Right of access

1.0.87 | 8 December 2025

Right of access

About this detailed guidance

This guidance discusses the right of access in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you apply the right of access in practice. It is aimed at data protection officers (DPOs) and those with specific data protection responsibilities in larger organisations. This guidance does not specifically cover the right of access under parts 3 and 4 of the Data Protection Act 2018 (DPA). However, some of the guidance contains practical examples and advice which will still be relevant. Please also refer to our separate guidance on the right of access – part 3 of the DPA 2018 and on intelligence services processing – the right of access.

If you haven't yet read the 'in brief' page on the right of access in the Guide to Data Protection, you should read that first. It introduces this topic and sets out the key points you need to know, along with practical checklists to help you comply.

To help you to understand the law and good practice as clearly as possible, this guidance says what organisations **must**, **should**, and **could** do to comply.

Legislative or legal requirements

Must refers to:

- legislative requirements within the ICO's remit; or
- established case law (for the laws that we regulate) that is binding.

Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. We expect you to do this unless there is a good reason not to. If you choose to take a different approach, you need to be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example that you may consider to help you to comply effectively. There are likely to be various other ways for you

to comply. This approach only applies where indicated in our guidance. We will update other guidance in due course.

Contents

What is the right of access?

In more detail

What is the right of access and why is it important?

The right of access, commonly referred to as subject access, gives people the right to obtain a copy of their personal information from you, as well as other supplementary information.

It is a fundamental right for people. It helps them understand how and why you are using their information and check that you are doing it lawfully.

What is a person entitled to?

People have the right to obtain the following from an organisation:

- Confirmation that you are processing their personal information.
- A copy of their personal information.
- Other supplementary information.

In most cases, you can confirm whether you are processing a person's personal information in general terms. However, this will depend on the nature of the request. If the request is for a specific piece of information, you **must** confirm or deny whether you are processing this information unless an exemption applies. This may be relevant if confirming that you hold the information would prejudice or undermine the purpose of the exemption. For example, telling someone information has been withheld because it would prejudice a criminal investigation might undermine the investigation. For further details about when this can apply, see What are exemptions and how do they work?

You may also be able to apply an exemption to the duty to provide supplementary information. For an example of how this works in practice, see Does this exemption apply to supplementary information?

What other information is a person entitled to?

People have the right to receive the following supplementary information:

- Your purposes for processing their information.
- The categories of personal information you're processing.
- The identities of specific recipients you have or will be disclosing the personal information to (including those in countries or territories outside the UK, or in international organisations), except where it would be impossible or manifestly unfounded or excessive to provide this information. In these circumstances, you **must** provide the categories of recipients instead.
- How long you will keep their personal information for – or, where this is not possible, the criteria for deciding how long you will store it.
- Their right to request rectification, erasure or restriction, or to object to processing.
- Their right to make a complaint to the controller.
- Their right to make a complaint to the ICO.
- Information about the source of their personal information, if you did not obtain it directly from them.
- Whether or not you use automated decision-making (including profiling), meaningful information about the logic involved in the processing, and the significance and envisaged consequences of the processing for the person.
- The appropriate safeguards you apply if you have transferred or will transfer personal information to a third country or international organisation.

This mostly matches the information you **must** provide in your privacy information.

When responding to a SAR, you **must** supply this supplementary information in addition to a copy of the requested personal information itself. You **could** include a link to this information in your response or when you acknowledge receipt of the SAR. See our guidance on the right to be informed for further information.

Are people only entitled to their own personal information?

The right of access allows people to access their own personal information. They are not entitled to information about other people, unless:

- their personal information also relates to other people (see What if a SAR involves information about other people?); or
- they are exercising another person's right of access on their behalf (see Can a request be made on behalf of someone else?).

Before you can respond to a SAR, you **should** decide whether the information you hold is personal information and, if so, whom it relates to.

Information is personal information if it relates to a living person who is identifiable from that information (directly or indirectly). The context in which you hold information, and the ways you use it, can influence whether it relates to a person.

Some information may be the personal information of two (or more) people. You can consider applying an exemption, if responding to a SAR involves providing information that relates to both the person making the request and another person. See What if a SAR involves information about other people? for more information.

In most cases, it will be obvious if the requested information is personal information. If you're unsure, please read our guidance on personal information to help you decide.

Who is responsible for responding to a request?

Controllers are responsible for complying with SARs. If you use a processor, you **must** have a contractual agreement in place to make sure that you can deal with SARs properly, whether they are sent to you or the processor. The processor **must** help you meet your SAR obligations. You **must** make this clear in your agreement. Read our guidance on contracts and liabilities between controllers and processors for more information.

The processor may hold personal information on your behalf. If so, your controller-processor agreement **must** allow you to obtain the necessary information from the processor to respond to a SAR. You are responsible for deciding how to deal with SARs.

If you are a joint controller, you **must** have a transparent arrangement in place with the other joint controller(s) which sets out how you will deal with SARs. You **could** choose to specify a central point of contact. However, people **must** still be able to exercise their rights against each controller.

If you are unsure whether you are a controller, joint controller or processor, read our guidance on controllers and processors.

Example

An employer is reviewing staffing and pay, which involves collecting information about a representative sample of staff. A third-party processor is analysing the information.

The employer receives a SAR from a member of staff. The employer needs information held by the processor to respond. The employer is the controller for this information and instructs the processor to retrieve any personal information that relates to the member of staff.

Relevant provisions in the UK GDPR - see Articles 4(1), 4(7), 4(8), 15, 26, 28 and Recitals 30, 63, 79, 81

http://www.legislation.gov.uk/eur/2016/679/contents

Further reading

- What is personal information: a guide
- Right to be informed
- Controllers and processors
- Contracts and liabilities between controllers and processors

How can we prepare for a subject access request (SAR)?

In more detail

Why is it important to prepare for the right of access?

It's important to be prepared and take a proactive approach to SARs, as this helps you respond to them more effectively and quickly. It also helps you:

- comply with your legal obligations under the UK GDPR and DPA and show how you have done so;
- streamline your processes for dealing with SARs, saving you time and effort;
- increase levels of trust and confidence in your organisation by being open with people about the personal information you hold about them;
- enable people to check that the information you hold about them is accurate, and to tell you if it's not;
- improve confidence in your information handling practices; and
- increase the transparency of what you do with personal information.

What steps should we take?

There are various ways that you can prepare for SARs. What is appropriate for your organisation depends on multiple factors, including the:

- types of personal information you hold and are using;
- number of SARs you receive; and
- size and resources of your organisation.

The following list is not exhaustive, but includes examples of ways that you can prepare:

- **Awareness** — You **could** make information available about how people can make a SAR (e.g. on your website, in leaflets or in your privacy notice).

- **Training** — You **should** provide general training to all staff to help them recognise a SAR. Provide more detailed training on handling SARs to relevant staff, dependent on their job role. If you are required to have a DPO, they are responsible for ensuring your organisation provides appropriate data protection training to staff.
- **Guidance** — You **could** create a dedicated data protection page for staff on your intranet with links to SAR policies and procedures.
- **Request handling staff** — You **should** appoint a specific person or central team that is responsible for responding to requests. Where possible, you **should** ensure that more than one member of staff knows how to deal with a SAR so you have a contingency if someone is absent.
- **Asset registers** — You **should** maintain information asset registers that show where and how you store personal information. This will help you locate the required information to respond to SARs.
- **Checklists** — You **could** produce a standard checklist that staff can use to ensure you take a consistent approach to SARs.
- **Logs** — You **could** maintain a log of SARs you have received and update it to monitor progress. It **could** include copies of information you supply in response to each SAR, as well as copies of any material you've withheld and the reasons why.
- **Retention and deletion policies** — You **should** have documented retention and deletion policies for the personal information you use. This helps to ensure that you don't keep information for longer than you need to. This may reduce the amount of information you need to review when responding to a SAR.
- **Security** — You **should** have measures in place to securely send information. For example, you **could** use a trusted courier or have a system to check email addresses and review responses before sending.

What about our information management systems?

You **should** ensure that your information management systems allow you to easily find and extract personal information, and to redact third-party information where necessary.

If you are implementing a new information management system, you **must** design and build data protection compliance into your processing activities and business practices from the start. This means that you **must** take steps to ensure that your new system complies with data protection principles and minimises the risks to people's rights and freedoms. You **should** also ensure that your system supports dealing with SARs.

You **should** also have effective records management policies, such as:

- a well-structured file plan;
- standard file-naming conventions for electronic documents; and
- a clear retention policy about when to keep and delete documents.

This will help you with your accountability and documentation obligations.

Relevant provisions in the UK GDPR - see Articles 5(1)(c), 5(2), 25, 30, 32, 26, 28 and Recitals 39, 78, 82, 83

http://www.legislation.gov.uk/eur/2016/679/contents

Further reading

- Data protection by design and default
- Documentation

How do we recognise a subject access request (SAR)?

In more detail

What is a SAR?

A SAR is a request made by or on behalf of a person for the information they are entitled to ask for under article 15 of the UK GDPR. This includes:

- confirmation of whether or not you are holding or using their information;
- a copy of their personal information; and
- other supplementary information.

Are there any formal requirements?

There are no formal requirements for a valid request. A person can make a SAR verbally or in writing, including by social media. They can make it to any part of your organisation, and they do not have to direct it to a specific person or contact point.

The person does not have to include the phrases "subject access request", "right of access" or "article 15 of the UK GDPR" in their request. It just needs to be clear that they are asking for their personal information. A request can be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002.

Any of your employees may receive a valid request. You **must** identify and handle each request correctly. You **should** consider training your staff so that they can identify a request.

You **should** have a policy for recording details of the requests you receive, including those made by phone or in person. This allows you to contact the person to confirm their identity or make sure you have understood their request, if you need to. For more information, see can we ask for ID?

People do not have to tell you their reason for making a request or what they intend to do with the information. However, if they do so, it may help you find the relevant information more easily.

Can we provide a standard form or online system for people to make a request?

Standard forms can make it easier for you to recognise a SAR and for people to include all the details you might need to locate their information.

You **should** enable people to make SARs electronically where possible, particularly if you use electronic systems for processing their information. You **could**:

- design a standard SAR form that people can complete and submit to you electronically; or
- enable people to make SARs to you via a secure online system, free of charge.

However, a person can make a SAR by any means. You can invite people to use your standard process, but you **should** make it clear that using the form or online system is not compulsory.

Can people make a request via social media?

Yes. People can make a SAR using any social media site where your organisation has a presence.

Therefore, you **must** take reasonable and proportionate steps to identify and disclose relevant information when people make requests on your social media channels.

In general, responding on social media is not a secure way of providing information. You **should** ask for alternative delivery details instead. For further guidance, see How do we provide the information securely?

Can a request be made on behalf of someone else?

Yes. A person may want a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. However, it is essential that you are satisfied that the third party making the request is entitled to act on the person's behalf. The third party is responsible for providing you with evidence of this — for example, by providing a written authority, signed by the person the information is about, stating that they give the third party permission to make a SAR on their behalf.

Example

A building society has an elderly customer who visits a particular branch to make weekly account withdrawals. Over the past few years her daughter, who is also a customer of the branch, has always accompanied her. The daughter makes a SAR on her mother's behalf. She explains that her mother does not feel comfortable making the request herself, as she does not understand data protection.

While the branch staff know the daughter and have some knowledge of her relationship with her mother, it is still necessary to obtain more formal authority.

If the daughter can provide written authority from her mother giving her permission to make a SAR on her mother's behalf, the building society can comply with the request.

You **could** accept electronically signed letters of authority as valid evidence, provided that:

- you are confident that the person whom the information is about made the electronic signature;
- the signature was made recently (ie it is not out of date and was not previously used to obtain information about the person); and
- you are satisfied that the third party is authorised to act on the person's behalf, and to receive the information on their behalf.

If the third party gives additional details with their request (eg the person's address, up-to-date ID and account number), this may help to show that the request is valid.

As a controller, you **must** ensure that you deal with information securely and responsibly. You **should** clearly explain in your privacy information what authority you require from a third party acting on someone's behalf. If you have concerns about the validity of electronically signed letters of authority, you **should** make it clear that you do not accept these as proof of authority.

Other mechanisms may allow a third party to make a SAR on a person's behalf, such as powers of attorney. You need to check the type and circumstances of the particular power of attorney to determine whether the third party is authorised to make a SAR. However, it's reasonable to assume that an attorney with authority to manage someone's property and affairs has the appropriate authority to make a SAR on their behalf.

If you have no evidence that a third party is authorised to act on a person's behalf, you cannot comply with the SAR until you receive the appropriate authority. However, you **should** respond to the third party and explain why you cannot comply.

In most cases, provided you are satisfied that the third party has the appropriate authority, you **should** respond directly to them. If you have reasonable grounds to believe that a person may not understand the nature of the information you are disclosing, and you are concerned about revealing excessive information to the third party, you **could** contact the person first to make them aware of your concerns. For example, this may be appropriate if the information is particularly sensitive or the person may not know the extent of the information that is likely to be disclosed.

If the person agrees with your concerns and is happy to receive the information from you directly instead, you **must** send the response directly to them rather than to the third party. The person may then choose to share the information with the third party after reviewing it. However, if the person responds and asks you to send the information to their third-party representative, you **must** do so.

If you do not receive a response from the person, you **should** provide the requested information to the third party. If the person has specifically asked you not to contact them directly, then you **should** only correspond with the

authorised third party. If you are processing health information, see What about requests for health information from a third party?

In some cases, a person does not have the mental capacity to manage their own affairs. There are no specific provisions that enable a third party to make a SAR on behalf of such a person in the UK GDPR, the Mental Capacity Act 2005, the Mental Capacity Act (Northern Ireland) 2016 (please note that not all provisions in the Act have been commenced at this time) or the Adults with Incapacity (Scotland) Act 2000. However, as mentioned above, it's reasonable to assume that an attorney with authority to manage someone's property and affairs has the appropriate authority to make a SAR on their behalf. The same applies to a person appointed to make decisions about such matters by:

- the Court of Protection (in England and Wales);
- the Sheriff Court (in Scotland); and
- the High Court (Office of Care and Protection) (in Northern Ireland).

Do we have to respond to requests made via a third-party online portal?

You may receive a SAR made on a person's behalf through an online portal (eg from a third party that provides services to help people exercise their rights).

To decide if you need to comply with such a request, you **should** consider whether you:

- have been made aware that a particular person is making a SAR;
- can verify the person's identity, if this is in doubt (see Can we ask for ID?);
- are satisfied that the third-party portal is acting with the authority of, and on behalf of, the person; and
- can view the SAR without having to take proactive steps, such as paying a fee or signing up for a service.

You don't have to take proactive steps to check if someone has made a SAR. If you can't view the request without paying a fee or signing up for a service, you haven't received the SAR and don't have to respond.

It's the portal's responsibility to provide evidence that it has the appropriate authority to act on the person's behalf when it makes the request. A person's agreement to the terms and conditions of the portal's service is unlikely to be

evidence of appropriate authority (see Can a request be made on behalf of someone else?).

If you're concerned that the person hasn't authorised the uploading of their information to the portal, you **should** contact the person before responding.

You also don't have to pay a fee or sign up to any third-party service to respond to a SAR. But this doesn't mean that you can ignore the request. Instead, you **should** provide the information directly to the person if they agree. If they don't agree, you **must** explain how they can make a SAR in another way. This is different from when a person makes a reasonable request for you to provide their information in a particular format. See In what format do we need to provide the information?.

Sometimes, you might not be able to contact the person directly — for example, if you don't have their address or aren't satisfied with the ID provided. If this is the case, you **should** advise the third-party portal that you won't respond to the request until it gives evidence that:

- it is acting with the authority of, and on behalf of, the person (which may involve ID checks); and
- the person has agreed to the uploading of the information to the portal.

Until then, you have not received a valid SAR. The time limit does not start until you receive the details you've asked for.

