Complying with a Subject Access Request

information commissioner
Barrantagh Fysseree

The contents of this guidance note are set out below.

Contents

Your Legal Responsibility

If you are a controller, it is your legal obligation to "facilitate the exercise of data subjects rights", including the right of access to personal data.

The right of access is exercised by making a request, usually known as a 'Subject Access Request' ("SAR"). This right allows people to find out what "personal data" about them is being processed by a controller; this may lead to the exercise of further rights.

Consequences of failing to comply with a subject access request

Failure to comply with a SAR could mean that the individual:

- takes the matter to Court which may result in the Court ordering steps to secure compliance with the SAR. Failure to comply with a Court order may be treated as contempt; and/or
- makes a claim for compensation; and/or
- makes a complaint to the Commissioner. The Commissioner has powers of investigation which can be used to enquire into the matter. Corrective powers can be used to rectify any failure to comply with a SAR and these include reprimands, enforcement notices and financial penalties of up to £1,000,000.

It is also an **offence** for a controller, or a person employed by the controller, to alter, deface, block, erase, destroy or conceal information sought by data subject exercising their right of access which the data subject would have been entitled to receive.

This is a recordable offence and a person committing this offence is liable to a fine of up to £10,000 and/or imprisonment for a term of up to 6 months.

What law gives this right and governs how we respond?

Article 15 of the Applied GDPR provides this right to individuals and, together with Article 12, sets out the requirements and obligations on controllers when complying with a SAR. Controllers should record the actions they take when dealing with SARs as this may be required by the Commissioner should a complaint be made. Where a data protection officer (DPO) has been designated under Article 37 of the Applied GDPR, the contact details for that DPO must be made available via transparency information. Data subjects may, under Article 38(4) of the Applied GDPR, contact the DPO with regard to the exercise of their rights.

In order to respond to a SAR it is important that the terms in the law are understood and information about the definitions can be found on the website at: https://www.inforights.im/information-centre/data-protection-law-2018/definitions/

The Commissioner cannot give you case-specific advice and this guidance note is intended to help you comply with your responsibility. Other related guidance is available on the website.

This guidance does not constitute legal advice.
If you require legal advice, you should contact a Manx Advocate.

Technicalities of subject access requests

Who can make a SAR?

The right of access can only be exercised by, or on behalf of, a data subject.

A data subject is an *"identified or identifiable natural person 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

Although a SAR is normally made by data subjects, third parties may make requests on their behalf, for example:

- A parent, or guardian, who has joint, or sole, parental responsibility can make a request on behalf of their child - this is dependent upon the age and maturity of the child.

- A legal representative acting on behalf of the person

The controller is responsible for ensuring that a third party is entitled to make a SAR for, and be supplied with, the personal data of another person.

If personal data is disclosed in response to a SAR to someone who is not entitled to receive it, the controller will contravene the principles and the data subject may take remedial action, including making a complaint to the Commissioner (who may exercise corrective powers including reprimands, financial penalties etc.) or seeking compensation through the courts.

What will a SAR look like?

There is no standard format. SARs can be made **verbally or in writing**, including via electronic means. Although controllers may produce SAR forms, individuals cannot be obliged to complete a form, nor can controllers make responding to a SAR conditional on completion of that form.

There is no requirement for the SAR to refer to the data protection law and may be worded in different ways, and could be as simple as 'Please provide me with copies of all the information you hold about me'.

- ❖ It is important that staff are able to recognise that a SAR is being made.
- ❖ If a request is made verbally, records of that verbal request should be maintained to provide a clear trail of correspondence.

Can I charge a fee for responding to a SAR?

No – Fees cannot generally be charged.
See more at: https://www.inforights.im/information-centre/data-protection-law-2018/rights/

Can I ask for some form of identification?

Whether you need any form of identification will depend on the relationship between the controller and the data subject. For example, if the data subject is a member of staff, or is known to the controller, there should be no need to seek further identification, but where the controller has no previous connection with the data subject, some form of identification may be required.

