Data Protection Guidance:
Data Subject Access Requests (DSARs)
May 2023

Introduction

Data Protection legislation gives individuals the right to obtain a copy of their personal data which organisations hold as well as other supplementary information (e.g. the source of that information and on what lawful basis it is being processed).

This helps individuals to understand how and why organisations are using their data and that they are doing so lawfully. Any individual can, therefore, ask your church about information you hold about them. They can ask you to confirm that you are holding personal information about them and ask you for a copy of what you hold. This is commonly referred to as a 'Data Subject Access Request' (DSAR) or 'Subject Access Request' (SAR).

Whilst is it is unusual for churches to receive such requests it should not be ruled out as a possibility. We assist a few churches every year with handling a DSAR and they often arise in connection with a grievance or investigation of some kind. Churches are therefore strongly advised to ensure that they have clear policies and procedures for dealing with all requests for information about personal data which they hold, and to have a data retention schedule, so that personal data which is not necessary to retain is deleted at the appropriate time. An example of a template data retention schedule can be found at www.baptist.org.uk/gdpr.

Getting Started

This document is intended to be a guide to creating your own policy so please use it in that way and adapt to your own situation as necessary. As a starting point you should identify the individuals within your church who would take responsibility for making sure the request is fulfilled. One of these would be the person who takes the lead for Data Protection matters in your church, but you do need another one or two people so that it is not left to one person to make all the decisions. Having a second person will also mean that any such requests would still be actioned even when the main person is on holiday or ill. In these notes we refer to 'DP Team' for these people – your policy though should use whatever term you choose.

You should make sure that the DP Team read the very helpful material on this subject produced by the Information Commissioner's Office (ICO), including a guide to the right of access which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/, and further detailed guidance on the right of access which can be found at 'Right of access | ICO'. There is also a section in our L13 Guideline leaflet on this subject (section 8) which can be found at www.baptist.org.uk/resources/L13.

Please note that whilst the BUGB Data Protection Team is willing to advise any BUGB member church which receives a Subject Access Request, we cannot respond to a DSAR for you and formal legal advice should be sought in all cases where there is uncertainty regarding the information to be provided to the requester, especially if it contains highly sensitive personal data such as criminal offence data, information relating to a safeguarding matter, or where the requester's personal data is inextricably intertwined with the personal data of a third party.

The BUGB Data Protection Team can be contacted by emailing dataprotection@baptist.org.uk.

Suggested Process and Policies for dealing with DSARs

1. **Log the DSAR**
   - DP Team agrees that this is a DSAR, logs it as such and notes the date by which the information must be provided (or a time extension notified to the requester)
   - SEE NOTES (i) and (ii) below for information about response times.

2. **Acknowledge request and confirm identity**

- If there is any reasonable doubt as to the identity of the requester then this should be verified before any personal data is disclosed.
- Evidence of legal authority to act on behalf of the data subject will be required when a request is made on behalf of someone else.
- SEE NOTES (iii) and (iv) below for information about 'legal authority' and dealing with requests from children.

3. **Clarify what is needed**
   - Depending on the request you may need to contact the requester to clarify if they are only looking for data which relates to a specific issue, is for a specific timeframe or held in a specific way. This particularly applies if you process a large amount of information about an individual e.g. a minister who has served in your church for many years.
   - If you process a large amount of information and need the requester to specify the information or processing activities their request relates to, the time limit for responding to the request is paused until you receive clarification. This means that you do not need to provide the individual with a copy of the information or supplementary information that you cannot reasonably provide unless the request has been clarified.
   - Clarification should not, however, be sought on a blanket basis but only if it is genuinely required in order to respond to a DSAR and you process a large amount of the requester's personal data.

4. **Assess the information held**
   - The DP Team will need to look at what information is held about the data subject, where it is stored and how this can be identified and provided to the person making the request.