If you have concerns about supplying the information via the portal for any reason, including security concerns, you **should** contact the person first to make them aware. If the person agrees with your concerns and is happy to receive the information directly, you **must** send the response directly to them rather than to the portal. If the person has asked you not to contact them directly, you **could** communicate via the portal that you will provide the response in an alternative format and invite the third-party representative to contact you directly.

A person can make a SAR using the portal but ask you to send them their information by another method. You **should** comply with their request where possible.

What about requests for information about children?

The right to access information you hold about a child is the child's right rather than anyone else's, even if:

- they are too young to understand the implications of the right of access;
- the right is exercised by those who have parental responsibility for the child; or
- they have authorised another person to exercise the right on their behalf.

Before responding to a SAR for information held about a child, you need to consider whether the child is competent to make a SAR. This means that you need to decide if the child is mature enough to understand their rights.

There's no set age for this in England, Wales and Northern Ireland. However, Scotland sets the age at 12 – so this is a good guide to help you decide.

When making this decision, you **should** consider the nature of the personal information, as well as the child's:

- level of maturity;
- ability to understand what they are asking for and what they will receive; and
- ability to understand the consequences of authorising someone to act on their behalf.

It's likely to be easier to assess competence if you have regular contact with the child. If you don't, you **should** take a common-sense approach based on the child's age and the nature of the information. If the information is sensitive, you **should** make stronger efforts to check the child's competence.

If a child is competent, they can make a SAR themselves or ask someone else to do so on their behalf (eg their parent or guardian, a child advocacy service, charity or solicitor. You'll need to obtain evidence that the child has authorised another person to make the SAR. If it's evident that a child is acting against their own best interests, you may be able to withhold the information if an exemption applies – for example, if a child asks a third party to make a SAR on their behalf, but you have reasonable concerns that the third party is pressuring the child to make the SAR, and disclosing the information is likely to cause serious harm to the physical or mental health of any person.

If the request is from a child and you're confident that the child can understand their rights, you **must** respond directly to the child.

If you're satisfied that the child is not competent, and the request is from a person with parental responsibility for the child, it's usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf.

If a parent or guardian, or someone authorised by the child, makes a SAR on the child's behalf, you also need to consider:

- any court orders about parental access or responsibility that may apply;
- any duty of confidence owed to the child;
- any consequences of allowing those with parental responsibility or those authorised to act on the child's behalf to have access to the child's information (this is particularly important if there have been allegations of abuse or ill treatment);
- any detriment to the child if people with parental responsibility, or their authorised representatives, cannot access this information; and
- if the child has expressed any views on whether they want their parents, guardians or authorised representatives to have access to information about them.

What should we do if a request mentions freedom of information?

A SAR may mistakenly state that it's a freedom of information (FOI) request. However, if it is about the requester's personal information, you **should** treat it as a SAR.

Example

A local authority receives a request from a person asking for a copy of any information the authority holds about them about a dispute over their council tax. Although the person states that this is a "freedom of information request", it's clear that they are only asking for their personal information. As such, the local authority treats this as a SAR.

You are more likely to receive a SAR in the form of an FOI request if your organisation is a public authority for the purposes of the:

- Freedom of Information Act 2000 (FOIA);
- Freedom of Information (Scotland) Act 2002 (FOISA);
- The Environmental Information Regulations 2004 (EIR); or
- The Environmental Information (Scotland) Regulations 2004 (EIRs).

For ease of reference, these are referred to as FOI law in this section.

How you deal with the request depends on whether it only relates to the requester's personal information or to other information as well.

If the requester is only asking for their own personal information, but they have mentioned FOI law, you **should** do the following:

- Deal with the request as a SAR in the normal way. The requester does not need to make a new request. You may need to ask the person to verify their identity.
- If your organisation is a public authority, the requested personal information is exempt from disclosure under FOI law. Strictly speaking, you need to issue a formal refusal notice saying so. But in practice, we do not expect you to do this in these circumstances. However, if you are a public authority in Scotland, you need to follow guidance issued by the Scottish Information Commissioner.
- If your organisation is a public authority, clarify within 20 working days that you are dealing with the request as a SAR under the UK GDPR, and that the one-month time limit for responding applies.

If you are a public authority and the request relates to both the requester's personal information and to other information, you **must** treat this as two requests:

- One for the requester's personal information, made under the UK GDPR.
- Another for the remaining information, made under FOI law.

It's important to consider the requested information under the correct legislation. This is because a disclosure under FOI law is made to the world at large, not just to the requester. If you mistakenly disclose personal information under FOI law, this will be a personal data breach.

Can we deal with a request in our normal course of business?

It's important to draw a practical distinction between formal requests for information and routine verbal enquiries and correspondence that you can deal with in your normal course of business. You can respond to an enquiry in the normal course of business if you provide such information routinely and can respond quickly. However, the SAR process may be appropriate where a person requests a high volume of information, and you need to conduct a time-consuming search of your records to comply.

If a person requests copies of letters you previously sent to them, it's unlikely that you need to deal with this as a formal SAR. You **could** consider these enquiries on a case-by-case basis. However, your normal business processes **should not** restrict or delay a person's right to access their information.

Example

If an employee requests a copy of their most recent payslip and their employment contract, you can deal with the enquiry in your normal course of business. The employee is entitled to this information under other laws. You do not need to treat the request as a SAR.

Example

A person phones their bank to query a charge and ask for a copy of their statement. Once the staff member verifies the person's identity, they discuss the matter on the call with the customer and arrange to send them a copy of their statement in line with the bank's normal business processes.

Relevant provisions in the UK GDPR - see Articles 15 and Recitals 59, 63

http://www.legislation.gov.uk/eur/2016/679/contents

Further reading

- Children and the UK GDPR
- Freedom of information guidance and resources
- EIR and access to information

What should we consider when responding to a request?

In more detail

How long do we have to comply?

You **must** comply with a SAR without undue delay and at the latest within one month of receipt of the request **or** within one month of receipt of:

- any information you request to confirm the identity of the person the information is about (see Can we ask for ID?);
- any information you request to confirm that the third party is authorised to act on behalf of the person; or
- a fee (only in certain circumstances – see Can we charge a fee?)

How do we calculate a month?

To calculate a month, you **must** start from the actual date you receive the request, fee or other requested information and count forward to the end of the same date in the following month. Even if you receive the request on a non-working day, you **must** start from this date.

Example

A request is received on 1 January (a bank holiday), so the one-month period ends at the end of 1 February.

If the date for responding falls on a weekend or is a public holiday, the deadline moves to the end of the next working day.

Example

A request is received on Monday 25 November. The time to respond will run until the end of Friday 27 December. This is because 25 and 26 December are both bank holidays.

If the same date doesn't exist in the following month (because it's shorter), use the last day of that month instead.

Example

A request received on 31 January will run until the end of 28 February (or 29 February in a leap year). If that date falls on a weekend, the deadline is the end of the next Monday.

This means that the exact number of days you have to comply with a request varies, depending on the month in which you receive the request.

If you need to specify a consistent number of days (eg for operational or system purposes), you **could** adopt a 28-day period to ensure that you always comply within a calendar month.

Can we extend the time for a response?

Yes. You can extend the time to respond by a further two months if:

- the request is complex; or
- you have received a number of requests from the same person. This can include other types of requests about their rights – for example, if a

person has made a SAR, a request for erasure and a request for data portability at the same time.

You **must** calculate the extension as three months from the original start date.

Example

An organisation receives a request on 7 August. The request is complex, so the organisation extends the period by two months.

The organisation has until the end of 7 November to comply with the request. If 7 November falls on a weekend or is a public holiday, the organisation has until the end of the next working day to comply.

You **must** let the person know that you are extending the time limit within one month of receipt of the request **or** within one month of receipt of:

- any information you request to confirm the identity of the person the information is about (see Can we ask for ID?);
- any information you request to confirm that the third party is authorised to act on behalf of the person; or
- a fee (only in certain circumstances — see Can we charge a fee?).

When is a request complex?

You **should** consider your specific circumstances and the particular request when determining whether a request is complex. What may be complex for one organisation may not be for another. For example, the size and resources of your organisation are likely to be relevant factors.

You **must** be able to show why a request is complex in the particular circumstances. The following are examples of factors that may, in some situations, add to the complexity of a request:

- Experiencing technical difficulties with retrieving the information (eg if information is electronically archived).
- Applying an exemption that involves large volumes of particularly sensitive information.

- Clarifying potential issues around disclosing information about a child to a legal guardian.
- Requiring specialist work to obtain the information or communicate it in an intelligible form.
- Clarifying potential confidentiality issues around disclosing sensitive medical information to an authorised third party.
- Needing to obtain specialist legal advice (however, if you routinely obtain legal advice, it's unlikely to be complex).
- Searching large volumes of unstructured manual records — only applicable to public authorities.

If a person requests a large volume of information, this may add to the complexity of the request. However, a request is not automatically complex because it involves a large amount of information.

A request is not complex just because you have to rely on a processor to provide the information you need to respond.

Can we clarify the request?

Yes. You can ask for further information to help you identify the personal information or the processing activity that the SAR relates to.

However, you **should not** ask for clarification on a blanket basis. You **should** only ask if it's reasonably required.

The legislation does not define what is reasonably required. However, it's likely to refer to circumstances where you are unable to provide an effective response to the SAR until you have received clarification. For example, this may be the case if the request is vague or you hold a lot of information about the person.

If you do ask for clarification, the time limit pauses on the day you request clarification and resumes on the day you receive it. This is referred to as 'stopping the clock'.

This means that you don't need to provide the person with a copy of the information until they clarify their request. This includes any supplementary information that you can't reasonably provide.

You are not required to seek clarification, and you may choose to perform a reasonable search instead. See What efforts should we make to find information?

What do we need to think about if we ask for clarification?

Given the importance of the right of access, you **should** be able to justify why it's reasonable for you to ask for clarification before you can identify the information that has been requested.

For example, it may be reasonable for you to ask for clarification if:

- you hold a large amount of information about the person; or
- the request is unclear.

You are responsible for justifying that you will need to search through a large amount of information to deal with a SAR. It's unlikely to be reasonable or necessary to ask for clarification if you can locate, retrieve and provide information about the person quickly and easily — even if you hold a large amount of information about them.

Whether you hold a large amount of information about a person will, to an extent, depend on your organisation's size and available resources:

- A big organisation may not consider a request to be high volume if it has significant resources for performing searches.
- A smaller organisation with fewer and less sophisticated resources at its disposal may be more able to argue that it holds a large amount of information.

Another factor to consider is whether, because of its volume, you are unlikely to be able to locate and retrieve all the requested information by performing a reasonable search.

If you need clarification, you can ask the requester to provide additional details, such as the context in which you are likely to hold their information and the relevant dates.

However, you cannot force a person to narrow the scope of their request, as they are entitled to ask for all their information. If the person responds to you and either repeats their request or refuses to provide any additional information, you **should** still comply with their request by making reasonable searches.

Example

A person writes to their local GP practice and asks for "all the information you hold about me". The practice employed the person as a receptionist for many years, and they are currently registered as a patient. As the person is now a carer for their elderly parent, the practice also holds personal information about them within their parent's file.

The practice believes that it has a large volume of information about the person. However, it is not clear from the request what information the person wants. If the practice performs a reasonable search of its records, it will be able to provide some of the information held about the person, but it would need to perform a much more extensive search to provide all the information it holds.

In these circumstances, it is reasonable to ask the person to clarify their request. The practice **should** explain to the person that, while they are entitled to request all information held about them, the practice is only required to conduct a reasonable and proportionate search of its records. This means that the person may only receive some of the information the practice holds about them. The practice **could** also explain that, if the person clarifies their request, it will be able to focus its searches on locating the specific information that they want.

The person may clarify the request by, for example, asking for:

- details of their employment from 1993 to 2008;
- their medical records relating to an accident in 2018; and
- "everything else you hold about me".

The practice **should** focus its searches on the first two enquiries and then perform a reasonable search for the rest of the information.

Even if you're seeking clarification, you can often still provide **some** information, although this depends on the circumstances.

For example, in many cases, you can confirm that you hold information about the person. In addition, you will likely be able to provide some of the supplementary information, including details of:

- their right to request rectification, erasure or restriction, or to object to processing;

- their right to complain to the controller; and
- their right to make a complaint to the ICO.

If you can reasonably provide any of the supplementary information without clarification, you **must** provide it within one month of receipt of the request. If your privacy notice already contains this supplementary information, you **could** provide the person with a link to it.

Example

A supermarket receives a SAR from a long-standing employee for "all the information you hold about me, based on my concerns about recent issues". The employee has recently had a complaint made about them by another employee.

As the supermarket holds a large amount of information about the employee, and the request is unclear, it asks them to clarify their request.

In particular, it asks if the employee:

- only wants information about the complaint; or
- also wants information about their employment between particular dates.

If they do want employment information, the supermarket asks them to clarify the date range they are interested in.

The supermarket also asks if they want information unrelated to their employment as well (eg information linked to their customer reward account).

The supermarket explains to the employee that it holds a large amount of information about them for different purposes. It also explains that, although they are entitled to ask for all their information, it is only required to perform a reasonable and proportionate search. Therefore, if the employee wants a very specific piece of information, they should clarify what it is. This will enable the supermarket to carry out effective searches and provide the information the employee needs.

Once the request for clarification is sent, the supermarket can stop the clock. It is not required to respond until the employee answers the request for clarification. However, it can still provide some of the supplementary information within one month, including:

- the purposes of processing;
- the categories of personal information it holds about the employee;
- the retention period;
- details of the employee's right to make a complaint to the supermarket; and
- details of the employee's right to make a complaint to the ICO.

The supermarket sends the employee a copy of its privacy information (which covers these supplementary points) when it asks for clarification on the other details of the request.

You **should** ensure the process of seeking and obtaining clarification is quick and easy for the requester. When asking for clarification, you **should:**

- provide advice and assistance to help them clarify their request;
- explain that the clock stops from the date that you request clarification and will resume once they respond; and
- specify if they need to reply by a certain time.

Where possible, you **should** contact the person in the same format they made the request. For example, if they emailed the SAR, you **should** email them to ask for clarification.

If you receive a request where it is genuinely unclear whether a person is making a SAR, the time limit does not begin until you have clarified:

- if the person is making a SAR; and
- what personal information they are requesting.

You **should** contact the person as soon as possible (eg by phone or email where this is appropriate). If you talk to the person, you **should** keep a record of:

- any conversation you have with them about the scope of their request; and
- the date(s) when you request and receive any further explanation.

In all circumstances, you **should** explain to the person why you are seeking further details and be able to justify your position to the ICO, if asked to.

When you ask for clarification, the timescale for responding will stop until the person clarifies their request and will resume on the date you receive that clarification. You **should** calculate the timescale as follows:

- When you receive a request, calculate when the response would normally be due. See How long do we have to comply?
- If you have requested clarification, you may extend this time limit by the number of days that you stopped the clock.

Example

If you receive a request on 14 May, the time limit starts on the same day. You will have one month to reply, which means the response is due by or on 14 June.

However, if you ask for clarification on 15 May, the clock stops from 15 May until the date the requester responds. If the requester gives you clarification on 18 May, the timing resumes on that date.

The clock was stopped from 15 May until 18 May. This means that you can extend the original one-month deadline by three days, and your response is due by or on 17 June.

You **should** ask for clarification as soon as possible after receiving the SAR. This will enable you to search for the information the person wants at the earliest possible stage and ensure that you have enough time to respond.

Example

An organisation receives a request on 19 June. As the equivalent date in July falls on a Sunday, the organisation has until Monday 20 July to comply.

The organisation waits until 15 July to ask for clarification. The person responds on 16 July, which means that the original deadline can only be extended by one day. The response is due by Tuesday 21 July.

However, the organisation can't comply by the deadline as it did not leave enough time to search for the information after obtaining clarification.