The basic requirements are full name and address (and previous address if the SAR covers a long period of time). If necessary, date of birth may be sought, for example if it is a common name or more than one person may live at an address with the same name.

If you do not know the data subject, for example, they are not a member of staff, or someone you have had regular dealings with, reference numbers or identifiers specific to the controller such as account number or client number, can assist in identifying the person accurately.

If the above information is insufficient to identify the data subject and you have reasonable doubts about their identity you must act **reasonably** in seeking further information to identify them.

Identifying information will itself be personal data which must be obtained and processed in compliance with the principles. In particular, it should be adequate, relevant and the minimum necessary for the purpose of identifying the data subject and the personal data they are seeking.

- Controllers are accountable for, and must be able to demonstrate, compliance with the principles.

In the majority of circumstances, the routine requesting of copies of photographic ID, and copies of multiple documents, such as utility bills etc., particularly if you do not already have any information against which this can be verified, would be beyond the 'minimum necessary'. The controller may need to justify why such identifying information was necessary in the circumstances.

It is equally important to ensure that the personal data supplied in response to the request is provided to the correct data subject.

It may be appropriate to ask the person collecting the information to provide suitable identification at the point of collection (recording what was provided but only retaining a copy if necessary), particularly if the personal data supplied in response to the SAR is sensitive, for example, medical, social care, or police records.

- A controller must act on the request unless it can **demonstrate** that it is not in a position to identify the data subject.

What can be sought under a SAR?

Information constituting the "personal data" of the data subject can be sought under a SAR, but it is not a right to copies of documents. Personal data is defined as "any information relating to an

identified or identifiable natural person". More information about what constitutes "personal data" can be found on the website.

A data subject is not obliged to tell you why they are making the request, or to specify what they are seeking. Many people make requests because they DON'T know what personal data you have about them and are trying to find out.

Equally, they may be seeking particular personal data and specify what they want, for example by event, time or date.

What if the request does not make it clear what information is required?

Contact the data subject. If there is any doubt as to what personal data the data subject requires, it is best to speak with them to clarify the matter. Checking with them may save a lot of time and effort.

This will make sure **the controller** is looking for the right personal data and **the data subject** will receive what they really want. The data subject may refine their request as a result, or still want "all personal data".

You cannot, however, reasonably expect a data subject to know how your filing systems work, where the information is stored, or who may have sent emails or correspondence they are requesting. Such information should not therefore be sought and failure to provide it cannot be used as an excuse for not complying with the SAR.

Is there any information that cannot be released?

Yes - in some cases there are restrictions on the right of access (i.e. Article 15 of the Applied GDPR) and those restrictions are set out in Schedule 9 of the Implementing Regulations.

However, the restrictions can only be applied in particular circumstances, to certain personal data, and sometimes only by specified controllers. These are not 'bans' on providing a data subject with their personal data, nor from providing as much personal data as possible that does not fall within the scope of the particular restriction.

If a restriction does apply, the controller can choose to apply that restriction and refuse the data subject access to particular personal data.

- A decision about whether a restriction applies cannot realistically be made until the information has been collated and the relevant personal data within the information identified.

- Controllers should justify and document the reasons for applying a specified restriction on access to particular personal data in order to demonstrate compliance with the law. Should a complaint be made to the Commissioner, it is likely that the information justifying the application of a restriction would be requested from the controller.

More information about restrictions, including a **summary of all restrictions on rights** set out in the law, is available on the website.

How long have I got to respond to a SAR?
To comply with the law you must provide the personal data requested **promptly** and in any event **within a calendar month**.

It will be a matter of fact as to whether the request was, or was not complied with 'promptly'. If the personal data is readily available, for example a personnel file, then there would be no reason to delay supplying the information to the person.

If you find that no personal data is being processed, you must still communicate this outcome to the data subject within a calendar month.

Can the response time be extended?
The time can only be extended in restricted circumstances. Article 12(3) of the Applied GDPR permits an extension of up to two further calendar months if necessary when a SAR is particularly complex.

