The Church of Scotland

Data Protection General Guidance for Congregations

Contents

1. Introduction

The right to privacy is a fundamental right, enshrined in the European Convention on Human Rights. There have been data protection laws in place for some time, the most recent change being the introduction of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA). Even though the UK is no longer a member of the EU, the UK Government has legislated to ensure the DPA and the revised UK GDPR will maintain equivalent high standards of protecting individuals' rights under privacy laws. This guidance provides congregations an overview of the main provisions of data protection laws. Further guidance, a set of FAQs and styles relating to specific areas where policies or procedures are required under law, are also available for use by congregations and Presbyteries.

2. The Key Definitions

Before looking at the key data protection principles which have underpinned data protection laws for a number of years, it is worth reviewing the key definitions in the law. These are:

- 'Personal data'
- 'Processing'
- 'Controller'
- 'Processor'

Personal data This is defined 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."*

This definition relates to living individuals and to data held electronically or in paper records/in manual filing systems. There is also inclusion of location data, online identifiers (e.g. IP addresses) and genetic or biometric data. The definition may include 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, 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. Congregations 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 congregation in accordance with data protection law. Further, if a congregation uses cookies on its website to monitor browsing, it will be collecting personal data of that individual and an appropriate cookie policy should be in place with functionality to allow the user to refuse all cookies. Further guidance on cookies is available on the ICO website Guidance on the use of cookies and similar technologies | ICO

Processing is defined in law as *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."* This definition is broad and captures all activities that are carried out with personal data. It includes collecting, editing, storing, holding, disclosing, sharing, viewing, recording, listening, erasing, deleting etc. Individuals responsible for processing personal information in congregations may include the minister and other office bearers, treasurers, administrators, group leaders, safeguarding coordinators and others.

Controller is defined in law as *"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. 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 must not use any personal information being processed on behalf of the congregation for their own personal use. This is unlawful under Section 170 of the Data Protection Act 2018 and individuals can be prosecuted by the regulator. Personal information must be used only for the specific purposes for which it has been lawfully obtained (see below for more on this and the other data protection principles).

Processor is defined in law as *"a natural or legal person, public authority, agency or 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. An example would be an IT supplier engaged by a congregation to provide a new system on which personal information will be stored. Under data protection laws, processors will be jointly and severally liable with controllers for data breaches, to the extent for which they are responsible. Any congregation using, or considering the use of, a 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.

3. Special category data

It is important that congregations are aware of what special category data is and understand that it requires additional safeguards to protect the data. It is personal data which are stated to be more sensitive than other types, and so require additional protection and safeguards. Special category data is:

- Information which discloses racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health or
- data concerning a natural person's sex life or 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.

It is important to note that one type of data which used to be classed as 'sensitive' under previous legislation no longer has this classification. This is criminal data: alleged crimes, convictions etc. This is handled separately to special category data and within the UK GDPR there is a specific article (Article 10) detailing how this data should be handled, what non-law enforcement organisations can do and what processing sits entirely with law enforcement and intelligence organisations.

3.1. How should special category data be handled?

When processing special category data, it is important that there are additional measures in place to protect the data. This can include files being encrypted or password protected if the data is electronic. If itis held in a physical/paper record then it should be locked away when not in use. Access control whether electronic or physical is important to protect the sensitive data from being disclosed to unauthorised recipients.

There are two main lawful bases for processing special category data by congregations (although others may also apply in certain circumstances):

- the data subject (individual) has given explicit consent to the processing of the personal data for one or more specified purposes (Article 9(2)(a)) 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 (Article 9(2)(d))

The latter lawful basis will 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, 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 congregation; 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" basis.

3.2. 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. If emailed to Presbytery, the transfer should be carried out securely with files being encrypted or password protected and the password provided in a separate email after confirmation that the initial email and file have been received.