If it only becomes apparent after starting a search that you need further information to respond to the SAR, you **should** be able to explain why it was not possible to request clarification earlier. You **should** record your reasons.

If you ask for clarification and receive it on the same day, the clock does not stop. You **should** calculate any extension to the time limit in terms of days, not hours.

Example

If you receive a SAR on 1 July, request clarification on 2 July at 9:00am and receive clarification later that day, up to 11:59pm, you cannot stop the clock and extend the time limit by one day. The original deadline of one month from 1 July still applies.

The clock only stops if you are seeking clarification about the information requested. It does not apply if you ask for clarification on any other matter — for example, the format of the response.

Example

A person requests a copy of their medical records from 5 February 2011 until 9 August 2017. They specifically ask for the medical practice to forward the records by email. However, because of security concerns, the practice cannot email the records. Instead, it can provide the person with remote access to their information. The practice asks the person whether they are happy with this.

> The clock does not stop when the practice asks for clarification, and the usual time limit of one month still applies. Since the time limit is not paused while waiting for a response, the practice **should** begin searching for the requested information as soon as possible.

If you seek clarification but do not receive a response, you **should** wait for a reasonable period of time before considering the request closed. While one month is generally reasonable, you **should** adopt a proportionate and reasoned approach. If you believe that a person might have difficulty in providing additional details within a specified timeframe, you **should** try and accommodate the person as much as possible — for example, where there are complex issues or accessibility considerations.

If you need to request clarification and proof of ID, you **should** do both as soon as possible. It's unreasonable to wait until the person gives clarification before asking for ID, unless there is a risk of disclosing personal information to the person before you have checked their identity.

You can extend the time limit by two months if the request is complex or the person has made a number of requests (see Can we extend the time for a response?). However, a request is not complex just because you need to seek clarification. See When is a request complex?

Can we charge a fee?

In most cases, you cannot charge a fee to comply with a SAR.

However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if:

- it is manifestly unfounded or excessive; or
- a person requests further copies of their information following a request.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request. See Exemptions: when can we consider a request to be manifestly unfounded or excessive?

When determining a reasonable fee, you can consider the administrative costs of:

- assessing whether or not you are processing the information;

- locating, retrieving and extracting the information;
- providing a copy of the information; and
- communicating the response to the person, including contacting them to tell them that you hold the requested information (even if you are not going to provide it).

As there may be substantial overlap across these activities, you **should** ensure that the fee is reasonable and that you do not double-charge the person. For example, you may locate, retrieve and extract the information in one action, depending on the context in which you hold the information and how you search for it.

A reasonable fee may include the costs of:

- photocopying, printing, postage and any other costs involved in transferring the information to the requester (eg the costs of making the information available remotely on an online platform);
- equipment and supplies (eg discs, envelopes or USB devices); and
- staff time.

You **should** base the costs of staff time on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate. Section 12(1) of the DPA allows for the Secretary of State to specify limits on the fees that organisations may charge to deal with a manifestly unfounded or excessive request by way of regulations. However, at present, there are no regulations in place.

You **should** ensure that you charge fees in a reasonable, proportionate and consistent manner. Therefore, you **could** establish an unbiased set of criteria for charging fees that explains:

- the circumstances in which you charge a fee;
- your standard charges (including a costs breakdown where possible, eg the cost per A4 photocopy); and
- how you calculate the fee — explaining the costs you take into account, including staff time.

Your criteria **should** be clear, concise and accessible. You **should** make these criteria available on request. You don’t need to publish them online.

When requesting a fee, you **should** explain the costs to the person. You **should** include a copy of the criteria in your request for a fee and explain

any charge that is unclear (see Do we need to explain the information we supply?).

You **should** be able to justify the costs you have charged if a person complains to the ICO.

If you choose to charge a fee, you don't need to comply with the SAR until you have received the fee. You **should** request the fee as soon as possible and, at the latest, within one month of receiving the SAR. The longer it takes for you to ask for a fee, the less likely it is that this is reasonable. It's unreasonable to ask for a fee as a way of extending the period of time you have to respond to the request.

You **should** record the reasons for any delay in requesting a fee and be able to provide your reasons to the ICO, if asked.

You **should** allow the person a reasonable period of time to respond to your request for a fee. It's generally reasonable to close the request if you do not receive a response within one month, although this also depends on the circumstances.

Do we need to make reasonable adjustments for disabled people?

You may need to make reasonable adjustments to ensure a disabled person can make a request.

What is a reasonable adjustment will depend on the person's specific needs. If you are aware that a person may require reasonable adjustments (eg they have told you what they need, or they have explained that they are disabled), you **should** communicate with them (eg by speaking to them) to find out how best to meet their needs before you respond to their SAR. For example, an adjustment may include providing the response in a particular format that is accessible to the person, such as large print, audio, email or Braille.

Your use of personal information **must** be lawful. As well as data protection requirements, you also need to consider whether you have obligations under other legislation.

Further information about how to make effective reasonable adjustments is available from the Equality and Human Rights Commission or from the Equality Commission for Northern Ireland.

Can we ask for ID?

Yes. To avoid personal information about one person being sent to someone else, either accidentally or as a result of deception, you need to be satisfied that:

- you know the requester's identity (or the person the request is made on behalf of); and
- the information you hold relates to the person in question (eg when a person has similar identifying details to someone else).

You can ask for enough information to judge if the requester (or the person the request is made on behalf of) is the person whom the information is about.

You **should** be reasonable and proportionate about what you ask for. Only request formal identification documents if necessary. You can use verification measures that you already have in place (eg an existing username and password).

If the requester's identity is obvious to you, you are unlikely to require more information. This particularly applies when you have an ongoing relationship with the person.

Example

An organisation receives a written SAR from a current employee. The staff member knows this employee personally and has even had a phone conversation with them about the request. Although the organisation's policy is to verify identity by asking for a copy of a utility bill, it is unreasonable to do so in this case since the staff member knows the person making the request.

If you have any doubts about the requester's identity, it's reasonable to ask them to verify their identity before sending the information.

How you receive the SAR might affect your decision about whether you need to confirm the requester's identity.

Example

An online retailer receives a SAR by email from a customer. The customer has not used the website for some time, and although the email address matches the company's records, the postal address given by the customer does not. Before responding to the request, it is reasonable to ask for further information, such as the customer's other account details.

The level of checks you make may depend on the nature of the information and on the possible harm and distress that an inappropriate disclosure may cause to the person concerned.

Example

A GP practice receives a SAR from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requester is the right patient. In this situation, it is reasonable for the practice to ask for more information before responding to the request, such as a birth certificate or another document confirming the person's identity. The potential risk to the former patient if the practice sends their health records to the wrong person is high, so the practice is right to be cautious.

You will sometimes need to request more information than usual to verify a person's identity – for example, where you hold records about different people with the same name.

The timescale for responding to a SAR does not begin until you have received the requested information. However, it's important to avoid delays. Therefore, you **should** request ID documents as soon as possible.

If the requested ID information is not sufficient and you need to take further steps to verify the person's identity, you can do so. The timescale for responding to the SAR resumes once you have completed the verification.

However, further requests for verification are only likely to be necessary in exceptional circumstances. See How long do we have to comply?.

The ID documents may not be sufficient if:

- the person supplies information which raises doubts about their identity; or
- you have reasonable concerns that the ID is fraudulent or that the person has obtained it fraudulently.

Example

After a company has received a SAR, it asks for proof of ID. However, when the person provides it, the name on the ID document is different from the name it has on record for the person. Therefore, the company cannot be certain that they are the same person.

In this situation, it is reasonable for the company to ask for further proof of the person's identity – for example, alternative ID or evidence that explains why the names are different. The timescale does not begin until the company has received sufficient information to verify the requester's identity.

While you do not need to keep copies of ID documents, you **could** keep a note of:

- what ID documents the person provided;
- the date you verified them; and
- who in your organisation verified them.

What if the person mentions other rights?

If you receive several requests from a person about other rights (eg the right to erasure and the right to data portability) at the same time as a SAR, you **should** deal with each request separately. However, certain steps may apply to all the requests, such as (where relevant):

- establishing proof of ID; and
- ensuring that a third party has authority to act on behalf of the person.

In these circumstances, you may be able to extend the time limit to respond by up to two months. See Can we extend the time for a response?.

How should we deal with bulk requests?

Depending on the size of your organisation and the nature of your business, you may receive multiple SARs in a short period of time. For example, in the financial services sector it is not uncommon for claims management companies to make bulk requests on behalf of multiple people. We refer to these here as bulk requests.

Although receiving bulk requests requires more resources, you **must** respond to each SAR made on a person's behalf.

Remember the following principles when dealing with high volumes of SARs:

- A SAR made as part of a bulk request has the same legal status as one person making a SAR.
- The person's reason for making a SAR is not relevant to whether their request is valid (except if you are considering applying the manifestly unfounded or excessive provisions).
- If a third party makes a request on behalf of a person, you **should** treat the SAR as if the person themselves had made the request. This means that you cannot take into account other requests made by the representative on behalf of other people.
- You need to satisfy yourself that the third party is authorised to make the request.
- You need to satisfy yourself as to the identity of the person concerned.
- Even if you hold no information about the person, you **must** respond to the request and tell them this.

Do we still need to comply if the person dies before we respond?

No. The definition of personal information only applies to a living person. If you receive a SAR but are aware that the person has died before you have provided your response, you don't have to respond to the request. If you receive a SAR from a person who was authorised to act on behalf of the deceased person when they were alive (eg a relative, a solicitor or someone who has power of attorney), you are not required to respond after the person has died. A person cannot make a SAR to access information about a deceased person, even if they previously acted on their behalf.

For circumstances where information about a deceased person is contained within the requester's personal information, see How do we deal with information that relates to the requester and a deceased person?

Relevant provisions in the UK GDPR - see Articles 12, 15 and Recitals 58, 59 63, 64

http://www.legislation.gov.uk/eur/2016/679/contents

How do we find and retrieve the relevant information?

In more detail

What efforts do we need to make to find information?

You **must** make a reasonable and proportionate search to respond to a SAR. This means that you **must** make reasonable efforts to find and retrieve the requested information. However, you are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information. To determine whether searches may be unreasonable or disproportionate, you **should** consider:

- the circumstances of the request;
- the volume of information you may need to search in order to respond;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

You **must** be able to show why a search is unreasonable or disproportionate.

Even where searching for certain information may be unreasonable or disproportionate, you **should** still search for any other information within the scope of a request. You may ask the person for further information to help you find the information they have requested. See Can we clarify the request? for more information.

You **should** ensure that your information management systems are well designed and maintained, so you can efficiently locate and extract requested

information and, where necessary, redact third-party information. For more information, see What about our information management systems?

What about electronic records that aren't easily available?

In most cases, you can easily find and retrieve information stored in electronic form. However, as it's very difficult to truly erase all electronic records, you may hold information that you do not have easy access to and that requires technical expertise to retrieve.

You may have removed the required information from your active systems in a number of different ways – for example, by:

- archiving it to storage;
- copying it to backup files; or
- deleting it.

Each of these is discussed in further detail below.

What about archived information and backup records?

You may archive or back up information for various reasons. For instance, you **should** be able to restore availability and access to personal information in the event of an incident. Read our guidance on security for more information.

The process of accessing electronically archived or backed-up information may be more complicated than the process of accessing 'live' information. However, there is no technology exemption from the right of access. You **should** have procedures in place to find and retrieve personal information that you have electronically archived or backed up.

Search mechanisms for electronic archive and backup systems might not be as sophisticated as those for active systems. However, you **should** use the same effort to find information to respond to a SAR as you would to find archived or backed-up information for your own purposes.

Remember that you cannot retain information indefinitely, just because you might find a use for it in the future. It may be more difficult for you to comply with a SAR if you have kept information for longer than you need it. You **should** have defined retention periods for how long you keep archived or backed-up information. Read our guidance on storage limitation for more information.

What about deleted information?

Information is 'deleted' when you try to permanently discard it and you have no intention of ever trying to access it again. Our view is that, if you delete personal information you hold in electronic form by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable you to recreate it does not mean you need to go to such efforts to respond to a SAR.

We will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously deleted personal information held in electronic form. We do not require you to use time and effort reconstituting information that you have deleted as part of your general records management.

What about information contained in emails?

It can sometimes be difficult to determine whether an email contains personal information. This depends on the contents of the email, the context of the information it contains, and what it's being used for. Remember:

- Just because the requester is the recipient of an email does not mean the whole content of the email is their personal information.
- The right of access only applies to the personal information in the email that relates to the person making the SAR. This means you may need to disclose only some of the email to comply with the SAR.
- An email has not been deleted just because a user has moved it to their 'Deleted items' folder, as it's still easily accessible in this location.
- Emails about a business matter may still contain personal information. This depends on the content of the email and whether it relates to the person.

Example

An employee makes a SAR for all the information you hold about them. During your search for their personal information, you find 2,000 emails that they are copied into as a recipient. Other than their name and email address, the content of the emails does not relate to the employee or contain their personal information.

You do not have to provide the employee with a copy of each email. Since the only personal information that relates to them is their name and email address, it is sufficient to:

- advise them that you identified their name and email address on 2,000 emails; and
- disclose to them the name (eg John Smith) and email address (eg JohnSmith@org.co.uk) contained in those emails.

Alternatively, you **could** provide one email with other details redacted as a sample of the 2,000 emails you hold. You **should** also clearly explain to the person why this is the only information they are entitled to under the UK GDPR. Remember, you **must** also provide them with supplementary information about how you use their personal information (eg retention periods for the emails).

However, if any content within any of the emails relates to the employee, you **must** provide them with a copy of those particular emails, redacted if necessary.

For further information on this, see our guidance on personal information — what is it?

What about information we store in different locations?

The right of access applies whether the personal information you hold is stored in one location or in many different locations.

It may be helpful to combine all your information stores in different locations into a single information store. This may help you in various ways, including for dealing with SARs. However, whether this is appropriate for you depends on your circumstances.

What about information stored on personal computer equipment?

If you are the controller, you **must** provide personal information in response to a SAR. In most cases, you do not have to supply personal information if someone else is storing it on their own computer systems (except where that person is your processor or if your staff have stored the requester's personal information on their personal devices).

It is not usually appropriate for your staff to hold information about customers, contacts or other employees on their personal devices (eg in private email accounts, smartphones, home computers or private instant messaging applications). You **should** have a policy which makes this clear, particularly as there may be security risks if staff keep information on devices that you do not control.

If you do permit staff to hold personal information on their own devices, they may be holding it on your behalf. This means that this information may be within scope if you receive a SAR. If you have a good reason to think your staff are holding personal information about the requester on their personal devices, you **should** ask them to search their private emails, devices or instant messaging applications, as appropriate.

What about other records?

Information held in other records can include:

- information held in non-electronic form (eg in paper files or on microfiche records); and
- information that was in an electronic record, but that you have removed from your live systems and archived in non-electronic form.

Whether information in hard-copy records is personal information depends primarily on whether the non-electronic records are held in a 'filing system'. This is because the UK GDPR does not cover information which is not, or is not intended to be, part of a filing system.

> 'Filing system' means any structured set of personal information which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

However, under the DPA, personal information held in unstructured manual records by public authorities is covered by the right of access. This includes paper records that are not held as part of a filing system. Therefore, public authorities may have to search this information to comply with SARs. For more information about this, see Unstructured manual records.

What about personal information in big datasets?

The volume and variety of big data, combined with the complexity of data analytics, may make it more difficult for you to meet your obligations under the right of access. However, these are not classed as exemptions and are not excuses for you to disregard these obligations.

Similarly, if you process information from a range of information sources, including unstructured information, this can pose difficulties when you need to produce all the information you hold about one person. This can be further complicated if you make use of observed or inferred information (ie information that a person does not provide to you directly). For example, if you generate insights about a person's behaviour based on their use of your service, where this information is identified or identifiable (directly or indirectly), then it's personal information and subject to the right of access.