However, the controller **must advise** the data subject that it is extending the time period **within the calendar month** and fully explain the reasons for the delay.

- ❖ It is the responsibility of the controller to be able to be accountable for, and be able to demonstrate, compliance with the law. Proper records evidencing why it was necessary to extend the period for compliance must be maintained.

How do I provide the response?
If a SAR is made by electronic means, the information shall be provided to the data subject by electronic means, wherever possible, unless the data subject requests otherwise. In other cases, it is suggested that you communicate with the data subject about the means by which the informationis to be provided.

What must be included in the response?

If the personal data sought is being processed, you must provide **a copy of that personal data** and details about:

- The purposes for processing
- The categories of personal data processed
- Recipients of classes of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries
- The envisaged period for which the personal data will be stored where possible, or , if not possible, the criteria used to determine that period
- The source of the data (if available) if they were not obtained directly from the data subject

- Details of any automated processing or profiling and the logic involved
- Details of the appropriate safeguards (Applied GDPR, article 46) relating to transfers of personal data to any third country
- The existence of the rights to rectification, erasure and restriction of, and/or objection to, processing
- The right to lodge a complaint with the Commissioner

Most of this information should be **recorded in some way by the controller**, for example in mandatory records of processing activities or other records maintained about the processing. This is part of accountability for, and governance of, the processing.

There is no exemption from providing those details even if the controller has not made such a formal/informal record. To comply with the right of access, the controller should determine the above points and provide the information to the data subject. No extension to the compliance period is provided for in such circumstances.

FAQs

They have previously made a SAR – do we have to do it again?
Not necessarily.

If a request is **manifestly unfounded or excessive**, in particular because of its repetitive character, the controller can either charge a reasonable fee for complying with the request (limited to the administrative costs incurred) or refuse to act on the request.

The controller must:

- ❖ inform the data subject without delay and within one month if it is **not going to act** on the request;
- ❖ be able to demonstrate why the request was manifestly unfounded or excessive.

Failure to do the above will contravene Article 12 of the Applied GDPR and may lead to remedial action be taken by the data subject, including the making of a complaint to the Commissioner.

There is information about other people mixed in with the data subject's personal data
The fact that third party personal data is included does not preclude the disclosure of the data subject's personal data to them, but the restriction in paragraph 8 of Schedule 9 to the Implementing Regulations describes the considerations that must be given in such circumstances.

- ❖ Controllers should record their decisions about disclosure.

I think the person is asking for this information to progress a legal action – do I still have to comply with the request?

Yes – A data subject is not obliged to tell you why they are making a request, nor what they intend to do with the personal data they receive. The fundamental right of access is not affected by any prospective, or ongoing, legal action, including employment tribunals etc.

The right of access is sometimes exercised by the data subject's legal representative as an alternative to the legal discovery/disclosure process when legal action is being considered, or is in progress.

However, there are significant differences between the right of access and the legal discovery/disclosure process and the information you are required to provide. The advice of an Advocate should be sought if you are in any doubt as to the appropriate method of dealing with a request for information, other than personal data, in these circumstances.

The file contains medical records, what should I do?

Medical records should not be disclosed unless the controller is a health professional or has consulted with the appropriate health professional to determine whether the personal data can be disclosed.

If the appropriate health professional is of the opinion that the release of the details is likely to cause serious physical or mental harm to the data subject or any other person, they need not be disclosed. Appropriate records of the decision must be maintained.

There are some unpleasant comments on the file about the person; do I have to include these?

Yes – You may not omit details just because they are unpleasant or even defamatory. This could amount to an offence under Regulation 128 of the Implementing Regulations 2018. (see: **Your Legal Responsibility**)

The request is for CCTV footage

You should ask the data subject to provide an up-to-date photograph of themselves against which images can be compared and details about where they were and an approximate time to help you locate the information they require.