5. **Decide if there is information which doesn't need to be provided**
   - You do **not** have to disclose everything you hold which relates to the data subject. There are a number of exceptions, such as confidential references and documents which also relate to another person (third party data) and these should be considered on a case-by-case basis.
   - Please see information in the box on page 4 and the flow-chart on page 5.
   - If you are unclear about whether something should be included or not please contact the BUGB Data Protection Team or obtain your own legal advice.
   - A DSAR is not an opportunity for an individual to carry out a "fishing exercise" to find out other information they may be interested in. It is important to remember the scope of the exercise – namely to provide an individual with a copy of their personal data, and how and why you are holding it.

6. **Assess whether a fee should be charged**
   - In most cases you cannot charge a fee to comply with an DSAR but where the request is "manifestly unfounded or excessive" you may charge a "reasonable fee" for the administrative costs of complying with the request. You can find a definition of excessive and unfounded requests and information on what you can charge for them at 'Right of access | ICO' but be aware that you will need to be able to justify any charge you make if challenged.
   - You can also charge a "reasonable fee" if the individual requests further copies of their data.
   - SEE NOTE (v) for information about response times when you charge a fee.

7. **Prepare the information to be provided**
   - This will involve compiling and reviewing the information as well as any redactions of third-party data which need to take place.
   - The requester should only be provided with a copy of their personal data that is within a document; they are not automatically entitled to see other information within the same document that is not about them.
   - It is imperative that you use a method of redaction that ensures all of the information to be redacted has been properly removed. If done using redaction software on a PDF document, please ensure that any hidden text or metadata is removed or 'sanitised' and that the redacted document is saved as a new file. **It is not sufficient to highlight or blackout text in Microsoft Word, and to then save the document as a PDF**. This method can easily be undone using PDF editing software. We can provide advice about suitable redacting tools.
   - Sometimes it may be easier to lift the requester's personal data out of a document into a separate document that you can disclose.

- SEE NOTE (vi) below for information on how the information should be provided to the requester.

8. **Send the information to the requester**
   - This must happen within one calendar month of the request being received unless an extension is sought and has been communicated to the person making the request within the one-month period.

NOTES

(i) The request must be responded to within one calendar month. This is calculated from the day you receive the request or other requested information (whether this is a working day or not) and the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. (For example, if you receive a DSAR on the 30 January you have to respond by 28 February). If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

(ii) The response time can be extended by a further two months if the request is complex or you have received a number of requests from the individual. If you need to do this, you will need to let the individual know within one month of receiving their request and explain why the extension is necessary.

(iii) Evidence of legal authority to act on behalf of an adult can include an original signed letter of authority from the data subject (where they possess full mental capacity) or an original (or certified copy) of a relevant Power of Attorney or Court of Protection Deputyship Order (where the data subject lacks mental capacity)

(iv) Children can also make DSARs and the ICO guidance referred to earlier has a section about how to deal with requests from children.

(v) If you choose to charge a fee, you do not need to comply with the request until you have received the fee. However, you should request the fee promptly and at the latest within one month of receiving the DSAR.

(vi) If an individual makes a request electronically, then we are expected to provide the information in a "commonly used electronic format", unless the individual requests otherwise.

Information you do not have to provide

REFERENCES

Confidential references (given or received) in respect of prospective or actual education, training, employment, volunteering, appointment to office of an individual or provision of a service by an individual are EXEMPT from disclosure under an DSAR.

THIRD PARTY INFORMATION

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

However, the Data Protection Act 2018 says that organisations do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

To help you decide whether to disclose information relating to a third party, you can follow the process in the flow-chart provided below.

In determining whether it is reasonable to disclose the information, you must, however, take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