It is important to remember that the "legitimate activities" lawful basis only applies if the special category data is not being disclosed out with the congregation 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 must not be done without explicit consent. In those instances, it is important that a record is kept of that consent and that the individual is able to withdraw that consent at any time. Further guidance on consent and a model consent form is available on the website.

"Legitimate activities" processing will involve special category data 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 lawful basis 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.

4. The Data Protection Principles

Data Protection laws have six key principles which must be complied with when processing personal data. There is also an overarching principle: 'Accountability'. The principles are as follows:

4.1. Lawfulness, fairness and transparency
4.2. Purpose limitation
4.3. Data minimisation
4.4. Accuracy
4.5. Storage limitation
4.6. Integrity and confidentiality and

4.7. Accountability

Principle 1 - Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner. People have a 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. More guidance on meeting the fairness and transparency part of this principle is detailed under Data Subject Rights – the Right to be Informed.

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

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

This is detailed under UK GDPR Article 6(1):

a) **the person has given consent to the processing of their personal data for one or more specified 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, Article 6(1)(f) will often be the lawful 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 purpose of which you are processing, but because consent can be withdrawn at any time. If it is withdrawn, you are

likely to have difficulty in continuing to process the data 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. There are specific rules detailed in Article 7 for consent to be valid. If these conditions, as described above, are not met then consent would be invalid and could not be relied upon for the lawful basis.

If relying on the legitimate interests as a lawful basis it is essential that you can demonstrate that this basis of processing applies, and there is a 3-stage test for doing so. You must: -

- 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 then the legitimate interests lawful basis will not apply. You must balance your interests against the rights and freedoms of individuals. 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. An LIA template and guidance note has been produced by the Law Department and is available on the website. You must include details of your legitimate interests in your privacy notice.

Consent as a legal basis for processing personal information

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 law. In particular, under the UK GDPR the legal basis of "consent" gives individuals much more control over their data and its uses than they had under the previous legislation.

In the previous law, consent was seen as the first choice for the lawful basis of processing personal data. Now, however, the high standard for consent to be valid means that in general consent would not be the correct condition to use. For congregations the more appropriate lawful basis of "legitimate interests" is likely to apply. There will be situations where consent is the appropriate legal basis for processing personal information, for example 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 and records of consent are held.

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 (purposes) 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.

A number of conditions must be met for consent to be valid. These conditions include that consent must 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 consent in the first place); it must be clearly distinguishable; and the congregation must be able to prove compliance. This means that the congregation should keep the signed consent forms as a record to evidence that consent has been properly given. If an individual does withdraw consent, then this record should be updated to ensure that the processing activity is no longer carried out with that individual's data. 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: Data Protection Consent Form along with guidance on consent.

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. When relying on consent, keeping the record of that consent is important to evidence compliance. The ICO has provided useful checklists (Consent | ICO) 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 to

(a) be clear about the reasons why you are collecting personal information from individuals
(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 collecting personal data excessively or in case it is considered it may be useful for another reason only collect what is necessary for the purpose.

Principle 4 – Accuracy

Personal data must be accurate and, where necessary, kept up to date. This means that every reasonable step must be taken to ensure that personal data which are inaccurate or incomplete, having regard to the purposes for which they are processed, are rectified without undue 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 regularly what information you are holding and with a view to assessing the retention periods to ensure data is not held longer than necessary.

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 is much easier to comply with the requirements of data protection laws. Carrying out the audit will enable you to assess what data does need to be destroyed as it is past the retention period, this will aid in improved information governance of the information held by the congregation.

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 7. Regular reviews of Supplementary Rolls should be carried out to determine why information is being held and whether it may be appropriate to no longer hold it and destroy the information securely. 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 details contained in the rolls there will be a record of their membership which can be provided to them if they exercise their Right of Access.

A separate guidance note on data retention is available: Data Retention Policy [insert link]. A data audit template is available: Data Audit Form [insert link].