In most cases, unless the CCTV system and software is sufficiently sophisticated to use facial recognition techniques, images cannot be located without human intervention in reviewing the footage. If the data subject cannot provide a reasonable timeframe, location and comparative image, the request may be excessive and the controller may refuse to act on the request of charge a reasonable fee based on administrative costs.

Can the Commissioner tell me whether we can apply a restriction?

No – Whilst the Commissioner makes general guidance available on the website, the controller must make and record that decision. The main obligation is to provide the personal data - if there is any doubt whether the right should be restricted, then the controller can seek legal advice as necessary.

How to determine which information to disclose

Start the search

Searches should be made of all the relevant servers, drives, email systems, databases and manual systems to collate information which may contain the personal data sought. Search parameters used can include, but are not limited to, variations of the name, pseudonyms, account number or other identifier.

Search completed, information collated – the next steps

1. **Identify the personal information**

The first decision to make once the searches are completed and you have gathered all the information together, is what information constitutes the "personal data" of the data subject making the SAR. If it is **not** "personal data", the right of access does not apply to that information.

2. **Is there information within that personal data that identifies a third party?**

Please see Appendix 2 for guidance on dealing with third party information and our advice note, "Subject access requests – Dealing with third party information".

3. **Are there any restrictions on the right of access that apply?**

Restrictions are not mandatory, nor are there any blanket restrictions on the right of access. Even when a restriction may reasonably be relied on, it will only apply to certain personal data. Any personal data, to which a restriction does not apply, must still be provided.

Details about the restrictions are available on the website: https://www.inforights.im/information-centre/data-protection-law-2018/rights/restrictions-on-rights/

Supply the personal information to the individual making the request

The right of access is not a right to copies of documents that contain personal data. You may, of course, provide the individual with a copy of the document if you wish, but you may also, for example, copy and paste the personal data contained within documents, emails etc, into a new document, or if a request has been made for a recording of a telephone call, transcribe the call. Both of these will satisfy the requirement to provide a copy of the personal data.

- Where the SAR has been made electronically, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic format.

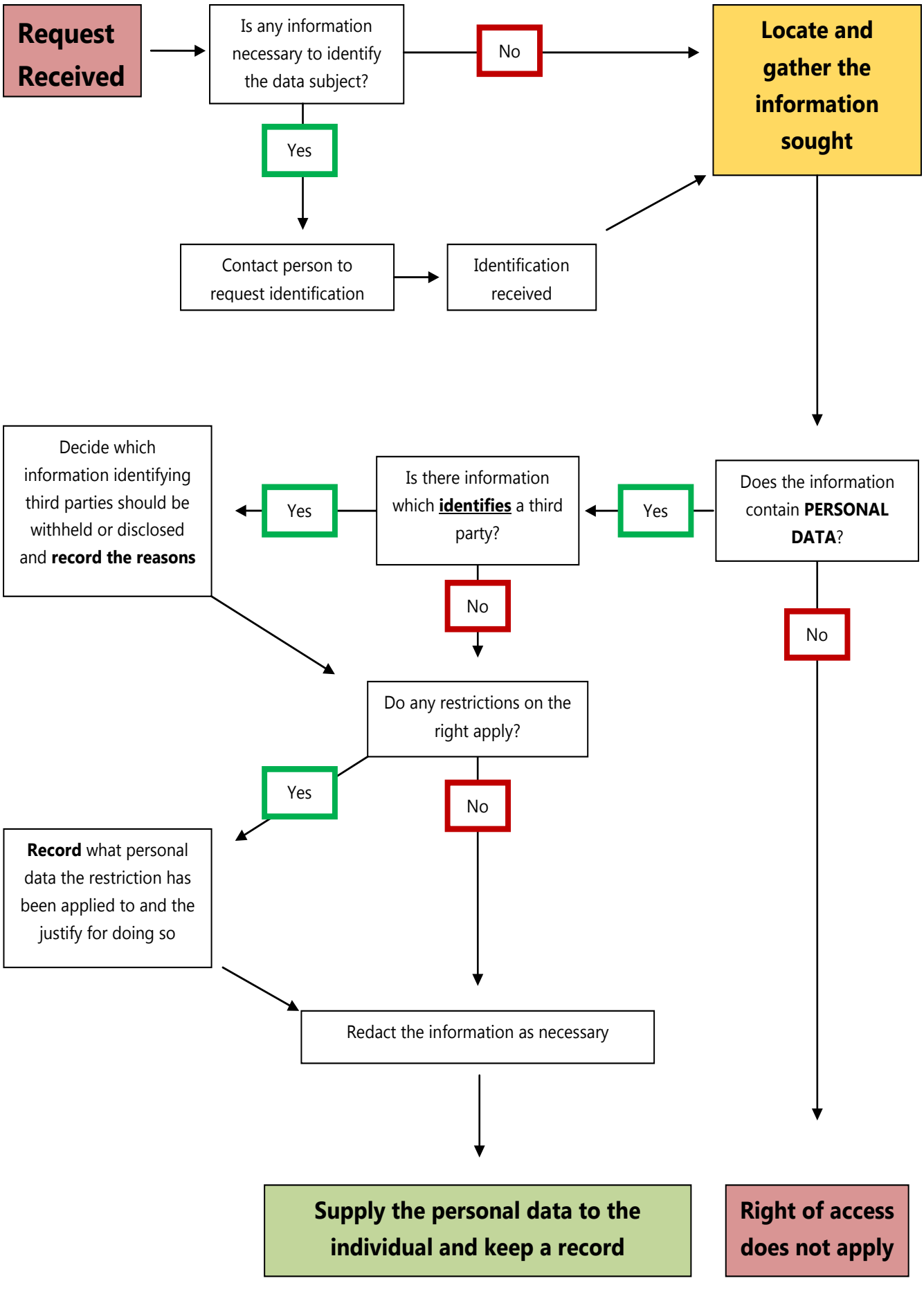
Before supplying the *personal information* –

