Presbyteries, Congregations, and the 'GDPR'

Some Common Myths and Frequently Asked Questions

Before we get to the FAQ's, here are some **common myths**:

Myth 1 - GDPR is only applicable to large organisations

This legislation applies as much to a small church as it does to a large company – providing that small church holds personal information.

Myth 2 - This only relates to information held electronically

Not true. The GDPR relates to all personal data held, whether it is in electronic or paper format. Electronically it can be held not just on computers but on any electronic device such as tablets, mobile phones, portable drives etc. In hardcopy or paper format it could be in a file, in a minute book, in a personal notebook etc.

Myth 3 - GDPR is completely new data protection legislation

We have all for many years been lawfully processing personal data under the Data Protection Act 1998. The GDPR is adding a few new elements, but this is not new legislation which suddenly imposes good data protection practice on you. There may, though, need to be some changes to your processes, particularly in how you respond to enquiries from data subjects.

Myth 4 - You have to fully comply by May 2018

The Information Commissioner's Office (the regulatory agency in UK overseeing GDPR) has already said that it expects organisations to work toward compliance, and if they aren't ready by May 2018 it would expect to see a plan for how it will be achieved within a reasonable time frame after May. However, GDPR has been in place since 2016 and the ICO will not adopt a lenient approach indefinitely. The time to act is now.

Myth 5 - Breaches will receive Huge Fines

The upper limit for fines is indeed much higher than previously, but the ICO has already said it much prefers the carrot to the stick and has in fact never levied the current maximum fine even in the most serious data breaches. The ICO concluded 17,300 cases last year (2016-17) and only 16 resulted in fines for the organisations concerned. The ICO remain committed to its main role of "guiding, advising and educating organisations about how to comply with the law." It is more concerned with helping organisations 'get it right' than it is with fining them for small misdemeanours, however, it is still possible that a church could be reported to the ICO for a Data breach.

Myth 6 - Everything needs Consent

There are many ways to legally process and share data without needing consent. We are already aware of some software companies saying that you'll need consent to store and use any personal data of any kind – this is simply not true. For example, some processing is legally required, or can be done in the legitimate interests of the data processor. You do not need and should not use consent to store specific information in personnel files for your employees.

Myth 7 - The right to be forgotten

This is actually a right to request erasure of data once an organisation has ceased processing that data. Clearly there will be data we hold e.g. related to safeguarding, which we will be processing for a very long time and for statutory reasons and so are unlikely to agree a request for erasure.

FAQs – Frequently Asked Questions

1. Can we still publish our Register/Directory of Members?
2. We share personal data with presbyteries and General Assembly – does this constitute sharing with a third party?
3. Does passing the church directory or yearbook to a printer constitute sharing data with a third party? And, how can we control what happens to our church directory which we make available to members in print or electronic format?
4. Do we have to appoint a Data Protection Officer/Lead?
5. Do we really need to have all these new policies?
6. Will we still be able to communicate prayer requests?
7. How are 'appropriate security measures' to be defined when it comes to processing personal information?
8. What about minutes of meetings which contain personal information?
9. How can we be sure that any Data Processor that we use (e.g. cloud-based storage, survey software, payroll processing, BB, Omega etc.) to process personal information is GDPR compliant?
10. What about groups within a church sharing contact details with each other – are privacy statements or specific consent needed?
11. When putting together a Registration Form for (for example) a Holiday Club, do we need to include the text of the Privacy Notice on the actual form or can we just provide a link to the Privacy Notice on our website?
12. How can we provide Data Protection training for our 'staff' (including volunteers)?
13. What about the use of images in our publications, social media or website?

14. Do we need to register with the Information Commissioner's Office (UK) or the Data Protection Commissioner's Office (RoI) and is there a fee payable?
15. As a trustee of the congregation could I be held personally liable for a data breach, and if so, is there any protection against personal liability?
16. Do we need to get all of our existing consents with people renewed?
17. I've heard people talk about having to do a Data Protection Impact Assessment – what is a DPIA and is this likely to affect us?