Principle 6 – Integrity and confidentiality

Personal data must be processed in a way that ensures there is appropriate security measures in place to protect the personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage. Technical and organisational measures which are reasonable and proportionate to the type of data held are required. So, data held electronically should be kept on secure computer systems and where the data is held in physical format it should be held in secure manual filing systems and be locked away. 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.uk" 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. It is also important that your computer has up to date anti-virus software to protect the data held on the computer from virus attacks.
- A hard copy of personal information should be securely stored and not visible or accessible when it is 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 in an electronic format or locked securely if in a physical format. This is to protect the individuals from damage or distress if the data was lost or stolen.
- Any data held on computers should be backed up regularly and these back-ups held securely.
- 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 to be publicly displayed.

The Church must respect the individual's right to privacy. 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 legally obliged to disclose the data.

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 any personal 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. It is therefore vital that identity checks are carried out to ensure no data is disclosed to unauthorised individuals.

Most breaches 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, whether sending it electronically or in hard copy and ensure that appropriate security controls are in place.

Principle 7 – Accountability

The Accountability Principle was introduced by GDPR. It is designed to ensure controllers and processors are able to evidence compliance with the six principles. So, you have to be able to demonstrate that you are compliant. To be able to do this, congregations should, for example, document the decisions taken about the various types of data processing, provide and record staff and volunteer training, review policies and procedures and audit processing methods and activities. There is a lot of material on the Church website to help with this:

- a data audit template
- a record of processing activities template
- privacy notice template
- a security breach management procedure and breach notification template
- a retention and disposal schedule
- legitimate interests assessment form

5. Data Subjects Rights

Individuals have a number of rights under data protection legislation. Not all of these are absolute rights, some only apply depending on the lawful basis for processing. With these rights, it's important to note that when individuals exercise their rights they are under no obligation to mention the right, or even reference data protection laws. They can exercise their rights either in writing or orally. The important aspect is that such requests are recognised and processed within a month of receipt of the request. All data subject rights and what they mean are detailed below. The chart highlights which rights apply, depending on the lawful basis for processing.

	Lawful Basis for Processing					
DS Right	**Consent**	**Contract**	**Legal Obligation**	**Vital Interests**	**Public Interests/task**	**Legitimate Interests**
Access	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Rectification	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Erasure	**Yes**	**Yes**	**No**	**Yes**	**No**	**Yes**
Restrict Processing	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Portability	**Yes**	**Yes**	**No**	**No**	**No**	**No**
Object	**No**	**No**	**No**	**No**	**Yes**	**Yes**
Automated Decisions	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Withdraw Consent	**Yes**	**No**	**No**	**No**	**No**	**No**

5.1. The right to be informed

Individuals have the right to be informed, by being given a "privacy notice" 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 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. It is recommended that privacy notices are published and provided to each individual when their data is collected either by a link to the relevant notice or by providing it in paper format.

Privacy notices should include:

- The identity of the congregation, and the key contact person, normally the Data Protection Co-ordinator
- how it is intending the information will be used (i.e. the purpose of processing),
- what personal data and special category data is collected
- what the source of the data is if not directly from the individual (if directly from individual then this section does not need to be included in the notice)
- the lawful basis for processing the information

- whether data is shared and if so with whom, (if applicable)
- whether the data is transferred outside the UK (if applicable)
- whether any automated individual decision-making, including profiling occurs (if applicable)
- how long the information will be retained for,
- what individual rights apply for the processing purpose
- and that individuals have a right to complain to the ICO if they are not happy with how their personal information is being processed.

Privacy notices 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).

Privacy notices should be provided at the point of data collection. 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. However, from a good practice perspective it's appropriate to ensure any individuals can view the privacy notices when/if they wish to and this is easily achieved by publishing the notices on the website.