In these situations, it's even more important that you practice good information management, not just for facilitating the right of access but also to ensure you meet the UK GDPR's legal requirements on accountability and documentation. You **should** have:

- adequate metadata;
- the ability to query your information to find all the information you hold about a person; and
- knowledge of whether the information has been truly anonymised, or whether it can still be linked to a person.

Can we amend or delete information following receipt of a SAR?

A SAR is about the information you hold at the time you receive the request. However, in many cases, routine use of the information may result in it being amended or deleted while you are dealing with the request. So, it's reasonable for you to supply the information you hold when you respond. This may be different from the information you held when you received the request.

However, it's not acceptable to amend or delete the information if you would not otherwise have done so. Under the DPA, you are committing an offence if you make any amendment to requested information with the intention of preventing its disclosure.

Relevant provisions in the UK GDPR - see Articles 4(6), 5(1)(e), 15, 32 and Recitals 39, 63, 83

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Chapter 3 and Section 173

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Further reading

- Integrity and confidentiality (security)
- Storage Limitation
- Bring your own device – what should we consider?

How can we supply information to the requester?

In more detail

What information do we need to provide?

The focus of a SAR is usually a copy of the requester's personal information. However, the right of access also entitles the person to other supplementary information (eg the purposes of processing). For a full list of the supplementary information that you **must** provide, see What other information is a person entitled to?

This supplementary information might be contained in the copy of the personal information you supply. If it is not, you **must** provide this supplementary information in addition to a copy of the personal information itself.

How do we decide what information to supply?

Documents (including draft documents) or files may contain a mixture of information that includes:

- the requester's personal information;
- personal information about other people; and
- information that is not personal.

In these circumstances, you **could** separately consider each document within a file, and even the content of individual documents, to assess the information they contain.

It may be reasonable (and more helpful) to give a requester a mixture of all the personal information and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it's their personal information. This is an appropriate approach where:

- none of the information is particularly sensitive or contentious; and
- none of the information refers to third parties.

When you respond to a SAR, you **should** provide enough contextual information to ensure that the response is concise, intelligible and easy for the person to understand.

Example

A person makes a SAR to their local authority, asking for specific personal information. The local authority provides an extract from a document that references the person's name and initials. However, it is not clear from the extract what the document is, or why the person's information is being used.

To comply with its SAR obligations, the local authority **must** provide additional contextual information to ensure that the SAR response is transparent and intelligible. For example, it **could** provide a copy of the document in full, redacting any information that is covered by an exemption, or provide further explanatory information in its cover letter.

In general, it may often be better to leave information in (unless it's covered by an exemption), particularly if it helps the person understand how you are using their information.

In what format do we need to provide the information?

Once you locate and retrieve the relevant personal information for the request, you **must** provide the requester with a copy.

How you do this, and the format you use, depend upon how the requester submits their request (ie electronically or otherwise).

If the SAR is submitted electronically (eg by email or via social media), you **must** provide a copy in a commonly used electronic format. You can choose

the format, unless the requester makes a reasonable request for you to provide it in another commonly used format (electronic or otherwise).

If the SAR is submitted by other means (eg by letter or verbally), you can provide a copy in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for you to provide it in another commonly used format.

Where the information is sensitive, you **should** ensure that you transfer it to the requester using an appropriately secure method. See How do we provide the information securely? for further details.

Whatever form you use to provide the information, you **must** ensure that it's clear and accessible to the person. It will not be sufficient to only allow them to view documents containing their personal information or listen to audio recordings — unless they are happy to do so.

You are responsible for providing the information to the person (or their appointed representative). This means that they do not have to take action to receive the information (eg by collecting it from your premises), unless they agree to do so.

You **could** supply a transcript or copy of a document if it exists. However, you do not have to create new information to respond to a SAR. Although the easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so.

What is a commonly used electronic format?

The UK GDPR does not define a 'commonly used electronic format'. When deciding what format to use, you should consider both the circumstances of the request and whether the person can access information in that format.

People do not have to take any specific action to access the information you provide in response to a SAR. This means that they do not have to download software, particularly because:

- it may involve people having to buy that software;
- depending on the source, it may pose a security risk to those people; and
- it does not provide them with 'direct access' to their personal information.

Example

A person makes a SAR for their personal information. The organisation gives a copy of this information using what it considers to be a commonly used electronic format.

When the person receives the response, some of the files are in a proprietary format, and they don't have the software needed to access these files. The organisation considers that it has provided the information in a commonly used format because of the availability of that software package.

However, the UK GDPR does not require people to purchase specific software packages to access a copy of their information. Therefore, the organisation has not fulfilled its obligation to provide a copy, as the person cannot access it.

You **could** ask the person for their preferred format before fulfilling their request.

You are providing the person with direct access to their information if:

- you send the person their information in an encrypted format; **and**
- you separately send them a secure code that they can use to access the encrypted information.

You **could** also use other alternatives, such as allowing the person to access their information remotely and download a copy in an appropriate format. See Can we provide remote access? for more information.

Can we provide remote access?

The UK GDPR encourages controllers to provide people with remote access to their personal information via a secure system.

This is not appropriate for all organisations, but there are some sectors where it may work well. It also helps you meet your obligations and reassure people about the amount and type of personal information you hold about them.

In general, you **could** satisfy the requirement to comply with a SAR by giving the person remote access to their information on a secure system. However, this will depend on whether they can download a copy of the requested information in a format that is accessible to them.

If a person can download a copy of their personal information in a commonly used electronic format, and they do not object to doing so, then this satisfies the requirement to provide a copy.

You **should** make it clear that a person has a right to ask for their information to be provided in a different format. If a requester is unable to, or does not want to, use a secure online platform to access their information, you **must** respond to the SAR using alternative methods. You **should** consider making reasonable adjustments where necessary.

If a person makes a reasonable request for you to provide their information in an alternative format, you **should** comply with their request where possible. However, if a person or their representative requests further copies in an alternative format after downloading their information from a portal, you **could** treat it as a manifestly unfounded or excessive request and refuse it, or charge a fee to respond. See Exemptions: when can we consider a request to be manifestly unfounded or excessive?

Can we provide the information verbally?

Yes. If a person asks you to, you can respond to their SAR verbally, provided you have confirmed their identity by other means. You **should** keep a record of the:

- date the person made their request;
- date you responded;
- details of who provided the information; and
- information you provided.

This is most likely to be appropriate if they have requested a small amount of information.

You are not obliged to provide information in this way. However, you **should** take a reasonable approach when considering such requests.

How do we provide the information securely?

As the controller of the information, you **must** take all reasonable steps to ensure its security. While there are many different ways to send the requested information to the person, there are some basic steps that you can take to help you with this.

On an organisational level, you **should** try and safeguard against human error. For example, you **should**:

- ensure that you have proper systems in place to record SARs;
- ensure that you properly train those responsible for responding to a request; and
- have a system or procedure in place to check email or postal addresses before responding to a request.

For more on this, see How can we prepare for a subject access request (SAR)?

The method you use to provide the information to the person may depend on any request they have made about the format they would like to receive their information in (see In what format do we need to provide the information?).

If you have any concerns over the method that the person has requested you use to send their information, you **should** contact them, explain your concerns and ask for an alternative method of providing the information.

If the person asks you to provide the information in hard copy, sending the information by post is secure in many circumstances. However, depending on the nature and sensitivity of the information, you **should** consider sending it by special delivery or via a courier service.

You **could** provide remote access to a secure system as a method of ensuring you provide the information securely. However, you **must** apply appropriate technical measures so that both the system and any information it holds are secure. You **could** use the security measures you already apply to your existing systems as a baseline. See Can we provide remote access? for more information.

Another option is that you **could** provide the information in an encrypted format and send a secure code to access the encrypted information separately.

See our guidance on security for more information on the security requirements of the UK GDPR, as well as our guidance on encryption for more details about how you can effectively implement encryption.

What if we have also received a data portability request?

If a person makes a SAR and a data portability request at the same time, you **should** consider what information comes under the scope of each request.

Remember that:

- the right of access concerns **all** the personal information you hold about a person (unless an exemption applies), including any observed or inferred information; and
- the right to data portability **only** applies to personal information 'provided by' the person, where you process that information (by automated means) based on consent or contract.

Also, while the right of access may require you to provide information in a commonly used electronic format, the right to data portability goes further. It gives people the right to receive personal information they have provided to you in a structured, commonly used **and** machine-readable format. It also gives them the right to request that you transfer this information directly to another controller.

Therefore, the required format for providing each piece of information depends on which right applies to that information.

Do we need to explain the information we supply?

You may need to explain some of the information you provide when you respond to a SAR. However, this depends on the type of information and the reason the person may have difficulty understanding it.

You **must** provide the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language:

- confirmation of whether you are processing the person's personal information;
- the other supplementary information you are required to provide (eg your purposes of processing); and
- any other communication you have with them about their request.

This means that you **should**:

- ensure that you do not include irrelevant or unnecessary details;
- be open, honest and truthful;
- ensure the information is easy to understand for the average person (or child);
- ensure the information is easy to access; and
- use common, everyday language.

This is particularly important to consider if you are providing the information to a child.

For more detail on how to provide information in a concise, transparent, intelligible and easily accessible form, see our guidance on the right to be informed.

You **should** give the person additional information to put their personal information into context and aid their understanding if the requested personal information is not in a form that they can easily understand. However, this is not meant to require significant effort, and you are not expected to translate information or decipher unintelligible written notes.

Example

A person makes a request for their personal information. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as 'A', while non-attendance at a similar event is logged as 'M'. Also, some of the information is in the form of handwritten notes that are difficult to read.

Without access to your key or index to explain the coded information, it is impossible for anyone outside your organisation to understand. In this case, you are expected to explain the meaning of the coded information. However, although you **could** do so, you are not required to decipher the poorly written notes, as the UK GDPR does not require you to make information legible.

Relevant provisions in the UK GDPR - see Articles 12, 15, 20 and Recitals 58, 63, 68

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading

- Right to data portability
- Right to be informed

Exemptions: when can we refuse a SAR?

In more detail

What are exemptions and how do they work?

There are a number of exemptions from the right of access. Where an exemption applies to the facts of a particular request, you **could** refuse to provide all or some of the requested information, depending on the circumstances. You can apply an exemption to any of the information you are required to provide to a person in response to their SAR. This includes:

- confirmation that you are processing their personal information;
- a copy of their personal information; and

- other supplementary information.

You can also apply an exemption to providing the supplementary information where doing this would prejudice the operation of the exemption. For further details about how this works, see Does this exemption apply to supplementary information?

Not all the exemptions apply in the same way. You **should** look at each exemption carefully to see how it applies to a particular SAR. Some exemptions apply because of the nature of the personal information (eg information contained in a confidential reference). Others apply because disclosing the information is likely to prejudice your purpose.

For more on prejudice, see What does 'prejudice' mean?

If an exemption does apply, you may sometimes be obliged to rely on it (for instance, if complying with a SAR would break another law). In other cases, you can choose whether to use the exemption or not.

You **should** consider whether an exemption applies on a case-by-case basis. You cannot routinely rely on exemptions or apply them in a blanket fashion.

In line with the accountability principle, you **should** document your reasons for relying on an exemption and be able to justify it.

What do we need to do if we refuse to comply with a request?

If you refuse to comply with a request, you **must** inform the person of:

- the reasons why;
- their right to make a complaint to the controller;
- their right to make a complaint to the ICO; and
- their ability to seek to enforce these rights through the courts.

If you believe that an exemption applies, you **must** be able to demonstrate this.

If you rely on an exemption, the reasons you give to the requester may depend on the circumstances. For example, if telling a person that you have applied a particular exemption would prejudice the purpose of that exemption, your response may be more general. However, where possible, you **should** be transparent about your reasons for withholding information.

What does 'prejudice' mean?

‘Prejudice’ is a term often used in the context of exemptions. Many of the exemptions discussed in this section allow a controller to withhold information to the extent that disclosure would prejudice a particular purpose or function.

The meaning of ‘prejudice’ may vary depending on the nature of the information and the specific circumstances. In general, it can mean:

- compromising or undermining a purpose or function;
- preventing a purpose or function from being carried out independently or fairly; or
- limiting rights and freedoms (for example, by compromising a person’s position in a negotiation).

Where you are applying an exemption based on prejudice to a particular purpose, function or right, you **should** clearly identify and document:

- the specific nature of the prejudice;
- a clear and direct link between the disclosure of the information and the prejudice likely to be suffered; and
- why the prejudice likely to be suffered is actual, real and of substance.

If a disclosure will only have trivial or insignificant consequences, this is unlikely to be sufficient to establish prejudice.

Prejudice may also occur where confirming or denying that you hold the information would itself undermine the purpose of an exemption. In these circumstances, you may be able to rely on an exemption to issue a ‘neither confirm nor deny’ (NCND) response.

Can an exemption be used to prevent prejudice to another organisation’s function?

Yes — but only in very specific circumstances. In the sections below, we discuss three exemptions you may apply if complying with a SAR (in full or in part) would likely prejudice another organisation’s function. These exemptions are:

- functions designed to protect the public;
- regulatory functions relating to legal services, the health service and children’s services; and
- other regulatory functions.

Please see the relevant sections below for more information about each of these exemptions.

When considering the use of an exemption in these circumstances, you **could** consult with the other organisation and seek their views before you respond. In such cases, you may consider the request to be complex, which will allow you to extend the time limit by up to two months. For more information, see Can we extend the time for a response?

You are responsible for deciding whether to disclose personal information in response to a SAR, and whether an exemption can be applied to withhold requested information. If you do apply an exemption, you **must** be able to explain why. If you choose to apply an exemption in these circumstances, consulting with the other organisation can support your reasoning and help you explain your actions more clearly.

Crime and taxation: general

There are two parts to this exemption.

The first part applies to personal information processed for the following crime- and taxation-related purposes:

- The prevention, investigation or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty, or an imposition of a similar nature.

You can only rely on this exemption to withhold this information to the extent that complying with a SAR is likely to prejudice these purposes. You need to judge whether or not this is likely in each case. You cannot use the exemption to justify denying access to whole categories of personal information, if its disclosure is unlikely to prejudice the crime and taxation purposes.

Example

A bank investigates one of their customers for suspected financial fraud. During the investigation, the customer who is under suspicion makes a SAR for all their personal information.

The bank decides that it will withhold information about the investigation. This is because disclosing it would likely damage the investigation, as the person may abscond or destroy evidence. However, the bank can provide other information that would not damage the investigation (eg the person's account details and transactions).

The second part of this exemption applies when another organisation obtains personal information used for any of the reasons mentioned above for the purposes of discharging statutory functions. The organisation that obtains the personal information is exempt from complying with a SAR to the same extent that the original organisation was exempt.

Example

The Independent Office for Police Conduct (IOPC) obtains information from the police for the purpose of carrying out its statutory function to investigate a complaint made against the police. The police advises the IOPC that this information is also being used as part of a criminal investigation. It tells the IOPC that it received a SAR while its investigations were in progress, and it applied a restriction under the relevant law enforcement provisions of the DPA to withhold the information to avoid prejudicing the prevention, investigation and detection of crime.

As this information is being used as part of a criminal investigation, the IOPC can rely on the crime and taxation exemption to withhold the relevant information if it receives a SAR, to avoid prejudicing the prevention, investigation and detection of crime.

If you are a competent authority using personal information for law enforcement purposes (eg the police conducting a criminal investigation), see our guidance on logging for law enforcement purposes for more information. If you are an intelligence service under part 4 of the DPA, see our guidance on intelligence services processing.