1. Can we still publish our Register/Directory of Members?

The church rules require that 'a register of members along with contributions must be maintained by each congregation'. That register must therefore be created and maintained and is a legitimate activity of a not-for-profit body under GDPR. As to whether it may be published that would depend on whether or not the names are disclosed outside of the church to third parties or not. If this is the case then the consent of the members should usually be obtained.

You should certainly seriously ask the questions why? and how?;

- 'is there an important legitimate reason why we publish this information?' and
- 'is there any other way in which that purpose might be served without publishing this information?'

It is also worth noting that where WFO contributions are published within a congregation best practice is to anonymise this using only WFO number and amount.

2. We share personal data with presbyteries and General Assembly – does this constitute sharing with a third party?

With regard to the relationship between Congregations, Presbyteries and the General Assembly the Information Commissioner's Office has been written to concerning relationships between these bodies in respect of GDPR. We shall be seeking agreement that the sharing of data within this relational arrangement does not constitute sharing with a third party.

3. Does passing the church directory or yearbook to a printer constitute sharing data with a third party? and ….. How can we control what happens to our church directory which we make available to members in print or electronic format?

In the first place you should always ask the question as to whether personal data needs to be processed in this way – is there an important and legitimate purpose fulfilled in doing so. If there is and you can justify it if required to do so then you might argue that there is legitimate basis.

In essence you will not be able to 'control' what happens to any directory once you have distributed it. This is the case whether it is sent by email or printed off and handed out – paper copies could be left lying around or passed on anywhere!

In both situations it is important is that those whose names and contact details are on such a list are aware of how their personal data is to be used and they can make their own judgement about the risks to them. You might communicate this through an appropriate privacy notice.

In the case of the printer you will need to have a contractual arrangement with them as they are a Data Processor acting on your behalf and they will need to comply with the GDPR as a Data Processor.

4. Do we have to appoint a Data Protection Officer/Lead?

Churches do not have to appoint someone in this capacity but they will find it extremely helpful to have a member take on responsibility for ensuring the church abides by its policy and to act as a point of contact for anyone with concerns as to how their information is being handled. We have provided a template for this role on our GDPR webpage (www.presbyterianireland.org/gdpr).

5. Do we really need to have all these new policies?

All presbyteries and congregations will be considered as Data Controllers under GDPR and will have a responsibility to comply. The template guidance, policies, and forms supplied on the GDPR webpage are there to assist you in complying. They should be regarded as a toolkit and not simply adopted uncritically, you may wish to modify (soften the language, simplify the processes and procedures) and adopt them to fit your own situation and circumstances. GDPR imposes new obligations on data controllers to be able to demonstrate compliance. The best way to do this is to implement and follow appropriate policies.

6. Will we still be able to communicate prayer requests?

Prayer requests are often communicated within a prayer chain or prayer group using email, messaging, WhatsApp groups etc. This can continue but you should take time to review their guidelines for how this is used. This is not a new issue as under the Data Protection Act 1998, a data controller passing on (in a 'written' form) sensitive personal information about someone without their consent is breaching the Data Protection guidelines. Please note that this only applies to the church itself in an official capacity. Individuals acting in a purely personal capacity are not covered by GDPR. Our general guidance on this issue would be that churches should ensure that:

a) Wherever possible they make sure that the people who are being prayed for have given their consent, (which can be verbal but should then be recorded), for this. There will be people (particularly if they are not actually part of the church) who would be very unhappy to discover that something they thought they had shared with one person in confidence was suddenly being relayed by email around a group of other people they don't know;

b) Nothing is included in an email which you wouldn't want the person concerned to see [e.g. opinions about the person];

c) The people on the prayer-chain are asked to delete the email once it is not needed any more. This could be as soon as they have prayed, when a further update is received or when a situation has changed/improved so that prayer is no longer needed.

7. **How are 'appropriate security measures' to be defined when it comes to processing personal information?**

Data protection legislation states that "appropriate technical and operational measures" need to be taken to protect personal information which is being held. It is up to organisations to work out what this means for them.

One rule of thumb is that the more sensitive the information (and therefore the more damaging the effect of it being lost or stolen) the greater the level of security which is needed. Churches need to consider how valuable, sensitive or confidential the information they hold is and what damage or distress could be caused to individuals if there was a security breach. They can then decide what security measures should be put in place to protect it. There is a lot of useful free guidance and resource available through the web that you can refer to for securing both physical and electronic data.

8. **What about minutes of meetings which contain personal information?**

In one way or another, most meeting minutes will contain personal information – whether that is the names of the people attending or speaking or being talked about. This means that any individuals who are named or explicitly referred to do have the right to see those minutes. It is therefore helpful to bear that in mind when writing the minutes.

Generally speaking, minutes do not (and probably should not) contain sensitive personal information. There will however be occasions where minutes are taken of meetings where such information is discussed and it is felt necessary to record details in those minutes. Greater care needs to be taken with how such minutes are stored and distributed

9. **How can we be sure that any Data Processor that we use (e.g. cloud-based storage, survey software, payroll processing, BB, Omega etc.) to process personal information is GDPR compliant?**

Many of the major providers of these services are making preparations for GDPR which are intended to allow people to continue to use their services. The church should look into these and consider what they might need to do to continue using these services in a compliant way. In many cases you will find reference to GDPR compliance on the supplier website: for example, Google has a dedicated page about "How to opt in to the Data Processing and Security Terms and EU Model Contract Clauses" – see https://support.google.com/cloud/answer/6329727?hl=en. Once the additional Terms and Conditions are accepted, Google does the rest. For some smaller suppliers, where personal data is involved, you may need to contact the supplier. It is important to have a record of what categories of data is being processed, why, for how long and the security measures taken to protect the data. These arrangements should be provided for in the church's policies.

10. **What about groups within a church sharing contact details with each other – are privacy statements or specific consent needed?**

It is our view that communications within Home Groups or internal church groups such as informal prayer triplets and such do not involve sharing information with the church/Trustees as the Data Controller, so would not require privacy statements or require consent. In addition you can argue that the operation of such church groups are in the legitimate interests of the church so specific consent is not required.

Presbyterian
CHURCH IN IRELAND

11. When putting together a Registration Form for (for example) a Holiday Club, do we need to include the text of the Privacy Notice on the actual form or can we just provide a link to the Privacy Notice on our website?

You can simply have a link to a privacy notice on your website but you would need to be sure everyone completing the form was able to access that. Also it would be helpful to at least include the basics of the Privacy Notice on the form so that the people from whom you are collecting information have some idea what you will do with it without having to look elsewhere, you can then refer to the more detailed policy on the website or otherwise available (see the guidance supplied regarding consent). The important thing is that the information is clearly communicated in a way which the individual can understand.

12. How can we provide Data Protection training for our 'staff' (including volunteers)?

- Consider using/modifying material made available through the PCI website, at this point of introduction of GDPR, to train individuals.
- Consider using materials available through the ICO website.
- Your Data Protection Lead should periodically attend courses on data protection to maintain an up to date knowledge in this area and could then facilitate refresher training
- There will be consultancies who can deliver training either on site or via computer based training and these might also be considered.

13. What about the use of images in our publications, social media or website?

GDPR should be applied with a common sense approach. It is best to make it clear to anyone attending an event or being invited to participate in a photograph that photographs or videos might be used in this way. It is also good practice to ask for and record permission from the individuals whose images you choose to use. Remember that under GDPR consent must now be freely given, specific, informed and unambiguous.

In many situations it is best, (for example; in the case of planned publications and website), to stage the photograph or video using individuals who have already consented to having their image used in this way.

14. **Do we need to register with the Information Commissioner's Office (UK) or the Data Protection Commissioner's Office (RoI) and is there a fee payable?**

YES - unless you are confident you meet the exempt conditions for not-for-profit organisations as outlined below. As the ICO Annual Fee for churches is only £40 (£35 if you pay by Direct Debit) (or €35 if you are based in ROI) you should register if you think you may be processing information which falls outside this exemption.

If you are not currently registered you will probably find it best to wait until after 25 May to register as the new registration process should be easier than the current notification process.

The quickest way to register with the ICO is online at www.ico.org.uk/for-organisations/register. The Office of the Data Protection Commissioner: performs the same function in the Republic of Ireland - https://www.dataprotection.ie/docs/Registration-Guidance/1050.htm

‘Not-for profit’ organisations (including churches) are exempt from registration if they meet all of the following conditions:

- you are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it
- you only hold information about individuals whose data you need to process for this exempt purpose
- the personal data you process is restricted to personal information that is necessary for this exempt purpose

Please note that if you use CCTV then you will need to register.

If in doubt, consult the ICO or DPC website as both have guidance on registration.

Please note that legislation is currently working its way through Parliament which will replace the requirement to register with ICO with a “data protection fee”. The fee for all churches is currently proposed to remain the same as it is currently and there will be no effect on existing registrations (i.e. you do not have to pay the new fee until the existing registration has expired). If you are required to register and you do not you will be breaking the law and risk having to pay a fine (currently the maximum fine is £4,350 for this offence).

15. As a trustee of the congregation could I be held personally liable for a data breach, and if so, is there any protection against personal liability?

First of all it is important to state that churches will generally not hold the kind of sensitive data, or be processing it in such volumes, or in such ways that this is a serious risk. The risk environment is low. That said, the most effective way of managing any such risk is to minimise the possibility that any form of significant breach could occur, and that is why it is important to take data protection seriously and pay particular attention to protecting those areas of data processing which may involve sensitive data.

The second point to be made is that the regulators are essentially focussed on helping organisations to achieve compliance, they only use fines as a last resort and the evidence is that this is indeed their approach - in 2016-17 the ICO concluded 17,300 cases and only 16 of these resulted in fines for the organisations concerned. Fines will be used judiciously and proportionately and are commensurate with the degree of negligence and the seriousness of the breach. The regulator is much more likely to use warnings, reprimands or corrective orders and our greater risk may well be reputational.

Finally – the General Assembly is reviewing indemnity insurance and will issue further guidance on this when clarification is obtained.

16. Do we need to get all our existing consents with people renewed?

Not necessarily. Where you rely on consent, the ICO has stated that it will not be required to obtain fresh consent from individuals if the standard of that consent meets the requirements of the GDPR, i.e. consent has been clearly and unambiguously given and you have a record of that consent.
Nevertheless, it is important to review all consent mechanisms to ensure that they meet the standards required under the GDPR. If you cannot reach the high standard of consent as

set out in the GDPR, you must look for an alternative legal basis for processing the data or stop processing the data in question. Under the GDPR, consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Consent must be freely given, specific, informed and unambiguous (i.e. consent requires clear affirmative action from an individual (i.e. the data subject)). Silence, pre-ticked boxes or inactivity on the part of the data subject will not be sufficient. Individuals must also be informed of their right to withdraw consent at any time and how they can do this. In fact, it should be no more difficult to withdraw consent as it is to grant it.

17. I've heard people talk about having to do a Data Protection Impact Assessment – what is a DPIA and is this likely to affect us?

Essentially, it's a documenting process which will allow an organisation to systematically describe and analyse its intended processing of personal information, helping to identify and minimise data protection risks at an early stage.

As well as being a key element of a controller's accountability obligations under GDPR, an effective DPIA could have real benefits down the line in ensuring compliance, building external trust and avoiding the possible reputational and financial implications of enforcement action following a breach.

Under the GDPR, controllers will be required to complete a DPIA where their processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.

'Likely' does not mean the risk is certain, but it will be the responsibility of the controller to assess the level of risk of their intended processing by making a reasoned judgement on the likelihood and potential severity of harm.

It is unlikely to be something that individual congregations or presbyteries will need to be concerned with and is more likely to be required when a significant new process or system is being planned or indeed where there are significant changes to an existing system that processes personal data.

In common sense terms it follows the principal of 'data protection by design' and is a way of building the idea of data protection into our thought and planning processes where personal data is involved.

If you think that you might need to use a DPIA then there are useful resources on the ICO website and you can also contact the Data Protection Lead in Assembly Buildings.