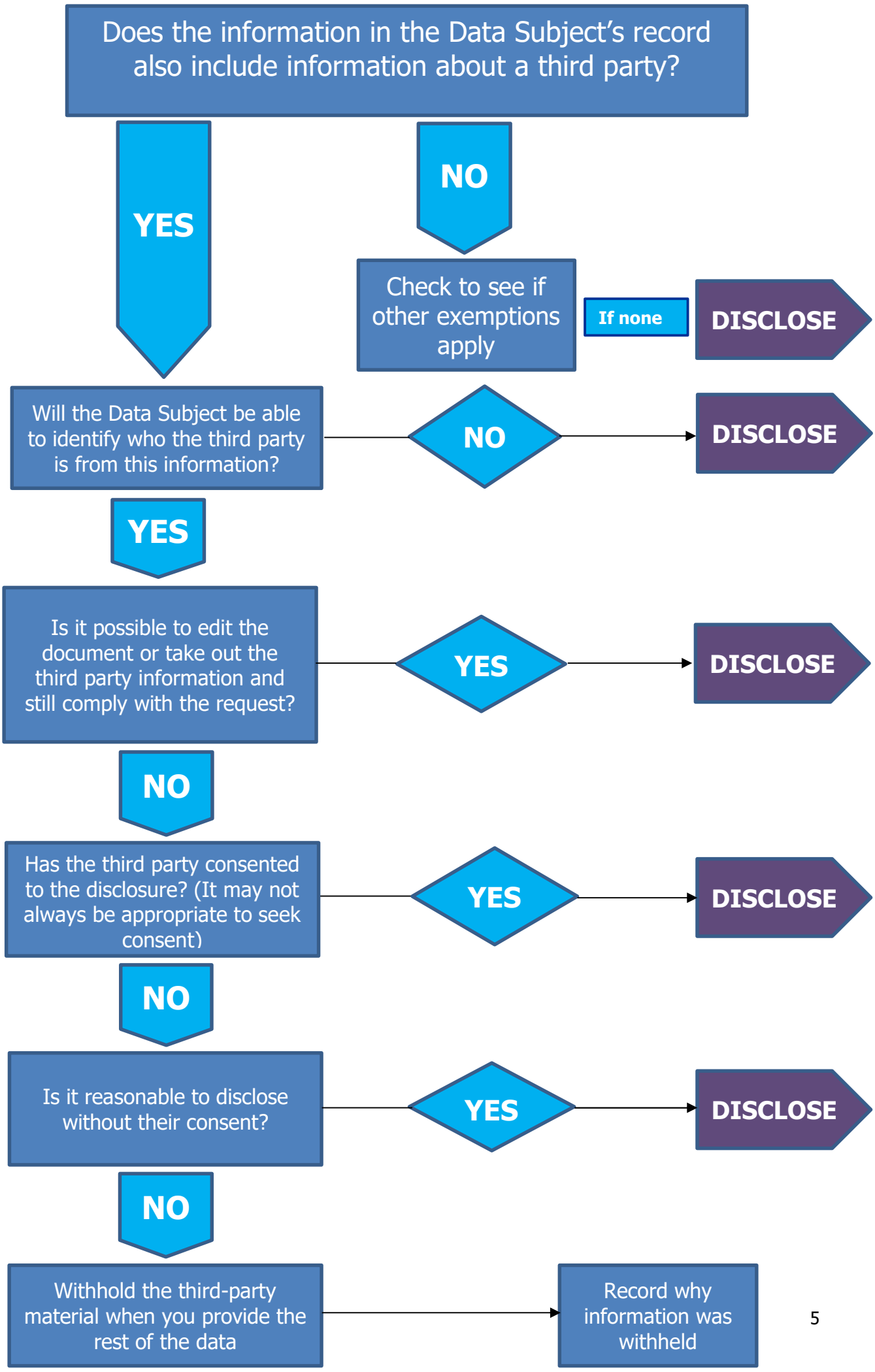
For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

More information is available from the ICO website here.

OTHER EXEMPTIONS

There are other exemptions (most of which are unlikely to apply to churches) e.g. legal professional privilege, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/ and 'What other exemptions are there? | ICO'.

Legal advice should be sought when it is thought that another exemption may be applicable.


Does the information in the Data Subject's record also include information about a third party?
YES
NO
Check to see if other exemptions apply
If none
DISCLOSE
Will the Data Subject be able to identify who the third party is from this information?
NO
DISCLOSE
YES
Is it possible to edit the document or take out the third party information and still comply with the request?
YES
DISCLOSE
NO
Has the third party consented to the disclosure? (It may not always be appropriate to seek consent)
YES
DISCLOSE
NO
Is it reasonable to disclose without their consent?
YES
DISCLOSE
NO
Withhold the third-party material when you provide the rest of the data
Record why information was withheld