Relevant provisions in the DPA (the exemption) – see Schedule 2, paragraph 2

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 19, 20(1)-(2), 21(1), 34(1) and (4)

https://www.legislation.gov.uk/eur/2016/679/contents

Crime and taxation: risk assessment

Personal information is exempt from the right of access if it would disclose a person's classification within a risk assessment system, but only to the extent that complying with a SAR would prevent the system from operating effectively. For example, where a person has been classified as a tax compliance risk following review of their tax returns by HMRC, disclosing this information would compromise the effectiveness of this system (by notifying the person of their classification or revealing the methods used).

A government department, local authority or other authority administering housing benefit **must** operate the risk assessment system for:

- the assessment or collection of a tax or duty, or an imposition of a similar nature; or
- the prevention or detection of crime or the apprehension or prosecution of offenders, where the offence involves the unlawful use of public money or an unlawful claim for payment out of public money.

Relevant provisions in the DPA (the exemption) – see Schedule 2, paragraph 3

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Legal professional privilege

Personal information is exempt from the right of access if it consists of information:

- to which a claim to legal professional privilege (or confidentiality of communications in Scotland) may be maintained in legal proceedings; or
- about which a professional legal adviser owes a duty of confidentiality to their client.

This exemption covers the two branches of legal professional privilege: litigation privilege and legal advice privilege. In England, Wales and Northern

Ireland, the concept of legal professional privilege encompasses both these branches, which apply as follows:

- Litigation privilege applies to confidential communications between a client, professional legal adviser or a third party, but only where litigation is contemplated or in progress.
- Legal advice privilege only applies to confidential communications between a client and a professional legal adviser for the purpose of seeking or obtaining legal advice.

Under Scottish law, the concept of confidentiality of communications gives protection for:

- confidential communications between a client and solicitor, where the client seeks, and the solicitor gives, legal advice; and
- confidential communications made in connection with legal proceedings (this extends beyond communications solely between solicitors and clients to cover communications with third parties, such as experts or witnesses).

In Scotland, you may withhold information that comprises confidential communications between a client and their professional legal adviser in the same way that you may withhold information covered by legal advice privilege under English law.

The Scottish law also says that a litigant is not required to disclose material they have brought into existence for the purpose of preparing their case. This is similar to litigation privilege under English law.

Legal professional privilege is only available for communications that are confidential in nature, and:

- where litigation is not contemplated or in progress, made solely between client and professional legal adviser acting in a professional capacity; or
- made for the dominant purpose of obtaining or providing legal advice or being used by lawyers where litigation is contemplated or in progress.

A communication is a document that conveys information. It can take any form, including a letter, report, email, memo, photograph, note of a conversation, or an audio or visual recording. It can also include draft documents prepared with the intention of putting them before a legal adviser.

This exemption only applies where the obligations under data protection legislation prejudice the confidentiality of the work that lawyers are doing for their clients. It does not apply to all the processing that a lawyer or a law firm carries out.

Relevant provisions in the DPA (the exemption) – see Schedule 2, paragraph 19

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Functions designed to protect the public

Personal information is exempt from the right of access if you process it to perform one of six functions designed to protect the public, or if it relates to the actions of another organisation to carry out these functions — for example, if it's information:

- that you have shared with the other organisation; or
- that shows that the other organisation has contacted you about the person in relation to its investigations.

This exemption only applies to the extent that complying with a SAR would likely prejudice the performance of a specific function or functions. If you can comply with a SAR (even partially) without prejudicing the function, you **must** do so.

The first four functions are to:

- protect the public against financial loss because of the seriously improper conduct (or unfitness or incompetence) of financial services providers, or in the management of bodies corporate, or because of the conduct of bankrupts;
- protect the public against dishonesty, malpractice or other seriously improper conduct (or unfitness or incompetence);
- protect charities or community interest companies against misconduct or mismanagement in their administration, to protect the property of charities or community interest companies from loss or misapplication or to recover the property of charities or community interest companies; or

- secure workers' health, safety and welfare, or to protect others against health and safety risks in connection with (or arising from) someone at work.

However, to rely on this exemption, you **must** be able to show that one of the above functions is:

- conferred on a person by enactment;
- a function of the Crown, a Minister of the Crown or a government department; or
- of a public nature and exercised in the public interest.

The fifth function is to:

- protect the public from maladministration, or a failure in services provided by a public body, or from the failure to provide a service that it is a function of a public body to provide.

You can only rely on this if you are one of the following bodies or if you have shared the requested information with one of these bodies to enable it to discharge its function:

- the Parliamentary Commissioner for Administration;
- the Commissioner for Local Administration in England;
- the Health Service Commissioner for England;
- the Public Services Ombudsman for Wales;
- the Northern Ireland Public Services Ombudsman;
- the Prison Ombudsman for Northern Ireland; or
- the Scottish Public Services Ombudsman.

The sixth function needs to be conferred by enactment on the Competition and Markets Authority. This function is to:

- protect members of the public from business conduct adversely affecting them, to regulate conduct (or agreements) preventing, restricting or distorting commercial competition, or to regulate undertakings abusing a dominant market position.

Relevant provisions in the DPA (the exemption) – see Schedule 2, paragraph 7

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 19, 20(1)-(2) and 21(1)

https://www.legislation.gov.uk/eur/2016/679/contents

Regulatory functions relating to legal services, the health service and children's services

Personal information is exempt from the right of access if it's used for carrying out a function of:

- the Legal Services Board;
- considering a complaint under:
    - part 6 of the Legal Services Act 2007,
    - section 14 of the NHS Redress Act 2006,
    - section 113(1) or (2), or section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003,
    - section 24D or 26 of the Children's Act 1989, or
    - part 2A of the Public Services Ombudsman (Wales) Act 2005; or
- considering a complaint or representations under chapter 1, part 10 of the Social Services and Well-being (Wales) Act 2014.

The exemption only applies to the extent that complying with a SAR would likely prejudice the performance of a function or functions. If you can comply with a SAR (even partially) without prejudicing a function, you **must** do so.

Relevant provisions in the DPA (the exemption) – see Schedule 2, part 2, paragraph 10

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 19, 20(1)-(2), 21(1)

https://www.legislation.gov.uk/eur/2016/679/contents

Other regulatory functions

This exemption is only available where a function has been conferred on one of the following bodies or persons (the 'specified organisations'):

- the ICO;
- the Scottish Information Commissioner;
- the Pensions Ombudsman;
- the Board of the Pension Protection Fund;
- the Ombudsman for the Board of the Pension Protection Fund;
- the Pensions Regulator;

- the Financial Conduct Authority;
- the Financial Ombudsman;
- the investigator of complaints against the financial regulators;
- the monitoring officer of a relevant authority;
- the monitoring officer of a relevant Welsh authority;
- the Public Services Ombudsman for Wales; or
- the Charity Commission.

Personal information is exempt from the right of access if it's used to either:

- perform a function conferred on one of the specified organisations; or
- enable one of the specified organisations to perform a function.

This exemption only applies to the extent that, in either case, disclosure of the information would likely prejudice the function, or the performance of a specific function or functions. For further details about prejudice, see What does 'prejudice' mean?

When considering the use of this exemption you **could** consult with the other organisation and seek their views before you respond. If you do this, you may extend the time limit by up to two months if you deem the request to be complex.

If disclosing the information is not likely to prejudice a function, then you **must** comply with the SAR.

Example

A person makes a SAR to their bank asking for all their personal information. The bank withholds some of the details because they relate to an ongoing investigation by the Financial Conduct Authority.

Although the bank is not one of the specified organisations, it is helping the FCA's investigation by providing it with relevant information. This means that it can rely on the exemption to withhold information (including correspondence between it and the FCA), as disclosure would likely prejudice the investigation.

If the person makes a SAR after the FCA investigation has ended, the bank cannot rely on this exemption if disclosing the information would no longer be prejudicial to the FCA.

Relevant provisions in the DPA (the exemption) – See Schedule 2, paragraphs 11-12

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Judicial appointments, independence and proceedings

Personal information is exempt from the right of access if you use it:

- for the purposes of assessing a person's suitability for judicial office or the office of King's Counsel;
- as a person acting in a judicial capacity; or
- as a court or tribunal acting in its judicial capacity.

This exemption only applies to the extent that providing access would likely prejudice judicial independence or judicial proceedings.

The purpose of this exemption is to protect judicial independence. It applies to any information used by the person, court or tribunal in the exercise of their judicial function — not just their final decision. This includes pleadings, statements and reports considered as part of the judicial decision-making process. For example, this exemption applies to notes made by a judge for their own use during a trial.

This exemption does not apply to all information used in connection with legal proceedings. For example, legal representatives cannot rely on it to refuse to disclose information contained in documents filed or placed in the custody of the court (eg witness statements, medical or forensic reports or skeleton arguments). However, there may be other rules that apply to this information.

Some exemptions specifically apply to health, education or social work information processed by the courts.

If you are not acting in a judicial capacity, you may rely on this exemption to the extent that disclosing personal information would likely prejudice judicial proceedings or judicial independence. This may apply to information that has been shared with you by a court or body acting in a judicial capacity – or to information you have shared with them. For example, this may apply if a judge has disclosed the information to you in confidence or has attached specific conditions to its disclosure. In such cases, it's important that you consider any court order or specific judicial instruction about the handling of the information.

If you process information in connection with a criminal investigation or criminal proceedings, including proceedings for the sentencing of an offender, please see our guidance on the right of access – part 3: what you need to consider if personal information is processed by a court for law enforcement purposes.

We do not regulate the processing of personal information by a person, court or tribunal acting in a judicial capacity. Other bodies with a regulatory remit over those acting in a judicial capacity oversee such processing.

Relevant provisions in the DPA (the exemption) – See Schedule 2, paragraphs 14

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) – See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 19, 20(1)-(2) and 21(1)

https://www.legislation.gov.uk/eur/2016/679/contents

Journalism, academia, art and literature

Personal information may be exempt from the right of access if you process it for:

- journalistic purposes;
- academic purposes;
- artistic purposes; or
- literary purposes.

These are known as the 'special purposes'.

This exemption only applies to the extent that:

- you are processing the information with a view to the publication of some journalistic, academic, artistic or literary material;
- you reasonably believe that the publication of the material would be in the public interest, taking into account:
    - the special importance of the general public interest in freedom of expression,
    - any specific public interest in the particular subject, and
    - the potential harm to the requester if they do not receive their information; and
- as the controller, you reasonably believe that compliance with a SAR would be incompatible with the special purposes (ie it is more than just an inconvenience).

When deciding whether it's reasonable to believe that publication would be in the public interest, you **must** (if relevant) take into account the:

- BBC Editorial Guidelines;
- Ofcom Broadcasting Code; or
- Editors' Code of Practice.

If you rely on this exemption and the person makes a complaint to the ICO, you **should** be able to explain:

- why you require the exemption in each case;
- how you applied it; and
- who considered it at the time.

We do not have to agree with your view, but we need to be satisfied that you have a reasonable belief that this exemption applies to the request in the circumstances, and you **should** document your reasons why you believe this exemption applies.

Example

An investigative journalist plans to publish an article about the illegal and abusive treatment of animals at several slaughterhouses. The journalist has interviewed multiple people in connection with this matter and will be ready to publish the piece later in the year. A person whose anonymised interview will feature in the publication makes a SAR for a copy of their interview many months before the planned publication date.

Although the person's responses to the interview questions are their personal information, the journalist is concerned that the nature of the questions and responses reveals the purpose of the investigation.

In deciding whether or not to apply the exemption, the journalist considers the following points:

- They are processing the person's information with a view to publishing a piece of journalism.
- Publishing the material is in the public interest, as it relates to broader animal welfare issues in agriculture. Also, this matter does not impact the requester personally. As the journalist intends to

fully anonymise the information, the person cannot be identified through the publication.
- Disclosing the information at this stage could damage the ongoing investigation (eg lead to concealment of evidence), particularly if the requester were to share this information with others.

On balance, the journalist decides to apply the exemption and does not provide a copy of the interview. They explain to the requester the reason for this and keep a record of their reasoning.

Please refer to our Data protection and journalism code of practice for further information about this topic.

Relevant provisions in the DPA (the exemption) - Schedule 2, paragraph 26

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5(1)(a)-(e), 6, 7, 8(1)-(2), 9, 10, 11(2), 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1)(a)-(b) and (d), 19, 20(1)-(2), 21(1), 34(1) and (4), 36, 44 and 60-67

https://www.legislation.gov.uk/eur/2016/679/contents

Research and statistics

There is an exemption from the right of access if you use personal information for:

- scientific or historical research purposes; or
- statistical purposes.

This exemption only applies to the extent that complying with the SAR would prevent or seriously impair the achievement of these purposes, **and** if:

- the processing is subject to appropriate safeguards for people's rights and freedoms (see article 89(1) of the UK GDPR);
- the processing is not likely to cause substantial damage or substantial distress to a person;
- the processing is not used for measures or decisions about a particular person (unless the purposes for which the processing is necessary include approved medical research); and

- the research results are not made available in a way that identifies people.

Please refer to our guidance on the research provisions for further information about this exemption.

Relevant provisions in the DPA (the exemption) - Schedule 2, paragraph 27

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5(1)(b) and (e), and 15(1)-(3

https://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the UK GDPR (the appropriate safeguards) - see Article 89(1) and Recital 156

https://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA (safeguards) - see Section 19

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Archiving in the public interest

There is an exemption from the right of access if you use personal information for archiving purposes in the public interest.

This exemption only applies to the extent that complying with the SAR would prevent or seriously impair the achievement of this purpose, **and** if:

- the processing is subject to appropriate safeguards for people's rights and freedoms (see article 89(1) of the UK GDPR);
- the processing is not likely to cause substantial damage or substantial distress to any person; and
- you are not using the processing for measures or decisions about a particular person (unless the purposes for which the processing is necessary include approved medical research).

Please refer to our guidance on the research provisions for further information about this exemption.

Relevant provisions in the DPA (the exemptions) - see Schedule 2, paragraph 28

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5(1)(b) and (e), and 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the UK GDPR (the appropriate safeguards) - see Article 89(1) and Recital 156

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the DPA (safeguards) - see Section 19

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Health, education and social work information

The exemptions that may apply when a SAR relates to personal information included in health, education and social work information are explained in detail in these sections:

- What if a SAR involves information about other people?
- Health information
- Education information
- Social work information

Child abuse information

Child abuse information is personal information consisting of information about whether the person is or has been the subject of, or may be at risk of, child abuse. This includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, a person aged under 18.

You are exempt from providing child abuse information in response to a SAR if you receive a request (in exercise of a power conferred by an enactment or rule of law) from someone:

- with parental responsibility for a person aged under 18; or
- appointed by a court to manage the affairs of a person who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would not be in the best interests of the child.

This exemption can only apply in England, Wales and Northern Ireland. It does not apply in Scotland.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 21

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Article 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Management information

An exemption applies to personal information that you process for management forecasting or management planning about a business or other activity. This information is exempt from the right of access to the extent that complying with a SAR would likely prejudice the conduct of the business or activity.

To rely on the exemption, you **should** be able to do the following:

- Show that the personal information is relevant to, and is being used for, the purpose of management forecasting or management planning. It may therefore involve an element of forward-looking strategic thinking or consideration, although this is likely to be at a relatively high level.
- Justify that disclosing the personal information would likely prejudice the conduct of your business or activity.
- Show that the prejudice likely to be suffered by your organisation is greater than the harm likely to be experienced by the person as a result of not having access to their personal information.
- Provide the person with your reasons for applying the exemption (in most cases).

This is not a blanket exemption, and you **should** be selective, ensuring that you disclose any information not covered by it.

Example

The senior management of an organisation is planning a reshuffle. This is likely to involve making certain employees redundant, and this possibility is included in management plans. Before the organisation reveals the plans to the workforce, an employee makes a SAR.

In responding to the SAR, the organisation does not have to reveal its plans to make the employee redundant if this would likely prejudice the

conduct of the business — for example, by causing staff unrest before the management's plans are announced.