NOTE: if your congregation has employees, there should be an employee privacy notice specifically detailing what personal data, and special category personal data, is collected for employment purposes, what the lawful basis is, whether it is shared and with whom, for example HMRC for tax purposes, and how long the data is held for. There is a sample privacy notice for use by congregations which cover employment privacy notices and a separate one for the data collection of congregations. These sample notices can be found here: Privacy Notice. There is also a template with all the relevant sections that privacy notices have to have and with drafting notes. This is available here.

Note: It's important to note that privacy notices and consent forms are not the same documents. Privacy notices tell individuals how their data will be processed and meet the legal requirement of individuals being fully informed. They are required to inform the individual what 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. Consent forms should be used to record the consent of the individual and to keep that record of consent.

5.1. The right of access

This right of access basically provides individuals with the right to access a copy of their personal data from the controller, by way of a "subject access request", also known as a SAR. Individuals are entitled to receive a copy of their information free of charge and within one month of the request being made. Depending on the request, it may be necessary to clarify the request and also verify the

identity of the requestor. It's important that there is an identity check carried out prior to any disclosure of information to ensure personal data is not disclosed to an unauthorised individual.

When answering such a request, individuals should also receive the associated privacy notices in relation to the processing. So, for example, if the individual is a member of the congregation then they should be provided with a copy of the privacy notice, along with the records relating to them. It's important to note that there are some exemptions to disclosing data under the subject access provisions. This can apply if the data held also contains a third party's personal data and therefore the data is known as mixed data. There are other exemptions for certain types of information, for example legal advice. In these instances, advice should be sought from the DPO at the National Offices to ensure appropriate redactions are made prior to disclosure.

It is possible to refuse manifestly unreasonable or excessive requests. However, this has a number of requirements to meet prior to refusing such a request and it is recommended that advice is sought before doing so.

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.

5.2. The right to rectification

Individuals have the right to have incorrect or incomplete data rectified if it is inaccurate or incomplete. This right links with Principle 4 - 'Accuracy' - and highlights the importance of keeping records accurate and up to date. As with all other rights, except for the right to be informed, this right requires the organisation to act within one month in receipt of the request.

5.3. The right to erasure - "right to be forgotten"

This is not an absolute right. Whether it applies will depend on the lawful basis of processing. Individuals have a right to have personal data erased by the 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 are no overriding legitimate interests for continuing the processing.
- the personal data are unlawfully processed (i.e. otherwise in breach of the data protection laws).
- 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 withdraws their consent or when the purpose for which the data was collected is complete. 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.

5.4. The right of restriction

This right links with the other data subject rights. 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 until the issue is resolved. In such an event the data can continue to be stored but not used or processed in any further way until the issues are addressed. It's important that the restriction is applied while the other right is fully exercised.

5.5. Right to data portability

The right to data portability will rarely arise in the Church setting. This right means an individual can request an organisation to provide an individual's data in a machine-readable format, e.g. a .csv file and transfer it to the data subject or to another organisation to access improved services. This right applies more in relation to changing banks or energy suppliers. It only applies to data that the individual has provided to the controller and allows individuals more control over their data to access better services. It is unlikely that this right would be exercised in the Church environment.

5.6. The right to object

Individuals have the right to object to the processing activity if they are not satisfied that you have a legal basis for doing so. The right is not absolute unless the objection is made in relation to marketing. When marketing, the right to object is absolute and the organisation must cease communicating marketing information to the individual. In general, the right to object only applies when the lawful basis is on public task/interest or legitimate interests. If the basis is one of these then it will be necessary to consider the objection fully. You must stop processing the personal data unless you 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 data collection" and in privacy notices. This applies to all data subject rights: they must be fully informed as to what rights apply to the processing and how they can exercise those rights.

5.7. Right to be informed of automated individual decision making, including profiling

Individuals have the right to be informed of any automated individual decision-making (i.e. the decision is made solely by automated means without any human involvement) and profiling (which is automated processing of personal data to evaluate certain things about an individual). Examples of this include credit references/scoring, recommendations based on items you've bought online etc. There are specific rules around whether this processing is allowed. There are only three lawful bases which allow it: contract, explicit consent or authorised by law applicable to the controller. If these lawful bases don't apply then this type of processing cannot be carried out.

