significant economic or social disadvantage to the individual. A breach can have a range of adverse effects on individuals, including emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience. Other breaches can significantly affect individuals whose personal data has been compromised. This will need to be assessed on a case by case basis, looking at all relevant factors.

Presbyteries and congregations should have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not there is a need to notify the ICO and the affected individual(s). Guidance will also of course be available from the Law Department.

A record must be kept of any personal data breaches, regardless of whether there is a requirement to notify the ICO.

What information should be provided when reporting a breach?

When reporting a breach, the GDPR says that the following information must be provided (and this can be done in phases, if it is not all available within 72 hours):

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Immediately you become aware of a possible breach, you should report this in the first instance to the Presbytery Clerk, who will take the appropriate steps in accordance with the Presbytery's data security breach management policy, which can be found here http://www.churchofscotland.org.uk/__data/assets/word_doc/0004/49234/Data_security_breach_management_policy_Presbyteries.docx.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says that those concerned must be informed directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, it will be necessary to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, those affected will have to be informed promptly, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If it is decided not to notify individuals, it will still be necessary to notify the ICO unless it can be demonstrated that the breach is unlikely to result in a risk to rights and freedoms.

All decision-making should be documented in line with the requirements of the accountability principle.

DATA PROTECTION OFFICERS

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances, and contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO. A DPO **must** be appointed if an organisation:

- is a public authority;
- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

The third category is the only one which might apply to congregational activities, although it is unlikely that normal processing of "special category data" (e.g. data relating to religious beliefs) in a congregational context would be deemed to be on a "large scale". Despite this, it would be prudent for the Church at Presbytery and congregational level to give one person formal responsibility for data protection issues and designate that person as the DPO. At Presbytery level, this will usually be the Presbytery Clerk, and reflects the current role of the Presbytery Clerk as data controller for all of the congregations within the bounds of the Presbytery.

The DPO's minimum tasks are:

- To inform and advise the congregation/Presbytery and its members and staff about their obligations to comply with the GDPR.
- To monitor compliance with the GDPR, including managing internal data protection activities, train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

REGISTRATION WITH THE ICO

The Current Regime

Related to this is the question of the need for data controllers to notify or register with the ICO. Under the current Data Protection Act, organisations that process personal information are required to notify the ICO as data controllers (unless an exemption applies). This involves explaining what personal data they collect and what they do with it. They are also required to pay a notification fee, based on their size, of either £35 or £500. Charities pay only £35, regardless of their size and turnover.

When the GDPR comes into effect there will no longer be a requirement to notify the ICO in the same way. However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

The New Regime

On 20 February 2018, the UK Parliament published draft Regulations setting out a requirement for data controllers to pay a charge, and provide information, to the ICO as of 25 May 2018.

A charge of **£40** (with a £5 discount for direct debit payment) will apply to charities in respect of each 12 month "charge period". The date on which that "charge period" begins will differ depending on whether the controller is an existing controller before, or only becomes a controller after the Regulations come in to force.

Although the 2018 Regulations come into effect on 25 May 2018, this doesn't mean everyone has to pay the new fee on that date. Controllers who have a current registration (or notification) under the 1998 Act do not have to pay the new fee until that registration has expired. Presbyteries should therefore continue to renew their notification as usual, and payments made during the 2017/18 financial year under the current system will run for a full year. It is expected that individual congregations will not have to pay separate fees, but that Presbyteries will continue to pay one "umbrella" fee for all congregations within their bounds.