Example

A business services organisation plans to onboard a new client to do a niche piece of work. The organisation reviews its current staffing levels to establish whether it has enough suitably qualified staff. It produces an inventory of its current staff, with each person assessed against a list of criteria. This will help the organisation assess its recruitment needs for the year ahead.

An employee who has been identified as suitably qualified in the inventory makes a SAR for all their personal information. However, the organisation decides to withhold the relevant information in its staff inventory. It believes that disclosing the information may cause staff to become concerned that their job roles are changing or at risk, or that their workload may increase, which could result in a drop in morale or staff applying for other roles. Staff may also incorrectly assume that the organisation is planning to promote some staff above others. The organisation will inform staff about the new client in due course, but at present, it is only at the planning stage.

Taking this into account, the organisation decides to apply the management forecasting exemption and withhold the information. However, it **must** still comply with the SAR and provide the employee with the rest of the information it holds about them.

Example

An employee of a local authority makes a SAR asking for all their information, including any records of discussions between senior managers about their performance. The employee is an administrative assistant and has been through various disciplinary procedures because of their absenteeism. Senior managers have been involved in discussions about whether to terminate their employment.

The organisation considers whether it can withhold the records of the discussions between senior managers about the possibility of terminating

the employee's contract. In considering the relevance of the management forecasting exemption, the organisation considers:

- whether the discussions relate to its wider strategic thinking or forward planning; and
- whether disclosure of the information would cause prejudice to its wider conduct or activities.

The discussions are about the specific employee, not about the wider strategy of the organisation. They do not relate to or impact other staff within the organisation. Therefore, the requirements of the management forecasting exemption are not met. The authority **must** disclose the personal information that relates to the employee. However, it may be able to withhold information that relates to other people.

You may also consider applying the management forecasting exemption to refuse to confirm or deny that you hold the information where this would prejudice the exemption.

Example

A person (the requester) has been employed by a technology company for six months. Recently, they have heard rumours that many employees might be made redundant in the next few months.

In fact, because of financial challenges, the company is considering several options — including potential redundancies. However, no final decisions have been made. Despite this, as the information relates to management forecasting, and the company is still considering its options, it is likely to be prejudicial to release details at this stage.

The requester makes a SAR for "any information you have about me which relates to your planned redundancies". Their name is on a list of employees who have been identified as being 'at risk' of being made redundant.

If the company confirms that it holds the information, the requester is likely to infer that they are being considered for redundancy — even if

the company withholds a copy of the list itself. In the circumstances, confirming the information is held is likely to prejudice the company's ability to carry on its business, as it is likely to reveal that the company is considering redundancies, and the requester may be affected. The company decides to neither confirm nor deny whether it holds the information.

Relevant provisions in the DPA (the exemption) - see Schedule 2, paragraph 22

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Negotiations with the requester

Personal information that is a record of your intentions in negotiations with a person is exempt from the right of access. This only applies to the extent that complying with a SAR would likely prejudice the negotiations.

Example

A person makes a claim to their insurance company. The claim is for compensation for personal injuries they sustained in an accident. The insurance company disputes the seriousness of the injuries and the amount of compensation it needs to pay.

An internal paper sets out the company's position on these matters, including the maximum sum it is willing to pay to avoid the claim going to court. If the person makes a SAR to the insurance company, it does not have to send them the internal paper — because doing so would likely prejudice the negotiations to settle the claim.

The exemption does not set limits on the timing of negotiations or say you can only withhold information where negotiations are still ongoing. Therefore, you may be able to apply the exemption after negotiations have ended, but only if you can show that disclosure would likely prejudice negotiations. This

may be most relevant where you can show that disclosure would prejudice your position in future negotiations.

Relevant provisions in the DPA (the exemption) - see Schedule 2, paragraph 23

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Confidential references

From time to time, you may give or receive references about a person. The personal information included in a confidential reference is exempt from the right of access when it relates to the prospective or actual:

- education, training or employment of a person;
- placement of a person as a volunteer;
- appointment of a person to office; or
- provision of any service by a person.

The exemption applies regardless of whether you give or receive the reference.

Example

Company A provides an employment reference in confidence for one of their employees to company B. If the employee makes a SAR to company A or company B, the reference is exempt from disclosure.

This exemption only applies to references given in confidence. You **should** make it clear to people, and those providing references, whether you will treat references confidentially or adopt a policy of openness. You **should** do this through the privacy information you provide when you request the reference.

You **should** be as open as possible with people about information that relates to them. You **must** ensure that people are able to challenge information that they consider to be inaccurate or misleading, particularly

when, as in the case of a reference, this may have an adverse impact on them.

Relevant provisions in the DPA (the exemption) - see Schedule 2, paragraph 24

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Exam scripts and exam marks

This applies to academic, professional or other examinations leading to qualifications. There are two parts to this exemption.

The first part applies to information recorded by candidates in an examination. Candidates don't have the right to a copy of their answers to the questions.

The second part applies to information recorded by the person marking the exam. If the SAR is made **before** the results are announced, you can delay providing this information. Instead, you **must** provide the information within:

- five months of receiving the request; or
- 40 days of announcing the exam results, if this is earlier.

However, if the SAR is made after the results are announced, you cannot rely on this exemption.

Relevant provisions in the DPA (the exemption) - see Schedule 2, paragraph 25

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

https://www.legislation.gov.uk/eur/2016/679/contents

Manifestly unfounded or excessive requests

See Exemptions: when can we consider a request to be manifestly unfounded or excessive?

Information about other people

See Exemptions: can we refuse a SAR if it involves information about other people?

Other exemptions

The exemptions described in this section are those most likely to apply to SARs. However, other exemptions may be relevant. For more information, see our guidance on A guide to the data protection exemptions.

Exemptions: when can we consider a request to be manifestly unfounded or excessive?

In more detail

Can we refuse to comply with a manifestly unfounded or excessive request?

You can refuse to comply with a SAR (wholly or partly) if it is:

- manifestly unfounded; **or**
- excessive; **or**
- **both** manifestly unfounded **and** excessive.

Remember that there is a high threshold for relying on the manifestly unfounded or excessive provisions. However, you can interpret these provisions broadly by reference to other factors. This means that you do not have to prove that a request is either manifestly unfounded or excessive, provided you can show that the provision generally applies in the circumstances, with reference to supporting factors. For example, a request may be either unfounded or excessive, or have elements of both.

Alternatively, you may choose to respond to a manifestly unfounded or excessive request and charge the requester a reasonable fee.

What do we need to think about when deciding if a request is manifestly unfounded or excessive?

You **should** consider the following when deciding if a request is manifestly unfounded or excessive:

- Deal with each request on its own merits – do not have a blanket policy.
- Do not assume that a request is manifestly unfounded or excessive simply because the person has previously submitted such a request.
- A request made by a person's representative **must** be treated as if it had been made by the person themselves.
- If you decide a request is manifestly unfounded or excessive, you need to have strong justifications that can be clearly explained to the person and, if necessary, the ICO.

Any decision that a request is manifestly unfounded or excessive needs to be supported by clear evidence.

You **should** consider all the circumstances of the request. This may include broader factors beyond the request itself or the right of access.

Broader factors may include if a person has previously:

- made FOI requests,
- made service level complaints, or
- exercised other data protection rights.

For these factors to be relevant, you need to be able to show that they indicate a pattern of behaviour that supports that the person made the SAR for a purpose other than to exercise the right of access.

Remember that there is a high threshold for applying these provisions. You need to be able to show why these broader factors are directly linked to the request, **and** that the person's behaviour forms a pattern of unreasonably repetitive or malicious behaviour, which might indicate that their request is manifestly unfounded or excessive.

Example

A person who was injured at work makes a SAR to their employer. Although the person does not expressly say so, the employer suspects they want the information to pursue a civil claim for damages or to obtain legal advice. The employer is aware that the person may be able to obtain this (or similar) information through other legal mechanisms if they bring a claim, but they have not already done so.

The employer cannot refuse to provide the information just because it thinks the person wants it for litigation purposes. The purpose behind a request is not relevant in considering whether a request is valid. However, it may be considered as one of multiple factors in justifying whether the request may be manifestly unfounded or excessive — for example, if it's clear the person is abusing their rights to further their position, whether in litigation or otherwise. The employer **must** respond within one month of first receiving the request.

The employer provides the information but redacts details about third parties and does not provide information that is covered by legal professional privilege. The person contacts the employer and demands copies of the unredacted original documents in which their personal information is contained. The employer decides that this request is excessive, as the person has already been given the information they are entitled to. They are not entitled to the documents, copies of documents, or information about other people they are requesting. The additional information contained in these documents is not information that relates to the requester.

Remember that a SAR gives a person the right to a copy of their personal information, some of which may be contained in documents. However, it does not necessarily give them the right to obtain documents or copies of documents. This depends on the contents.

What does manifestly unfounded mean?

'Manifestly unfounded' means that:

- the person clearly has no intention to exercise their right of access. For example, they make a request, but then offer to withdraw it in return for some form of benefit from the organisation; or
- the request is clearly malicious and is being used to harass an organisation with no real purpose other than to cause disruption. For example, if a person:
    - explicitly states, in the request itself or in other communications, that they intend to cause disruption;
    - makes unsubstantiated accusations against your organisation or specific employees, which are clearly prompted by malice;

- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to you as part of a campaign (eg once a week), with the intention of causing disruption.

This is not a simple tick-list exercise that automatically means a request is manifestly unfounded. You **should** consider a request in the context in which it is made. If the request appears to be a reasonable and genuine attempt to exercise the right of access, it's unlikely that the request is manifestly unfounded.

While aggressive or abusive language is not acceptable, the use of such language does not automatically make a request manifestly unfounded. You **should** consider all the circumstances of the request and take a reasonable and proportionate approach in deciding whether or not this is a relevant factor.

Example

A person makes a SAR to an online retail company for their personal information. They state that they are making a SAR in accordance with the UK GDPR, and that if the company credits their online account with a specified sum of money, they will withdraw their request. The company is correct to consider the request as manifestly unfounded.

What does 'excessive' mean?

To determine whether a request is 'excessive', you **should** consider if it's clearly or obviously unreasonable. You **should** take into account **all** the circumstances of the request, including:

- the nature of the requested information;
- if it's proportionate when balanced with the burden or costs involved in responding to it;
- the context of the request, and the relationship between you and the person;
- if a refusal to provide the information or even acknowledging if you hold it may cause substantive damage to the person;

- your available resources;
- if the request largely repeats previous requests, a reasonable interval hasn't elapsed, and the person's circumstances haven't changed;
- if it overlaps with other requests made by the same person (although, if it relates to a completely separate set of information, it's unlikely to be excessive); or
- if you have already provided a copy of the same information to the person by alternative means.

A request is not necessarily excessive just because the person requests a large amount of information. You **should** consider all the circumstances of the request.

If it's a large request, you **should** consider asking the person for more information to help you find the information they want, and whether you can make reasonable searches for the information. See Can we clarify the request? and What efforts should we make to find information?

A repeat request may not be excessive if a reasonable amount of time has passed since the last request. When considering if a reasonable interval has elapsed you **should** consider the following:

- The nature of the information — for example, is it particularly sensitive to the requester.
- How often you alter the information — if the information is unlikely to have changed, you may not need to respond to the same request twice. However, if you have changed the information since the last request, you **should** inform the person of this.

Requests about the same issue are not always excessive - it depends on the circumstances. There may be valid reasons for making a request that repeats the substance of a previous one. For example, if the organisation did not handle previous requests properly, or if the response to a previous request revealed new information that the person was not previously aware of – prompting a new request.

However, in other circumstances, a request which repeats the substance of a previous request may be excessive. For example, a request may be excessive if someone makes a new request before you have had the opportunity to address their earlier request – as long as the substance of the new request repeats some of the previous request.

A SAR is not automatically excessive just because the information was previously made available in another way (eg through litigation). However, if a person has already received **exactly the same** information through another method, this may be a factor in deciding whether this exemption applies.

Remember, even where a copy of the personal information you hold has already been disclosed to a person via a separate mechanism, you **must** provide the other supplementary information.

Relevant provisions in the UK GDPR - see Articles 12, 15 and Recitals 58, 63

https://www.legislation.gov.uk/eur/2016/679/contents

Exemptions: can we refuse a SAR if it involves information about other people?

In more detail

What if a SAR involves information about other people?

Personal information can relate to more than one person. Therefore, responding to a SAR may involve providing information that relates to both the requester and another person.

You do not have to provide information in response to a SAR, to the extent that this would reveal information about another person, unless:

- the other person has consented to the disclosure; or
- it is reasonable to disclose the information without their consent.

This is known as the 'rights of others' exemption (and sometimes as the 'third-party data' exemption). You can also rely on this exemption to issue an NCND response if simply confirming that you hold the information would prejudice the exemption.

In this section, we sometimes refer to the other person as a 'third party'.

Example

A person makes a request to their local authority for a copy of information about their noise complaint. The file also contains

information about their neighbour. This requires the authority to consider both the requester's right of access and their neighbour's rights in relation to their own personal information.

If you are dealing with a SAR for information that is also the personal information of a third party, you **must** consider whether either of these factors applies. If the other person consents to you disclosing the information about them, you will not be able to rely on this exemption to withhold it. If there is no consent (or if they refuse to give it), you **must** still decide whether to disclose the information anyway.

What approach can we take?

To help you decide whether to disclose information relating to a third party, you **should** follow the three-step process described below.

Step one — Does the request require disclosing information that identifies another person?

You **should** consider whether you can comply with the request without revealing information that relates to and identifies another person. You **should** take into account the requested information **and** any information you reasonably believe the person making the request may have, or may get access to, that would identify the third party.

Example

Consider the previous example about a person's request for a copy of their noise complaint about their neighbour. Even if the authority redacts the neighbour's name, they are likely to still be identifiable based on information already known to the person making the request.

As you are obliged to provide information rather than documents, you **could** delete names or redact documents if the third party's information does not form part of the requested information.

If you cannot take out the third party's information and still comply with the request, you **should** follow step two below.

Step two — Has the other person provided consent?

You **must** disclose the information if the third party has provided consent. Therefore, you **could** ask relevant third parties for their consent to the disclosure of their personal information in response to a SAR.

However, you are not obliged to ask for consent. Indeed, in some circumstances, it may not be appropriate to do so – for instance, where:

- you don't have contact details for the third party;
- it would potentially disclose personal information of the requester to the third party that they were not already aware of;
- it would be inappropriate for the third party to know that the requester has made a SAR; or
- the third party cannot give their consent freely because there is an imbalance of power between you and them (for example, if they are your employee).

Step three — Is it reasonable to disclose without consent?

In practice, it may sometimes be difficult to get consent from a third party. If you don't have consent, you **must** consider whether it's reasonable to disclose the information about them anyway.

You **must** take into account all the relevant circumstances, including:

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

This is a non-exhaustive list, and ultimately, it's your decision whether to disclose the information to the requester. You **must** make the disclosure if it's reasonable to do so without the third party's consent.

Are there any other relevant factors?

In addition to the factors listed in the DPA, the following points are likely to be relevant when considering whether it's reasonable to disclose information about a third party in response to a SAR.

- **Information generally known to the person making the request.** It's more likely to be reasonable for you to disclose the information if:
    - the requester has previously received the third-party information;
    - the requester already knows the information; or
    - the information is generally available to the public.

  Third-party information about a member of staff (acting in the course of their duties), whom the person making the request knows well through their previous dealings, is more likely to be disclosed than information relating to an anonymous person.

- **Circumstances relating to the person making the request.** The importance of the information to the requester is also a relevant factor. You **should** balance the need to preserve confidentiality for the third party against the requester's right to access their personal information. Depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party withholds consent.
- **Context in which the SAR is made.** You **should** consider the context in which the SAR is made, including the behaviour of the parties and the potential impact of disclosure on those involved. As a controller, you have discretion in deciding on the reasonableness of disclosure in the absence of consent.

What about confidentiality?

