


About this detailed guidance	2
What is the right of access?	3
How should we prepare?	6
How do we recognise a subject access request (SAR)?	9
What should we consider when responding to a request?	17
How do we find and retrieve the relevant information?	29
How should we supply information to the requester?	34
When can we refuse to comply with a request?	40
Information about other individuals	44
What other exemptions are there?	50
Are there any special cases?	62
Health data	64
Education data	69
Social work data	73
Can the right of access be enforced?	76
Can we force an individual to make a SAR?	78

About this detailed guidance

We are currently experiencing problems with guidance downloads, which means that you may not be able to access the PDF of this guidance using the "download options" button. [You can access a PDF version of this guidance at this link](#) .

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. [Guidance tailored towards small organisations](#) can be found in our data protection advice for small organisations. This guidance does not specifically cover the right of access under Parts 3 and 4 of the Data Protection Act 2018. However, some of the guidance contains practical examples and advice which will still be relevant.

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.

Contents

- [What is the right of access?](#)
- [How should we prepare?](#)
- [How do we recognise a subject access request \(SAR\)?](#)
- [What should we consider when responding to a request?](#)
- [How do we find and retrieve the relevant information?](#)
- [How should we supply information to the requester?](#)
- [When can we refuse to comply with a request?](#)
- [What should we do if the request involves information about other individuals?](#)
- [What other exemptions are there?](#)
- [Are there any special cases?](#)
- [Health data](#)
- [Education data](#)
- [Social work data](#)
- [Can the right of access be enforced?](#)
- [Can we force an individual to make a SAR?](#)

What is the right of access?

In more detail

- [What is the right of access and why is it important?](#)
- [What is an individual entitled to?](#)
- [What other information is an individual entitled to?](#)
- [Are individuals only entitled to their own personal data?](#)
- [Who is responsible for responding to a request?](#)

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

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

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

What is an individual entitled to?

Individuals have the right to obtain the following from a controller:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information.

In most cases, you can confirm whether you are processing their personal data in general terms. However, this will depend on the nature of the request. If the request is for a specific piece of information, you should be able to confirm or deny whether you are processing this information.

What other information is an individual entitled to?

Individuals have the right to receive the following information (which largely corresponds with the information that you should provide in a privacy notice):

- your purposes for processing;
- categories of personal data you're processing;
- recipients or categories of recipient you have or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- your retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- the individual's right to request rectification, erasure or restriction or to object to processing;
- the individual's right to lodge a complaint with the Information Commissioner's Office (ICO);

- information about the source of the data, if you did not obtain it directly from the individual;
- whether or not you use automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- the safeguards you have provided where personal data has or will be transferred to a third country or international organisation.

When responding to a subject access request (SAR), you must remember to supply this information in addition to a copy of the personal data itself. If you provide this information in your privacy notice, you can include a link to or a copy of your privacy notice. Please see our guidance on [the right to be informed](#) for further information.

Are individuals only entitled to their own personal data?

Yes. Under the right of access, an individual is only entitled to their own personal data. They are not entitled to information relating to other people, unless:

- their data also relates to other individuals (see [‘What should we do if the request involves information about other individuals?’](#)); or
- they are exercising another individual’s right of access on their behalf (see [‘Can a request be made on behalf of someone?’](#)).

Before you can respond to a SAR, you need to decide whether the information you hold is personal data and, if so, who it relates to.

The UK General Data Protection Regulation (UK GDPR) says that, for information to be personal data, it must relate to a living person who is identifiable from that information (directly or indirectly). The context in which you hold information, and the way you use it, can have a bearing on whether it relates to an individual and therefore if it is the individual’s personal data.

In most cases, it is obvious whether the information is personal data, but we have produced [guidance on what is personal data](#) to help you decide if it is unclear.

The same information may be the personal data of two (or more) individuals. An exemption may apply, if responding to a SAR involves providing information that relates to both the individual making the request and to another individual. Please see [‘What should we do if the request involves information about other individuals?’](#) for more information.

Who is responsible for responding to a request?

Controllers are responsible for complying with SARs, not processors. If you use a processor, you need to have contractual arrangements in place to guarantee that you can deal with SARs properly, irrespective of whether they are sent to you or the processor. The processor must help you meet your obligations for SARs and you should make this clear in the agreement between your two parties. Please read [our guidance on contracts between controllers and processors](#) for more information.

In some cases the processor may hold personal data on your behalf (and you, as controller, do not hold that data). If so, you should be able to require the processor to search for this data and, if necessary, give you a copy. However, it is your responsibility, as controller, to decide whether individuals need to provide

clarification, or if a request is manifestly excessive, for example.

If you are a joint controller, you need to have a transparent arrangement in place with your fellow joint controller(s) which sets out how you deal with SARs. You may choose to specify a central point of contact for individuals. However, individuals must still be able to exercise their rights against each controller. It is also good practice to make each joint controller aware of every SAR.

If you are unsure whether you are a controller, joint controller or processor, please read [our guidance on controllers and processors](#).

Example

An employer is reviewing staffing and pay, which involves collecting information from and 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 should instruct the processor to retrieve any personal data that relates to the member of staff.

Further Reading

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

Further reading

- [What is personal data?](#)
- [Right to be informed](#)
- [Controllers and processors](#)
- [Contracts and liabilities between controllers and processors](#)

How should we prepare?