Check:

- Is it all "personal data"?
- Does it all relate specifically to the data subject?
- Is there any information identifying third parties that should be withheld/redacted?
- Are the files marked to show this data has been supplied under a SAR?
- Is there a copy of the details in case they get lost in transit, or are queried?
- If a copy is kept, where, and for how long, should it be stored?

Send/supply the personal data to the data subject together with the other information specified in ***"What must be included in the response?"***

Appendix 1 – example of procedure



APPENDIX 2 – suggested approach to third party information

Responding to a SAR may involve providing information that relates to both the requester and another individual. The rules about third-party information described here, apply only to personal data that includes information about the individual who is the subject of the request and information about someone else.

Example

> An employee makes a request to her employer for a copy of her human resources file. The file contains information identifying managers and colleagues who have contributed to (or are discussed in) that file. This will require you to reconcile the requesting employee's right of access with the third parties' rights in respect of their own personal data.

The law says you do not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information.

BUT this does not excuse a controller from communicating as much of the information sought by the request as possible without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars.

For the avoidance of doubt, you cannot refuse to provide personal data about an individual just because it includes some third-party information, or simply because you obtained that data from a third party.

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 in respect of their own personal data.

You should make decisions about disclosing third-party information on a case-by-case basis. You must not apply a blanket policy of withholding it.

The DPA expects controllers to have regard to the following:

- has the other individual consented to the disclosure? or
- is it reasonable in all the circumstances to comply with the request without that individual's consent?

If the other person consents to you disclosing the information about them, it may be disclosed to the requester. However, if there is no consent, you must decide whether it is reasonable to disclose the information anyway.

Suggested approach to dealing with information about third parties

Does the request require the disclosure of information that identifies a third party?
You should consider whether it is possible to comply with the request without revealing information that relates to and identifies a third-party individual. In doing so, you should take into account the information you are disclosing and any information you reasonably believe the person making the request may have, or may get hold of, that would identify the third-party individual.