Confidentiality is one of the factors you **must** consider when deciding whether to disclose information about another person without their consent. You have a duty of confidence when a person discloses genuinely confidential information (ie information that is not generally available to the public) to you, with the expectation that it remains confidential. This expectation might result from:

- the content and context of the third-party information – for example, if it reveals that the third party is the subject of an ongoing disciplinary investigation; or
- the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence:
    - medical (doctor and patient),
    - employment (employer and employee),
    - legal (solicitor and client),

- financial (bank and customer),
- caring (counsellor and client), and
- trade unions (trade union representative and member).

However, you cannot always assume confidentiality. Here are some examples of why confidentiality may not apply:

- A duty of confidence does not arise merely because a letter is marked "Confidential" (although this marking may indicate an expectation of confidence).
- If the information in such a letter is widely available elsewhere, it may not have the 'necessary quality of confidence'.
- There may be other factors, such as the public interest, which mean that an obligation of confidence does not apply.

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

Does this exemption apply to supplementary information?

Yes — this exemption may apply to any of the information you consider disclosing in response to a SAR, including the supplementary information.

Example

An employee (the requester) is currently subject to disciplinary proceedings based on reports that they are harassing other staff – for example, by using offensive language. The requester makes a SAR for their personal information.

In responding to the SAR, the employer is also required to provide the requester with a copy of the supplementary information. Although this largely corresponds with its privacy information, the employer also needs to provide details about the specific people it has disclosed the employee's personal information to – including, where appropriate, other members of staff.

As the employer previously sought advice from its legal department about the requester's behaviour, it has shared this information with a number of lawyers and paralegals. The employer has concerns about

disclosing the specific identities of these staff members in case this also exposes them to similar harassment by the requester.

The employer applies the rights of others exemption to withhold details about the specific identities of the staff members. However, the employer **must** disclose details about the categories of people it has shared the requester's information with. Therefore, it **must** inform the requester that it has shared the information with its legal department more generally.

What about health, educational and social work information?

If the person requests information that is also the personal information of a health worker, an education worker or a social worker, it's reasonable to disclose information about them without their consent, if the disclosure meets the appropriate 'test'.

For health workers, information meets the 'health data test' if:

- a health record contains the information; and
- the third party is a health professional who:
    - compiled the record,
    - contributed to the record, or
    - was involved in the requester's diagnosis, care or treatment.

A 'health record':

- consists of information concerning health; and
- is made by or on behalf of a health professional (eg a doctor, dentist or nurse) in connection with a person's diagnosis, care or treatment.

For education workers, information meets the 'education data test' if:

- the other person is:
    - an employee of a local authority that maintains a school in England or Wales,
    - a teacher or other employee at a voluntary aided, foundation or foundation special school, an academy school, an alternate provision academy, an independent school or a non-maintained special school in England or Wales,
    - a teacher at a school in Northern Ireland,

    - an employee of the Education Authority in Northern Ireland, or
    - an employee of the Council for Catholic Maintained Schools in Northern Ireland; or
- the other person is an employee at an education authority in Scotland (as defined by the Education (Scotland) Act 1980) in connection with their statutory education functions, and:
    - the information relates to the other person in their capacity as an employee, or
    - the other person supplied the information in their capacity as an employee of an education authority.

For social workers, information meets the 'social work data test' if:

- the third party is:
    - a children's court officer,
    - a person employed by a body in connection with their statutory social work function(s), or
    - a person who provides a similar, non-statutory, social work service (for reward); and
- the information relates to, or was supplied by, the other person in their official capacity (or in connection with a non-statutory social work service).

Example

A person makes a SAR to their local council for a copy of all the information it holds about them. The information it holds includes several social services reports that contain the personal information of the person, a family member and a social worker.

The council employs the social worker in connection with its statutory social work service, and they wrote the reports in their official capacity as a social worker. As such, it is reasonable for the council to provide the social worker's personal information to the requester in response to the SAR.

However, the council **must** either have the consent of the family member or consider whether it is reasonable to disclose their personal information without consent. If the council does not have consent, it is

likely that it needs to consider any duty of confidence owed to the family member before responding to the SAR.

Do we need to respond to the request?

Yes. You **must** respond to the person, whether or not you decide to disclose information about a third party. If the third party gives their consent, or you are satisfied that it's reasonable to disclose it without consent, you **must** provide the information in the same way as any other information you provide in response to the SAR.

If you do not have the third party's consent and you are not satisfied that it's reasonable to disclose their information, then you **should** withhold it. However, you **must** still provide as much of the requested information as you can, without disclosing the third party's identity. Depending on the circumstances, you may be able to provide some information, after editing or redacting it to remove information that identifies the third party.

You **must** be able to justify your decision to disclose or withhold information about another person, so you **should** keep a record of what you decide and why – for example, why you chose not to seek consent or why it was inappropriate to do so in the circumstances.

How do we deal with information that relates to the requester and a deceased person?

The UK GDPR does not apply to a deceased person. Therefore, the rights of others exemption does not apply where the third party is deceased.

The death of a person does not mean that any information about them is freely available to anyone who requests it. Other legal protections may still apply, such as the common law duty of confidentiality. However, in some situations, redacting information about a deceased person may be unnecessary or inappropriate.

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA 2018 - see Section 205 and Schedule 2, paragraphs 16 and 17

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Are there any special cases?

In more detail

Special cases

There are special rules and provisions about SARs and some categories of personal data, including:

- unstructured manual records;
- credit files;
- health information;
- educational information; and
- social work information.

These are all covered in the following sections.

Unstructured manual records

Unstructured manual records relate to information held in a non-automated format which is not, or is not intended to be, part of a 'filing system'.

Data protection law only applies to information held in unstructured manual records if a public authority is processing it. This includes paper records that public authorities do not hold as part of a filing system.

Therefore, public authorities may have to search such information to comply with a SAR.

However, they are not obliged to do so if:

- the request does not contain a description of the unstructured information; or
- the estimated cost of complying with the request would exceed the appropriate maximum.

The 'appropriate maximum' is currently £600 for central government, Parliament and the armed forces, and £450 for all other public authorities.

When estimating the cost of compliance, you **must** only take into account the cost of the following activities:

- Determining whether you hold the information.
- Finding the requested information or records containing the information.
- Retrieving the information or records.
- Extracting the requested information from records.

The biggest cost is likely to be staff time. You **must** rate staff time at £25 per person per hour, regardless of who does the work (including external contractors). This means a limit of 18 or 24 staff hours, depending on whether the £450 or £600 limit applies.

For further information, see the Fees Regulations made under section 12(5) of FOIA. These regulations apply to all public authorities in England, Scotland, Wales and Northern Ireland, for the purposes of estimating the costs of responding to SARs for unstructured manual records.

Personal information held in an unstructured manual record (by a public authority) is also exempt from disclosure if it is about appointments, removals, pay, discipline, superannuation or other personnel matters related to service in:

- any of the armed forces of the Crown;
- any office or employment under the Crown or under any public authority;
- any office or employment, or under any contract for services, in respect of which, power to take action, or to determine or approve the action taken in such matters, is vested in:
    - His Majesty;
    - a Minister of the Crown;
    - the National Assembly for Wales;
    - the Welsh Ministers;
    - a Northern Ireland Minister (within the meaning of FOIA); or
    - an FOI public authority (as defined in FOIA or FOISA).

Relevant provisions in the DPA See Chapter 3, Sections 21 and 24

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Credit files

The DPA has special provisions about access to personal information held by credit reference agencies. Unless otherwise specified by the requester, a SAR to a credit reference agency only applies to information relating to the person's financial standing. Credit reference agencies **must** also inform people of their rights under section 159 of the Consumer Credit Act 1974 when responding to a SAR.

Relevant provisions in the DPA See Chapter 2, Section 13

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Health information

In more detail

What is health information?

The DPA defines information concerning health as personal information about the physical or mental health of a person, including the provision of health care services, which reveals information about their health status.

Relevant provisions in the DPA See section 205(1)

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Can we charge a fee for providing access to health information?

In general, you cannot charge a fee to comply with a SAR for health information. However, if a request is manifestly unfounded or excessive, you may charge a fee to respond. For more information about when you can charge a fee, see Can we charge a fee?

Is health information ever exempt from the right of access?

The exemptions and restrictions that apply to other types of personal information also apply to personal information concerning health. For example, if health information contains personal information about someone other than the requester (such as a family member), you **must** consider the rules about third-party information before disclosing it to the requester.

It's normally reasonable to disclose information that identifies a health professional (eg a doctor, dentist or nurse) carrying out their duties if the

information meets the appropriate test. See Exemptions: can we refuse a SAR if it involves information about other people? for more information.

Some further exemptions and restrictions also apply to health information. In particular, there is a restriction that prevents you from disclosing information that may cause serious harm.

These exemptions and restrictions are explained in detail in the following sections.

Is there an exemption for health information processed by the courts?

Yes. There is an exemption from the right of access for health information if:

- it is processed by a court;
- it is supplied in a report or given to the court as evidence in the course of proceedings where specific court rules apply; and
- in accordance with these specific court rules, the court may withhold the person's information in whole or in part.

The specific court rules which may apply are:

- the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969;
- the Magistrates' Courts (Children and Young Persons) Rules 1992;
- the Family Proceedings Rules (Northern Ireland) 1996;
- the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996;
- the Act of Sederunt (Child Care and Maintenance) Rules 1997;
- the Sheriff Court Adoption Rules 2009;
- the Family Procedure Rules 2010; or
- the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013.

Relevant provisions in the DPA (the exemption) See Schedule 3, paragraph 3

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), 21(1)

http://www.legislation.gov.uk/eur/2016/679/contents

Is health information exempt if disclosure goes against a person's expectations and wishes?

Yes. There is an exemption from the right of access if you receive a request (in exercise of a power conferred by an enactment or rule of law) for health information from someone who:

- has parental responsibility for a person aged under 18 (or 16 in Scotland); or
- is appointed by the court to manage the affairs of a person who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would disclose information that the person:

- provided to you in the expectation that it would not be disclosed to the requester (unless they have since expressly indicated that they no longer have that expectation);
- consented to provide as part of an examination or investigation in the expectation that the information would not be disclosed in this way (unless they have since expressly indicated that they no longer have that expectation); or
- has expressly indicated cannot be disclosed in this way.

Relevant provisions in the DPA (the exemption) See Schedule 3, paragraph 4

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), 21(1)

http://www.legislation.gov.uk/eur/2016/679/contents

Is health information exempt if disclosure may cause serious harm?

Yes. You are exempt from complying with a SAR for health information to the extent that complying with the right of access would likely cause serious harm to the physical or mental health of any person. This is known as the 'serious harm test' for health information.

You can only rely on this exemption to withhold health information if:

- you are a health professional; or
- you are not a health professional but, within the last six months, you have obtained an opinion from the appropriate health professional that

the serious harm test applies (even if you have done this, you still cannot rely on the exemption if it would be reasonable to reconsult the appropriate health professional).

The appropriate health professional is the health professional currently or most recently responsible for the diagnosis, care or treatment of the person in connection with the matter in question. If there is more than one responsible health professional, it means the one who is most suitable to provide an opinion on the matter. If there is no such health professional available, you can appoint a health professional with the necessary experience and qualifications.

See paragraph 2(1) of schedule 3 of the DPA for full details of who is considered the appropriate health professional.

If you are not a health professional, you can only disclose health information in specific circumstances. See the next section, What are the restrictions on disclosing health information?, if you intend to disclose health information.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 5

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

What are the restrictions on disclosing health information?

If you are not a health professional, you **must not** disclose health information in response to a SAR unless:

- you are satisfied that the person it is about has already seen, or knows about, the health information; or
- within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health information is not met. Even if you have done this, you **must** reconsult the appropriate health professional if it would be reasonable to do so.

Example

A person obtains a note from their GP about their absence from work for a number of weeks. The person then provides this information to their employer.

Some years later, the person makes a SAR to their employer for "all the information you hold about my absences from work". The GP's note is therefore within the scope of the SAR. Since the person is already aware of this information, the employer does not need to obtain an opinion from the GP who prepared the note about whether the serious harm test is met.

Health professionals include, for example, registered medical practitioners, dentists and nurses. Section 204 of the DPA gives a full list of the types of professionals that fall within the definition.

If you need to consult with an appropriate health professional in this context, you **could** consider the request to be complex. If so, you can extend the time limit to respond by a further two months. See When is a request complex? and Can we extend the time limit for a response? for further information.

When you receive a SAR that relates to health information, you **should** make all reasonable efforts to obtain an opinion from the appropriate health professional as soon as possible. If you are unable to obtain an opinion within the time limit for responding to the request, you **must** withhold the health information.

You **should** document all the efforts you make to consult with the appropriate health professional. You **should** be able to provide evidence of your efforts to the ICO, if asked to. In particular, you **should** be able to show that you have made all reasonable steps to contact the health professional.

Because of the nature of this exemption (and the potential nature of the information in question), you may not be able to tell the person why you have extended the time limit to respond or why you have withheld the information. This will depend on the circumstances and the nature of the requested information. In general, you **should** be as transparent as possible. See What do we need to do if we refuse to comply with a request?

Relevant provisions in the DPA (the exemption) - see Section 204(1) and Schedule 3, paragraph 6

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

What about requests for health information from a third party?

A third party can make a SAR on behalf of a person, as long as they are entitled to act on the person's behalf. For example, a solicitor may make a SAR on behalf of a client. The third party is responsible for providing you with evidence of this. See Can a request be made on behalf of someone else? for more information.

If you have a genuine concern that the third party has requested excessive information, or you have reasonable grounds to believe that the person whom the information is about does not understand how much information will be disclosed to the third party, you **could** contact the person first to make them aware of your concerns. If the person agrees, you **could** send the response directly to the person rather than to the third party. The person may then choose to share the information with the third party after reviewing it.

If you are unable to contact the person, you **should** provide the requested information to the third party (if you are satisfied that they are authorised to act on the person's behalf). If the person has specifically asked that you do not contact them directly, then you **should** only correspond with the third party authorised to act on their behalf.

A SAR is not appropriate in situations where the third party's interests are not aligned with the person the information is about — for example, an insurance company needing to access health information to assess a claim. In such circumstances, if a person consents, an insurer can apply to the person's GP, who may produce a tailored medical report, providing only the information the insurer needs, under the provisions of the Access to Medical Reports Act 1988 (AMRA). The AMRA does not lie within our remit, but we refer to it here for completeness.

Remember that the definition of personal information only relates to a living person, so a SAR cannot be used to obtain information about a deceased person. In certain circumstances, a third party may be able to access this information under the Access to Health Records Act 1990 or the Access to Health Records (Northern Ireland) Order 1993.

Education information

In more detail

What is education information?

The DPA defines education information as personal information that:

- consists of information forming part of an educational record; and
- is not information concerning health.

The definition of 'educational record' in the DPA differs between England and Wales, Scotland and Northern Ireland. In general, it has a broad meaning and includes most information about current and past pupils that is processed by or on behalf of a school. The definition applies to nearly all schools, including maintained schools, independent schools and academies.

Most of the personal information a school holds about a particular pupil is likely within the pupil's educational record. However, some of the information may fall outside the educational record. For example, this includes:

- information a parent of another child gives about the pupil; and
- information a teacher keeps solely for their own use.

Relevant provisions in the DPA 2018 - see Schedule 3, paragraphs 13-17

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

How can people access education information?

There are two distinct rights to information that schools hold about pupils:

- The pupil's right of access under article 15 of the UK GDPR.

- A parent's right to access their child's educational record.
    - In England and Wales, this right only applies to maintained schools.
    - In Northern Ireland, this right applies to all grant-aided schools — but not independent schools, academies or free schools.
    - In Scotland, this right applies to all schools.