If you are processing in this way, you need to ensure that individuals are fully informed about the processing, that there are simple processes for the individual to request human intervention or challenge a decision and that checks are carried out regularly to ensure the systems are working as intended. In general, the Church does not process data in this way so it's unlikely that congregations will have to consider this right.

6. Data Security Breach Procedure

A data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". It's not just losing data; it includes disclosure to the wrong person and alteration of data. Breaches can be classified in three ways:

- Confidentiality breach – this is an unauthorised or accidental disclosure of or access to personal data. This is the most common type of breach.
- Integrity breach – this is an unauthorised or accidental alteration of personal data
- Availability breach – this is an accidental or unauthorised loss of access to, or destruction of personal data.

Whatever type of breach it is, the key points are to act swiftly to try and contain the breach and if possible recover the data. It is also vital that a breach is reported to the Church's Data Protection Officer (DPO) quickly to ensure that breaches are reported to the regulator, if necessary, within 72 hours of the breach being detected. It's also important to assess the potential impact it could have on the affected individuals. If it could cause unwarranted harm and/or distress then the individuals should be informed to enable them to take action to protect themselves. However, it is not always necessary to report to the regulator or to the affected individuals.

6.1. What breaches must be reported to the ICO?

When a personal data breach has occurred, the 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 within 72 hours. If it is unlikely that there is such a risk then it would not need to be reported to the ICO. 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. It is important to record a breach, carry out the investigation and assess whether there are any lessons learned which would reduce the risk of the breach occurring again.

It is for the controller to decide whether a breach is reportable. However, processors are legally required to notify the controller without undue delay after becoming aware of a personal data breach.

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, specifically the DPO.

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

6.2. What information should be provided when reporting a breach?

When reporting a breach, 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 breach; and
- a description of the measures taken, or proposed to be taken, to deal with the breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

You should use the breach notification form provided within the style data security breach management procedure on the Church website. This should be sent to the Church DPO to assist in assessing whether it needs to be reported to ICO and if appropriate the DPO will make that report.

6.3. 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 controller must communicate the breach to the data subject(s) without undue delay. This is not required if the data is encrypted or there are other controls in place which make the data inaccessible.

'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.

In making this assessment 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 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.

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 the rights and freedoms of the affected individuals.

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

7. Data Protection Co-ordinators

The UK 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 DPO's minimum tasks are:

- To inform and advise the congregation/Presbytery and its members and staff about their obligations to comply with the data protection laws.
- To monitor compliance with data protection laws, including managing internal data protection activities, training staff and members and conducting internal audits.
- To be the first point of contact for supervisory authorities, i.e. UK Information Commissioner's Office (ICO) and for individuals whose data is processed for them to exercise any of their rights and if they have queries in relation to the processing of their data.

The third category which may require a DPO to be appointed is the only one which may 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 Data Protection Co-Ordinator. At Presbytery level, this will usually be the Presbytery Clerk, and reflects the current role of the Presbytery Clerk as controller for all of the congregations within the bounds of the Presbytery. The Data Protection Co-Ordinators can act as the key contact for individuals and ensure the appropriate policies and procedures are in place. The Data Protection Co-Ordinators can seek advice and guidance from the Church's DPO.

8. Notification with the UK Information Commissioner's Office (ICO)

The Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader who processes personal information to notify with the ICO that they process personal data and pay a data protection fee, unless they are exempt. For the Church as we are a charity we are only required to pay £40 (with a £5 discount for direct debit payment). The notification and fee should be made on an annual basis. Congregations do not have to pay for the notification fee: the Presbytery acts as the controller and pays the notification fee which will cover all the congregations within that Presbytery.