Example

> In the previous example about a request for an employee's human resources file, even if a particular manager is only referred to by their job title it is likely they will still be identifiable based on information already known to the employee making the request.

As your obligation is to provide information rather than documents, you may delete names or edit documents if the third-party information does not form part of the requested information.

However, if it is impossible to separate the third-party information from that requested and still comply with the request, you need to take account of the following considerations.

Has the third-party individual consented?
In practice, the clearest basis for justifying the disclosure of third party information in response to a SAR is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a SAR.

However, you are not obliged to try to get consent and in some circumstances it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. Indeed, it may not always be appropriate to try to get consent, for instance, if to do so would inevitably involve a disclosure of personal data about the requester to the third party.

Would it be reasonable in all the circumstances to disclose without consent?
In practice, it may sometimes be difficult to get third-party consent, e.g. the third party might refuse consent or might be difficult to find. If so, you must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway.

The law provides a **non-exhaustive** list of factors to be taken into account when making this decision. These are set out in paragraph 8 of Schedule 9 to the Implementing Regulations 2018 and include:

- any duty of confidentiality owed to the third-party individual;
- any steps you have taken to try to get the third-party individual's consent;
- whether the third-party individual is capable of giving consent;
  and
- any stated refusal of consent by the third-party individual.

Confidentiality

Confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third party without their consent.

A "duty of confidence" arises where information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to you with the expectation it will remain confidential. This expectation might result from the relationship between the parties.

For example, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and patient)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

However, you should not always assume confidentiality. For example, a duty of confidence does not arise merely because a letter is marked 'confidential' (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.

In most cases where a duty of confidence does exist, it will usually be reasonable to withhold third-party information unless you have the third-party individual's consent to disclose it.

Other relevant factors

In addition to the factors listed in the law, the following points are likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

Information generally known by the individual making the request.

If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely to be reasonable for you to disclose that information.

It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual.

Circumstances relating to the individual making the request.

The importance of the fundamental right of the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life.

Health, educational and social work records.

There are special rules governing subject access to health, educational and social-work records. In practice, these rules mean that relevant information about health, education or social work professionals (acting in their professional capacities) should usually be disclosed in response to a SAR. These are set out in paragraphs 25 – 29 of Schedule 9 to the Implementing Regulations 2018.

Responding to the SAR

Whether you decide to disclose information about a third party in response to a SAR or to withhold it, you will need to respond to the requester. If the third party has given their consent to disclosure of information about them or if you are satisfied that it is reasonable in all the circumstances to disclose it without consent, you should provide the information in the same way as any other information provided in response to the SAR.

If you have not got the consent of the third party and you are not satisfied that it would be reasonable in all the circumstances to disclose the third-party information, it may be withheld.

However, you are still obliged to communicate as much of the information requested as you can without disclosing the third-party individual's identity. Depending on the circumstances, it may be possible to provide some information, having edited or 'redacted' it to remove information that would identify the third-party individual.

- You must be able to justify your decision to disclose or withhold information about a third party, so it is good practice to keep a record of what you decide, and why. For example, it would be sensible to note why you chose not to seek consent or why it was inappropriate to do so in the circumstances.

Appendix 3 - Good Practice Recommendations

- Respond to the person as soon as you receive the SAR either advising that the request is being undertaken or to request information to identify the person if necessary.

- Communicate with the person to assist you in identifying the information they actually want.

- Comply as quickly as possible; do not use the maximum time allowed as your target date for completion.

- Ensure that you maintain an audit trail; keep a record of dates for commencement, completion, details of correspondence sent and received, thought processes and reasons for non-disclosure etc.

- Mark the files that you copy to denote that a SAR has been complied with.

- Maintain a separate file for SARs received by the controller; this should contain the correspondence, a copy of the information sent and the audit trail documenting the handling of the request.

- *It is important to maintain records about compliance with Subject Access Requests. If you fail to respond to a SAR the person can make a complaint to the Commissioner and such records are likely to be required by the Commissioner to investigate the complaint.*