

Data Protection Frequently Asked Questions



1. [What is meant by GDPR?](#)
2. [How seriously do churches need to take Data Protection?](#)
3. [Does being a CIO make any difference to the church in terms of our responsibility as a data controller?](#)
4. [What should we be doing to make sure we comply with this legislation?](#)
5. [Do we really need to have a Data Protection Policy?](#)
6. [Do we have to appoint a Data Protection Officer?](#)
7. [Can we use email to send prayer requests round our church?](#)
8. [How secure is 'secure' when it comes to holding personal information?](#)
9. [How can we control what happens to our church directory which we circulate by email?](#)
10. [What about minutes of meetings which contain personal information?](#)
11. [Do we need to have Data Sharing Agreements in place between different groups in our church who all hold their own lists of people attending?](#)
12. [How can we be sure that any cloud-based storage we use to store personal information is GDPR compliant?](#)
13. [How do we know that the US-based company we use to store/process our data provides 'adequate' protection?](#)
14. [Is it acceptable for church staff and volunteers to use their own computers for processing personal information on behalf of the church?](#)
15. [How can we provide Data Protection training for our 'staff' \(including volunteers\)?](#)
16. [Do we need to register with the ICO?](#)
17. [What advice can you give about groups within a church sharing contact details with each other?](#)
18. [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?](#)
19. [We use CCTV on our premises. What do we need to do?](#)
20. [Can you provide us with more information about obtaining consent – can we use tick boxes? How long does consent last? Is there an age limit?](#)
21. [Do we really have to get consent from everyone whose photograph we use on our website or in publicity?](#)
22. [What data protection matters do we need to consider when we live stream or record and upload videos of services or events for use on our website?](#)
23. [How does Brexit affect data protection?](#)
24. [What do churches need to do now the transition period has ended?](#)

What is meant by GDPR?

GDPR stands for the new General Data Protection Regulations which took effect from 25 May 2018. These regulations (and the Data Protection Act 2018) replaced the 1998 Data Protection Act strengthening the rights of individuals to control the personal information which organisations hold about them. Once the UK left the EU the 'UK GDPR' replaced the existing 'EU GDPR' but kept all of the main principles, obligations and rights in place.

Under these regulations the ICO (Information Commissioner's Office) has powers to impose very large fines on organisations which misuse personal information. Many have had to make significant changes to their ways of working. The Baptist Union are committed to providing information and resources specifically tailored to the needs of our member churches.

How seriously do churches need to take Data Protection?

Very seriously. This legislation applies as much to a small church as it does to a large company – providing that small church holds personal information either on a computer or in a paper-based filing system. This is why we have revised our [Guideline Leaflet](#) (L13) and put together a web-page of helpful information. (www.baptist.org.uk/gdpr) From this page you can follow a link to our [Data Protection Documents](#) page.

It is important to note that for all the talk about the potential for large fines to be imposed, the ICO remain committed to their main role of “guiding, advising and educating organisations about how to comply with the law.” They are more concerned with helping organisations ‘get it right’ than they are with fining them for small misdemeanours, however, it is still possible that a church could be reported to the ICO for a Data breach.

Does being a CIO make any difference to the church's responsibility as a data controller?

No. There is a technical difference in that in a CIO it is the CIO itself which is the Data Controller rather than the Trustees in an unincorporated church - but their responsibilities are the same in both cases.

What should we be doing to make sure we comply with this legislation?

Make sure at least one person in your church reads our Guideline Leaflet and then works through the checklist at the end.

Do we really need to have a Data Protection Policy?

If you hold personal information either on a computer or in a paper-based filing system then the answer is YES. To assist with churches with this we have provided a template policy for churches to adapt to suit their own circumstances. This is available free of charge on the [Data Protection Documents](#) page on our website. There is also a link to this from our main Data Protection page: via www.baptist.org.uk/gdpr

It is, however, equally important to make sure you have reviewed your processes and procedures for handing personal information so that they are compliant with your policy.

Do we have to appoint a Data Protection Officer?

Churches do not need to appoint someone in this capacity, but churches will find it extremely helpful to have a member of staff or one of their Charity Trustees 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. This person could be a “Data Protection Trustee” or whatever title you choose.

Can we use email to send prayer requests round our church?

YES - but churches should take time to review their guidelines for how this is used. This is not a new issue as under the 1998 Data Protection Act, passing on (in a 'written' form) sensitive personal information about someone without their consent was breaching the Data Protection guidelines. 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) 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.

Some churches send such emails by text message or 'WhatsApp' and the same principles apply for this or any similar method.

How secure is 'secure' when it comes to holding 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.

How can we control what happens to our church directory which we circulate by email?