Relevant legislation

- The Education (Pupil Information) (England) Regulations 2005
- The Pupil Information (Wales) Regulations 2011
- Education (Pupil Records) Regulations (Northern Ireland) 1998
- The Pupils' Educational Records (Scotland) Regulations 2003

It's important to be aware of a parent's separate right to access their child's educational records. The law on this right is outside our remit, but we refer to it here for completeness.

The information you provide may differ depending on which right applies. Remember that:

- the SAR provisions provide a right of access to personal information in general; and
- the relevant education regulations only allow a parent to access their child's educational record.

The two rights also have different time limits for compliance:

- You **must** comply with a SAR within one month (or within three months, if the request is complex or you receive multiple requests from the same person at the same time).
- You are required to respond to a parent's right of access to their child's educational records within 15 school days. You will need to consider your obligations under the relevant legislation.

Unlike a parent's right to access their child's educational record, it is the pupil's right to make a SAR. Parents can only submit a SAR for information about their child if the child is not competent to act on their own behalf or has given their consent. For guidance about deciding whether a child is able

to make their own SAR, see What about requests for information about children?

If it's not clear whether a requester has parental responsibility for the child or is acting on their behalf, you need to clarify this before responding to the SAR. If the school is in England, Wales or Northern Ireland, the school is responsible for dealing with the SAR. If the school is in Scotland, the relevant education authority or the proprietor of an independent school is responsible for dealing with the SAR.

Can we charge a fee for providing access to education information?

In general, you cannot charge a fee to comply with a SAR for education information. However, if a request is manifestly unfounded or excessive, you may charge a fee to respond. For more information about when you can charge a fee, see Can we charge a fee?

How long do we have to comply if we receive a SAR in school holidays?

There are no special rules that allow you to extend the time for dealing with a SAR that you receive during school holidays. If you receive a SAR when the school is closed, you **must** comply within the normal time for responding. See How long do we have to comply? for more information.

Is education information ever exempt from a SAR?

The exemptions and restrictions that apply to other types of personal information also apply to education information. For example, if an educational record contains personal information relating to someone other than the requester (such as a family member), you **must** consider the rules about third-party information before disclosing it to the requester. It's normally reasonable to disclose information that identifies a teacher. See Exemptions: can we refuse a SAR if it involves information about other people? for more information.

Some further exemptions and restrictions apply to education information. These are explained in the next sections.

Is there an exemption for education information processed by the courts?

You are exempt from providing education information in response to a SAR if:

- it is processed by a court;
- it is supplied in a report or given to the court as evidence in the course of proceedings where specific court rules apply; and
- in accordance with these specific court rules, the court may withhold the person's information in whole or in part.

The specific court rules which may apply are:

- the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969;
- the Magistrates' Courts (Children and Young Persons) Rules 1992;
- the Family Proceedings Rules (Northern Ireland) 1996;
- the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996;
- the Act of Sederunt (Child Care and Maintenance) Rules 1997;
- the Sheriff Court Adoption Rules 2009;
- the Family Procedure Rules 2010; and
- the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013.

However, this does not mean that you can withhold all information just because there are ongoing legal proceedings.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 18

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), 21(1)

http://www.legislation.gov.uk/eur/2016/679/contents

Is education information exempt if disclosure may cause serious harm?

Yes. In most circumstances, you are exempt from providing education information in response to a SAR to the extent that complying with the request would likely cause serious harm to the physical or mental health of any person. This is known as the 'serious harm test' for education information. However, this exemption does not apply to independent schools in Scotland.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 19

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

Is there a restriction if you are an education authority in Scotland?

If you are an education authority in Scotland (as defined by the Education (Scotland) Act 1980), there is a restriction in place where a question arises of whether you are required to disclose education information in response to a SAR. The restriction applies if:

- you believe that the relevant information came from the Principal Reporter (as defined by the Children's Hearings (Scotland) Act 2011) in the course of their statutory duties; and
- the person whom the information is about is not entitled to receive it from the Principal Reporter.

You **must** inform the Principal Reporter of the issue within 14 days of the question arising.

You are not permitted to disclose the education information in response to the request if the Principal Reporter has told you they think the serious harm test for education information is met.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 20

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

Social work information

In more detail

What is social work information?

The DPA defines social work information as personal information which:

- paragraph 8 of schedule 3 of the DPA applies to (generally this includes particular bodies processing personal information in connection with their social services functions or to provide social care); but
- is not education or health information.

Relevant provisions in the DPA - see Schedule 3, paragraph 7-8

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Can we charge a fee for providing access to social work information?

In general, you cannot charge a fee to comply with a SAR for social work information. However, if a request is manifestly unfounded or excessive, you may charge a fee to respond. For more information about when you can charge a fee, see Can we charge a fee?

Is social work information ever exempt from subject access?

The exemptions and restrictions that apply to other types of personal information also apply to social work information. For example, if social work information contains personal information relating to someone other than the requester (such as a family member), you **must** consider the rules about third-party information before disclosing it to the requester. However, it's

normally reasonable to disclose information that identifies a professional, such as a social worker, carrying out their duties. See What if a SAR involves information about other people? for more information.

Some further exemptions and restrictions apply to social work information. These are explained in the next sections.

Is there an exemption for social work information processed by the courts?

You are exempt from providing social work information if:

- it is processed by a court;
- it is supplied in a report or given to the court as evidence in the course of proceedings where specific court rules apply; and
- in accordance with these specific court rules, the court may withhold the person's information in whole or in part.

The specific court rules which may apply are:

- the Magistrates' Courts (Children and Young Persons) Rules (Northern Ireland) 1969;
- the Magistrates' Courts (Children and Young Persons) Rules 1992;
- the Family Proceedings Rules (Northern Ireland) 1996;
- the Magistrates' Courts (Children (Northern Ireland) Order 1995) Rules (Northern Ireland) 1996;
- the Act of Sederunt (Child Care and Maintenance) Rules 1997;
- the Sheriff Court Adoption Rules 2009;
- the Family Procedure Rules 2010; and
- the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013.

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), 21(1)

http://www.legislation.gov.uk/eur/2016/679/contents

Is social work information exempt if disclosure goes against a person's expectations and wishes?

Yes. There is an exemption from the right of access if you receive a request (in the exercise of a power conferred by an enactment or rule of law) for social work information about a person from someone:

- with parental responsibility for a person aged under 18 (or 16 in Scotland); or
- appointed by a court to manage the affairs of a person who is incapable of managing their own affairs.

But the exemption only applies to the extent that complying with the request would disclose information that the person:

- provided in the expectation that it would not be disclosed to the requester (unless they have since expressly indicated that they no longer have that expectation);
- consented to provide as part of an examination or investigation, in the expectation that the information would not be disclosed in this way (unless they have since expressly indicated that they no longer have that expectation); or
- has expressly indicated cannot be disclosed in this way.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 10

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), 21(1)

https://www.legislation.gov.uk/eur/2016/679/contents

Is social work information exempt if disclosure may cause serious harm?

Yes. You are exempt from complying with a SAR for social work information to the extent that complying with the request would likely compromise social work duties because it would likely cause serious harm to the physical or mental health of any person. This is known as the 'serious harm test' for social work information.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 11

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) See Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

Is there a restriction if you are a local authority in Scotland?

Yes. The restriction applies if you:

- are a local authority in Scotland (as defined by the Social Work (Scotland) Act 1968); and
- receive a request for social work information.

This restriction means that you cannot disclose social work information in response to a SAR if:

- there is a question of whether you need to respond to the SAR;
- the information came from the Principal Reporter (as defined by the Children's Hearings (Scotland) Act 2011) in the course of their statutory duties; and
- the person whom the information is about is not entitled to receive it from the Principal Reporter.

You **must** inform the Principal Reporter of the issue within 14 days of the question arising.

You are not permitted to disclose the social work information in response to the SAR if the Principal Reporter has told you they think the serious harm test for social work information is met.

Relevant provisions in the DPA (the exemption) - see Schedule 3, paragraph 12

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Relevant provisions in the UK GDPR (the exempt provisions) - see Articles 15(1)-(3)

http://www.legislation.gov.uk/eur/2016/679/contents

Can the right of access be enforced?

In more detail

What enforcement powers does the ICO have?

Anyone has the right to make a complaint to the ICO about an infringement of the data protection legislation involving their personal information – for example, if a controller fails to comply with a SAR.

In appropriate cases, we may take action against a controller or processor if they fail to comply with data protection law. For example, we can issue a controller or processor with a:

- warning;
- reprimand;
- information notice;
- assessment notice;
- interview order;
- enforcement notice; or
- Monetary penalty notice (fine).

We will exercise these enforcement powers in accordance with our Regulatory Action Framework.

A processor is not responsible for complying with a SAR, but the controller and processor must have a contract in place to cover SARs. For more information, read our guidance on contracts and liabilities between controllers and processors.

Can a court order be used to enforce a SAR?

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply. The court will decide whether to make such an order on a case-by-case basis.

Can a person be awarded compensation?

If a person suffers damage or distress because you have breached their data protection rights — including by failing to comply with a SAR — they are entitled to claim compensation from you. Only the courts can enforce their right to compensation. However, they may seek to settle their claim with you directly before starting court proceedings.

You will not be liable to pay compensation if you can prove that you are not responsible in any way for the event that causes the damage.

Is it a criminal offence to force a person to make a SAR?

In certain circumstances, it is a criminal offence to require a person to make a SAR for certain information. For more information, see Can we force a person to make a SAR?

Is it a criminal offence to destroy and conceal information?

Yes. It is a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR is entitled to receive.

It is a defence to prove that:

- the alteration, defacing, blocking, erasure, destruction or concealment of the information would have happened regardless of whether the person made a SAR; or
- you acted in the reasonable belief that the person making the SAR was not entitled to receive the information requested.

Relevant provisions in the UK GDPR - see Articles 77, 82 and Recitals 141, 146

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Part 6 (which explains our enforcement powers) and Section 184

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Further reading

Can we force a person to make a SAR?

In more detail

What is an enforced SAR?

An enforced SAR is when someone:

- requires a person to make a SAR to gain access to certain information about them (eg their convictions, cautions or health records); and then
- uses this information – for example, as supporting evidence for a job application or before approving a contract for insurance.

Forcing a person to make a SAR in such circumstances is a criminal offence.

Example

A person applies for a position as a waiter at a restaurant, but they are told that they cannot be offered the position until they provide a copy of their criminal record. The employer states that they need to make a SAR to gain this information and they will only be appointed if they supply it. The employer is likely to have committed a criminal offence.

Example

A person makes an application to an insurance provider for private health insurance. The provider agrees to insure the person but explains that, as a condition of the insurance, the person needs to make and provide the results of a SAR for their medical records. The insurance company is likely to have committed an offence.

More appropriate ways are available for accessing relevant information – for example, through the criminal disclosure regime for criminal records or the Access to Medical Reports Act 1988 for health records.

When does it apply?

It is a criminal offence to require a person to provide you with a copy of or access to a relevant record in connection with:

- your recruitment of an employee;
- a person's continued employment by you; or
- a contract for the provision of services to you.

It is also a criminal offence to require another person to make and provide the results of a SAR for a relevant record if:

- you are involved in providing goods, facilities or services to the public or a section of the public; and
- it is a condition of providing a person with goods, facilities or services, or allowing them to do voluntary work.

Example

A person applies to do voluntary work with a charity. The charity explains that the person can work for them, but they will first need to exercise their subject access rights and provide the charity with their criminal record before they can start. The charity is likely to have committed an offence.

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Section 184, paragraphs 1 and 2

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

What is a relevant record?

A 'relevant record' is a record which has been, or will be, obtained by a person exercising their right of access **and**:

- is a health record;

- contains information about a conviction or caution; or
- contains information about a statutory function of that person.

A 'health record':

- consists of information concerning health; and
- has been made by or on behalf of a health professional (eg a doctor, dentist or nurse) in connection with the diagnosis, care or treatment of the person it relates to.

'Information about a conviction or caution':

- consists of information processed by the police, the Director General of the National Crime Agency or the Secretary of State; and
- relates to a conviction or to a caution issued against a person.

'Information relating to a statutory function':

- consists of information processed in connection with certain statutory functions of:
    - the Secretary of State,
    - the Department for Communities in Northern Ireland,
    - the Department of Justice in Northern Ireland,
    - the Scottish Ministers, or
    - the Disclosure and Barring Service or the independent reviewer appointed under section 12 of the Age of Criminal Responsibility (Scotland) Act 2019; and
- relates to:
    - prisons and prisoners,
    - the detention of a person aged under 18 who was convicted of murder or another serious offence,
    - social security contributions and benefits (eg statutory sick pay or accident insurance), and the administration of such matters,
    - jobseeker's allowance and related schemes,
    - employment and support allowance on grounds of incapacity or disability,
    - universal credit (England, Scotland and Wales only),
    - criminal records history, and
    - the vetting and barring of those who wish to work with children or vulnerable adults.

Example

A person applies for a job as an office receptionist. The employer offers the person the job, on the condition that they exercise their subject access rights and provide the employer with details of their benefits entitlements during a period of unemployment. The employer is likely to have committed an offence.

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Section 184, Paragraph 6 and Schedule 18

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

What does 'require' mean?

If you 'require' a person to do something, you ask, order, demand or command them to take a specific action. This means that you instruct them to do something and make it clear, either directly or indirectly, that you expect them to take this action.

You may also make it clear that if they do not take the specified action, this may result in a negative outcome for them, or they may be less likely to achieve an objective. For example, you suggest or imply that a particular action is necessary to achieve a particular purpose or objective, or that the action is likely to help them in some way to achieve the objective or avoid an undesirable outcome.

If you are an employer, you are in a position of power over your employees and over people who want you to employ them. So, if you require an employee or job seeker to do something, they may feel obliged to take the action or believe that if they don't, they will be negatively affected. This is the case whether or not the person is happy to take the action in question.

You have required another person to make a SAR if you:

- know that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request; or
- are reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request.

A person may also feel obliged to make a SAR if they would:

- be left in a detrimental position by not making a SAR; or
- miss out on an incentive by not making a SAR.

There may also be other circumstances in which you require someone to make a SAR.

Example

A person applies for a job and is successful. Their potential employer informs them that they will be given the job whether or not they make a SAR for their criminal record. However, the potential employer explains that if they do not make a SAR, their annual salary will be lower than the advertised rate. This would obviously leave the person in a detrimental position if they did not make a SAR.

The offence is the act of requiring a person to make a SAR. The requirement is enough – whether you have committed an offence is not dependent on, for example, withdrawing an offer of employment or the provision of goods, facilities or services.

Asking a person to make a SAR means you have required them to do so. This still applies, even if you give a choice between them making a SAR and you accessing the information through an appropriate and lawful channel.

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Section 184, paragraph 5

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Are there any exemptions?

It is not a criminal offence for you to require a person to make a SAR if you can prove that:

- it was required or authorised by another piece of legislation, a rule of law or by order of a court or tribunal; or
- it can be justified as being in the public interest.

Given the importance of the right of access as a core right within the UK GDPR, you need an extremely strong justification that enforced subject access is in the public interest, supported by clear, specific and convincing evidence. This may be difficult to achieve, as clear public policy and laws exist about criminal record checking and access to medical records.

You cannot use the defence that an enforced SAR is in the public interest if your basis is that the public interest relates to the prevention or detection of crime.

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Section 184, Paragraphs 3 and 4

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

What are the penalties?

A person who requires someone to make a SAR may be committing a criminal offence. This is an offence which can be heard either by a magistrates' court or a crown court, in England, Wales and Northern Ireland. In Scotland, it will be heard in a sheriff court.

Committing such an offence in England and Wales can carry an unlimited fine, while in Scotland the fine can be unlimited if heard under solemn procedure or £10,000 for less serious offences under summary procedure. In Northern Ireland, the maximum fine if convicted under a summary offence is £5,000, or if convicted on indictment, the maximum fine is unlimited (unless expressly limited by statute).

Relevant provisions in the UK GDPR - see Article 15 and Recital 63

http://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the DPA - see Section 196

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted