

## GDPR: Frequently Asked Questions

### 1. What is the GDPR and must we comply with it?

The General Data Protection Regulation (GDPR) will take effect in the UK on 25 May 2018. It replaces the existing law on data protection contained in the Data Protection Act 1998. Broadly speaking, it gives individuals more rights and protections with regard to how their personal data is used by organisations. Conversely, this means that stricter laws are imposed to ensure that organisations securely manage any personal data they hold and are transparent about how they use this data. Congregations and Presbyteries must comply with the new law, as there are no relevant exemptions for charities or small organisations.

### 2. Are there any positive steps we should be taking to comply with GDPR?

Yes. The new legislation provides an incentive to consider what information is being held and whether it might be time to let go of anything that is no longer required. In line with that, a data audit should be carried out with the aim of establishing exactly what personal information is held, along with a number of other essential details. A data audit template has been created which you may find useful. [Data Audit Form](#)

Once it is known what information is held, it will be much easier to take steps to comply with the new legislation, as this will hopefully aid a “clear out” of redundant personal data and result in a more streamlined information management system.

### 3. Must we obtain consent from all members on the Congregational Roll to hold or process their personal data?

No. Generally speaking, a consent exercise will not need to be carried out to hold or process the personal data of those listed on the Congregational Roll. Processing what the GDPR calls “special category personal data” (such as information about religious belief) is permitted when it is carried out in the course of its legitimate activities by a not-for-profit body with a religious aim. So long as information relates solely to members (or former members) of the congregation or people who have regular contact with the congregation, and the information is not shared beyond the congregation, this is permitted without the need for explicit consent.

Consent will be required where personal information (such as names, contact details, photographs) can be accessed by third parties. This could include uploading personal information to a congregational website or printing it in a church magazine. Consent will also be required where the data concerns children (a child is deemed to be someone under the age of 18).

### 4. What about information held on the Supplementary Roll?

Whether or not it is appropriate to retain information about members or former members on a Supplementary Roll will depend on what information is held and what use is made of it. If you know why you want to retain it, and have a legitimate reason for doing so, then this will be permitted. If you have no real or foreseeable need to retain the information, it should be deleted.

#### **5. What form should consent take, if explicit consent is necessary?**

Any consent must be freely given, specific and informed. It must be explicit: in other words it must represent an unambiguous indication of the wishes of the individual. At the point consent is given, it must be made clear that it can be withdrawn at any time. A style consent form can be found here. [GDPR Consent Form](#). Where it is not practical to use a written consent form an exchange of email will suffice.

It is not always essential that consent be written. Oral consent can also be given. For example, if photographs are taken at a church event for which written consent forms were not prepared in advance, those attending can simply be asked if they are willing to agree to their photographs being published or used in a particular way. This could be done by an announcement at the event, indicating how the pictures will be used. You should also make sure that people are aware of who they should speak to if they do not wish to be in the pictures or do not agree to their photograph being used in this way. Where consent is provided orally a note of that should be made on the day and retained. Please refer to the separate note in relation to information storage containing practical hints and tips. [Information Storage and Security Practical Hints and Tips](#)

If the photograph is of the event in general, and not a close-up of an individual, you do not need consent for this to be published. It is a question of whether the individual is the focus of the photograph; if not, their consent is not needed.

#### **6. Do we need to renew existing consents?**

Not necessarily. If consent is the appropriate legal basis for processing personal data, and that consent has been clearly and unambiguously given and is documented, it does not need to be renewed. You should, however, review whether this is the case. Consent can, over time, “degrade”, so it is a good idea to revisit and renew consents periodically, perhaps every 5 years or so.

#### **7. What is a Data Privacy Notice and do we need one?**

From 25 May 2018, congregations will need to have a Privacy Notice in place. This is a policy document which sets out how personal data will be stored and processed by the congregation, the legal basis for processing, and the rights of the individuals in relation to that data. A style Privacy Notice for congregations can be found here. [Privacy Notice](#)

The Privacy Notice should be available on the church website, if there is one, and a copy should be put up on a noticeboard where those whose information is being gathered will be able to see it. Awareness of the Privacy Notice should be raised now, and on an annual basis by drawing attention to it by, for example, including reference to it in the intimation sheet or church magazine.