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! What is important is that those whose names and contact details are on such a list are aware of how it is to be circulated and they can make their own judgement about the risks to them.

It is, however, a good idea to ask people to destroy old copies of a church directory when a new one is issued and to ensure that anyone who no longer wants their details to be included in the directory are removed from it as soon as reasonably practicable.

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 and, as they are often made widely available, there is no real need to hold these 'securely'.

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.

Do we need to have Data Sharing Agreements in place between different groups in our church who all hold their own lists of people attending?

You do not need Data Sharing Agreements in place as they are only recommended where data is being shared between different organisations (as Data Controllers). Unless all your church groups are going to register as separate Data Controllers (which they shouldn't unless they are separate organisations or charities) you do not need any such agreements in place.

How can we be sure that any cloud-based storage we use to store personal information is GDPR compliant?

Many of the major providers of these services will have published information about their terms and conditions and how they are GDPR-compliant. The church should look at these and consider what they might need to do to continue using these services in a compliant way.

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 Ts&Cs are accepted, Google does the rest. These arrangements should be provided for in the church’s policies.

How do we know that the US-based company we use to store/process our data provides ‘adequate’ protection?

The DP principle on this states that personal data should not be transferred outside the UK unless that country provides an ‘adequate’ level of protection for the processing of personal data. There is no definition of ‘adequate’ but it will depend on what that data is (which isn’t very helpful).

The UK has not yet made an adequacy decision regarding the US and so the Information Commissioner’s Office (ICO) would expect that Standard Contractual Clauses (SCCs) be included in any agreement between the church (as a data controller) and any organisation processing personal data on behalf of the church where that processing takes place in the US (this includes data storage). The church, as a data controller, has a duty to ensure that SCCs are applied to restricted international transfers of personal data to the US.

Thankfully, large multinational organisations are aware of international data protection requirements and typically they already have the SCCs in place. However, you should still check that the company/organisation is GDPR compliant by checking out their privacy policy, which will be on their website. For example, you can find information on Apple’s compliance with UK GDPR international data transfer requirements under the heading “Transfer of Personal Data Between Countries” on their website [here](#). Apple clearly does use SCCs in international data transfers, and this is the basis on which you can be confident that using iCloud data storage is GDPR compliant.

This guidance also applies when transferring personal data to any organisation that is based in a country not covered by an adequacy decision from the UK.

Is it acceptable for church staff and volunteers to use their own computers for processing personal information on behalf of the church?

GDPR does not prohibit the use of personal computers and email accounts as long as it is done with the approval of the data controller. What is important is that the church has clear policies in place about how data should be handled and what security measures need to be taken.

How can we provide Data Protection training for our ‘staff’ (including volunteers)?

- The L13 Guideline Leaflet has a page with some suggestions for training
- Our webinars are available from www.baptist.org.uk/GDPR which some may find helpful
- We have a PowerPoint (and a script) with some basic data protection training for church members available on our [Data Protection Documents](#) page.

Do we need to register with the ICO?

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

The quickest way to register with the ICO is online at www.ico.org.uk/for-organisations/register.

Alternatively, you can ring 0303 1123 1113

'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 (i.e. your church), or providing or administering activities for individuals who are members of the body or association (your church) or have regular contact with it
- you only hold information about individuals whose data you need to process for this exempt purpose (i.e. church members and those in regular contact with it)
- the personal data you process is restricted to personal information that is necessary for this exempt purpose only

What advice can you give 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 House Groups or internal church groups 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.

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.

Using the sample 'holiday club' privacy notice in our Privacy Statements leaflet you could put the information in paragraph 2 on the form and then say 'For more information about how we hold your data and your rights under Data Protection legislation please go to"

We use CCTV on our premises. What do we need to do?

The ICO have information about the use of CCTV (including a Code of Conduct) which can be found at [Video Surveillance | ICO](#)

If you do have CCTV then you will certainly need to be registered with the ICO.

Can you provide us with more information about obtaining consent – can we use tick boxes? How long does consent last? Is there an age limit?

Much of what we do in church life does not require the consent of individuals as we can use 'Legitimate Interest' as the legal grounds for processing.

You will need consent for 'Direct Marketing' of people who are not members or regular attenders and the advice we have received is that churches should also obtain consent where personal information is to be published in any way where it can be seen or accessed by people outside the church. This includes a published 'Church Directory' (or similar) as well as photographs or recordings of clearly recognisable people on a church's website or social media sites or in printed publicity.

Tick boxes: The best way to obtain consent is to use a form – paper or electronic – which people complete. Using tick-boxes are fine but what you should not use are 'pre-ticked' boxes or any other form of default consent.

Time limits: GDPR does not set a specific time limit for how long consent will last. This will depend on the "context, the scope of the original consent and the expectations of the data subject". However, the guidelines recommend that as best practice, consent should be refreshed at appropriate intervals in order to ensure that the data subject remains well informed about how their data is being used and their rights. You will need to interpret this for your own context.

Age of consent: Under GDPR the default age at which a person is no longer considered a child is 16. It is therefore our view that you should obtain specific consent from young people aged 16 and over to be included in a Church Directory (and not just included along with their parents) or to have their photographs published.

In the UK children aged 13 or over are able provide their own consent for **online services**. More information on gaining consent from children in this context can be found at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/>

Do we really have to get consent from everyone whose photograph we use on our website (or other social media sites) or in publicity?

Someone's photograph is part of their personal information and should be treated in the same way as other personal information. In our view it would be difficult to argue that it is in the church's legitimate interest to publish photos of easily identifiable individuals. Even if a church believes that this is possible, they should not be doing so in a way that could cause upset or offence to those whose pictures they want to use.

The reality is that there are some people who have very good reasons for not wanting their photograph published and we need to respect that.

There are no hard and fast rules on this but in our view churches should

- always gain specific consent when publishing photographs of named individuals (or of any children under 16)
- always seek to gain consent when publishing pictures of clearly identifiable unnamed individuals
- provide as much information as possible when taking pictures at services or events. Such information should explain what the photographs will be used for and give clear instructions as to what people should do if they do not wish their picture to be taken or used by the church.
- Provide a 'photo' free area of the worship area where people can sit if they do not wish to be photographed.

What data protection matters do we need to consider when we live stream or record and upload videos of services or events for use on our website?

A church should seek consent from any individuals appearing on screen (where they can be identified) for their involvement in the filming and the processing of their personal data through video footage. Records of these consents should be kept, in line with the church data retention policy. This should be straightforward when there are limited numbers of people involved who are clear on the purpose for which their data will be used in the service.

Where a church is planning to hold a service in the church with a congregation and broadcast it at the same time to a wider audience (either live or later) then this may involve processing images of the persons attending the service who might be filmed and identifiable from the footage. It would be disproportionate to obtain consent from everyone in the congregation for their personal data to be used in this way. The simplest way to achieve data protection compliance is to position cameras in such a way as to avoid capturing the images of those in the wider congregation. Where this is not possible, the church should make every effort to provide information about the filming to members and attendees in advance, which will enable those attending to decide to opt out if they wish or to sit in a designated area in the church

where they will not be filmed. Notices should be placed in a prominent place at the entrances, and you may also consider the newsletter/notice sheet/church website to explain that the service will be filmed. A reminder can also be given from the front at the start of the service. Particular care should be taken in relation to children or adults at risk, unless prior consent from them or their parents/guardians has been obtained. The church leaders can take the following steps:

- Create a clear delineation between the areas covered by the camera and those which are not.
- Ensure that attendees at church know that they may be caught on camera when sitting in the designated area and that by sitting in those areas they are consenting to being filmed.
- This can be made clear through posters around the church, on the church notices, or in a powerpoint slide playing before the service begins.
- When new people attend church those who are welcoming people at the door could take that opportunity to let them know about the livestreaming or filming of the service and which areas are or are not covered by the camera(s).
- ensure that those who do not consent to being filmed know where they should sit.

A privacy notice setting out exactly what information is being gathered, how this will be stored and how long for should also be readily available. This statement could be made available through a link on the church website or set out in the church notice sheet, if this is produced in paper form.

How does Brexit affect data protection?

When the post-Brexit transition period ended on 31 December 2020, the 'UK GDPR' replaced the existing 'EU GDPR' and together with the Data Protection Act 2018 now comprises the personal data protection legislation in the UK. All of the main principles, obligations and rights remain in place and this means that the way we process personal data largely stays the same, but the UK now has the independence to keep this framework under review. The Information Commissioner's Office (ICO) remains the UK's regulator for data protection law, but data protection decisions from the European Union (EU) no longer apply to the UK GDPR.

Transfers of personal data between the UK and the EU/EEA may continue without any additional safeguards, following the European Commission's adequacy decisions on data protection in the UK.

What do churches need to do now the transition period has ended?

Baptist churches do not need to make any new arrangements for transfers of personal data between the UK and the EU/EEA. Note that transfers of personal data to countries outside the UK/EU/EEA must continue to be assessed for appropriate safeguards such as Standard Contractual Clauses (SCCs). You can find out more about this at the ICO website [here](#).

You should review your privacy notices, Data Protection policy and other documentation to consider making changes to any references to EU law, and UK-EU transfers. We have updated both the template Data Protection Policy for churches and our Guideline Leaflet L13: Data Protection from February 2021.