**8. Are there any GDPR implications when 'streaming' church services?**

Streaming is the broadcasting of church services online via the internet, whether in a 'live' or pre-recorded format. There are important considerations to bear in mind both before and during the broadcast if your congregation is keen to proceed in this way. Please refer to the separate guidance note on this topic. [Live streaming Guidance Note](#)

**9. If someone wants to have their personal data deleted do we need to comply with this request?**

Whilst this is not an absolute right, there are circumstances where individuals have a right to have their data erased without undue delay. Such circumstances include: the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; the individual withdraws their consent; the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; the personal data is unlawfully processed i.e. in breach of the GDPR; or the personal data must be erased in order to comply with a legal obligation. For more information please refer to pages 14-15 of the GDPR general guidance for Congregations note. [GDPR General Guidance for Congregations](#)

**10. We understand that some records ought to be archived: at what point are we required to do this?**

Manual records and any mobile devices such as laptops holding information electronically should be kept in lockable fire retardant storage in the Church Office or Vestry. Once minutes and other records of future historical interest are more than 50 years old, they should be sent to the Principal Clerk's Department. They will then be passed to the National Archives for safe keeping and made available to the public after approximately 100 years for research purposes.

**11. We rent our Church Hall to various groups (including the Guides and BB). How should we be dealing with them?**

The BB and others will be covered by their national bodies and those who are using the halls ought to be compliant with data protection law. This is a condition of the style hall letting agreement available on the Law Circulars section of the website. [Letting of church halls to non-church bodies](#)

The congregation will not legally be responsible for any data security breaches by users of the Hall, but if you are aware that there are breaches occurring, it is recommended that you have

a word with those involved to check they know that they ought to be complying with the GDPR.

#### **12. Can we continue to display Cradle Rolls?**

Congregational cradle rolls which are on public display should only include the name of the individual and the date of their baptism. Before such personal data is publically displayed consent to do so should also be obtained from the parents, if it is a child that has been baptised, and otherwise from the individual themselves. Note, however, that retrospective consent for those named on a baptismal role already on display (pre-GDPR) is not required as there is already an existing relationship with those individuals and a legitimate interest to display the data.

#### **13. What about Baptismal Registers?**

As long as there is a legitimate reason for collecting and retaining information, it is lawful to continue to do so. Use of personal data for public interest archiving, scientific, genealogical and historical research and statistical purposes is permitted. You should inform individuals at the point you are collecting information for baptismal registers that this is why you are doing so. You must store this information securely – for example, by using a lockable document case – if you are transporting the information out with a secure storage location. This could occur if records are to be inspected by Presbytery and you are required to take the baptismal register to a specified location for checking.

#### **14. Can we include people on prayer lists which are circulated amongst members of the congregation?**

You will need their consent if you are going to publish these lists on the church website or in a newsletter or church magazine. You won't need explicit consent if prayer lists are simply circulated amongst (for example) members of a prayer group.

#### **15. Can we continue to circulate congregational or Presbytery directories?**

Yes, so long as the information contained in such directories is accurate, relevant and you know why it is needed. They should contain the minimum personal information necessary for the purpose (for example, name, email address and telephone number), should be kept securely and should not be circulated beyond those who need to have this information for congregational or Presbytery purposes.

#### **16. How long should we keep information for?**

This depends on the type of information involved. Please refer to the style data retention policy which is on the Church website, a link to which can be found here. [Data Retention Policy](#)

#### **17. What if we have a data security breach?**

Generally speaking, data security breaches required to be notified to the Information Commissioner within 72 hours (where feasible). All potential data breaches should in the first instance be reported to the Presbytery Clerk as soon as possible and the Law Department, in liaison with the Clerk, will make any necessary notification. The breach notification form [Breach Notification Form](#) should be completed and the data security breach management procedure should be followed. [Data Security Breach Management for Presbyteries](#)