In more detail

- [Why is it important to prepare for the right of access?](#)
- [What steps should we take?](#)
- [What about our information management systems?](#)

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

Whether or not you receive SARs on a regular basis, it is important that you are prepared and take a proactive approach. This helps you to respond to requests effectively and in a timely manner. It also helps you to:

- comply with your legal obligations under the UK GDPR and Data Protection Act 2018 (DPA 2018) – 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 individuals about the personal data you hold about them;
- enable customers, employees and others to verify that the information you hold about them is accurate, and to tell you if it is not;
- improve confidence in your information handling practices; and
- increase the transparency of what you do with individuals' data.

What steps should we take?

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

- type of personal data you are processing;
- 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 could prepare:

- **Awareness** – Make information available about how individuals can make a SAR (eg on your website, in leaflets or in your privacy notice).
- **Training** – Provide general training to all staff to recognise a SAR. Provide more detailed training on handling SARs to relevant staff, dependent on job role.
- **Guidance** – Create a dedicated data protection page for staff on your intranet with links to SAR policies and procedures.
- **Request handling staff** – Appoint a specific person or central team that is responsible for responding to requests. Ensure that more than one member of staff knows how to process a SAR, so you have resilience against absence.

- **Asset registers** – Maintain information asset registers which state where and how you store personal data. This helps speed up the process of locating the required information to respond to SARs.
- **Checklists** – Produce a standard checklist that staff can use to ensure you take a consistent approach to SARs.
- **Logs** - Maintain a log of SARs you have received and update it to monitor progress. The log may include copies of information you've supplied in response to a SAR, together with copies of any material you've withheld and why.
- **Retention and deletion policies** – Have documented retention and deletion policies for the personal data you process. This helps to ensure that you don't keep information longer than you need to and therefore potentially reduces the amount of information you need to review when responding to a SAR.
- **Security** – Have measures in place to securely send information. For example, by using a trusted courier or having a system to check email addresses and review responses before sending.

What about our information management systems?

You will find it difficult to deal with SARs effectively without adequate information management systems and procedures. Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs. They should enable you to easily locate and extract personal data and allow you to redact third-party data where necessary.

If you are implementing a new information management system, you need to take a data protection “by design and default” approach and ensure that the system facilitates 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 assist you with your accountability and documentation obligations.

Further Reading

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

External link

Further reading

- [Data protection by design and default](#)
- [Accountability and governance](#)
- [Documentation](#)

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

In more detail

- [What is a subject access request \(SAR\)?](#)
- [Are there any formal requirements?](#)
- [Should we provide a standard form for individuals to make a request?](#)
- [Can a request be made via social media?](#)
- [Can a request be made on behalf of someone?](#)
- [Do we have to respond to requests made via a third party online portal?](#)
- [What about requests for information about children or young people?](#)
- [What should we do if a request mentions Freedom of Information?](#)
- [Can we deal with a request in our normal course of business?](#)

What is a subject access request (SAR)?

A SAR is a request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR.

Are there any formal requirements?

No. The UK GDPR does not set out formal requirements for a valid request. Therefore, an individual 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.

A request does not have to include the phrases 'subject access request', 'right of access' or 'Article 15 of the UK GDPR'. It just needs to be clear that the individual is asking for their own personal data. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) or the Freedom of Information (Scotland) Act 2002 (FOISA).

This presents a challenge as any of your employees could receive a valid request and you have a legal responsibility to identify and handle any request from an individual correctly. Therefore, you may need to consider which of your staff need specific training to identify a request. In particular, staff members who regularly interact with the public should be able to identify a SAR and know the next steps.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. If you receive a request verbally, you are still likely to need to contact the individual in writing in order to confirm their identity. You may also wish to check with the requester that you have understood their request, as this can help avoid later disputes. For more information please see ['Can we ask for ID?'](#)

You should also note that individuals do not have to tell you their reason for making the request or what they intend to do with the information. However, it may help you to find the relevant information if they do explain the purpose of the request.

Should we provide a standard form for individuals to make a request?

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

Recital 59 of the UK GDPR recommends that organisations “provide means for requests to be made electronically, especially where personal data is processed by electronic means”. You should therefore consider designing a subject access form that individuals can complete and submit to you electronically.

However, you should note that a SAR is equally valid whether an individual submits it to you by letter, email or verbally. You must therefore make it clear that it is not compulsory to use the form and simply invite individuals to do so.

Can individuals make a request via social media?

Yes. Individuals may make a SAR using any social media site where your organisation has a presence. Although this might not be the most effective way to deliver the request, there is nothing to prevent an individual doing so.

You should therefore recognise the potential for individuals to make SARs via your social media channels and ensure that you take reasonable and proportionate steps to respond effectively to these requests.

In most circumstances, it will not be appropriate to use social media to supply information in response to a SAR for information security reasons. Instead you should ask for an alternative delivery address for the response. For further details, please see [‘How do we provide the information securely?’](#).

Can an individual make a request on behalf of someone?

Yes. An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. The UK GDPR does not prevent this, however you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party’s responsibility to provide you with evidence of this. For example by providing a written authority, signed by the individual, 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 behalf of her mother and explains that her mother does not feel comfortable making the request herself, as she does not understand data protection. The building society is rightly cautious about giving customer information to a third party, as the information they hold is mostly financial. If the daughter can provide written authority from her mother giving her permission to make a SAR on her behalf, the building society would be happy to comply.

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

You can accept electronically signed letters of authority as valid evidence, provided that you are satisfied that the third party is authorised to act on the individual's behalf. If the third party provides additional details with their request (eg the individual's address and account number), this may help to satisfy the validity of the request.

There are also other mechanisms that may allow a third party to make a SAR on behalf of an individual, 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 is reasonable to assume that an attorney with authority to manage the property and affairs of an individual has the appropriate authority to make a SAR on their behalf.

If there is no evidence that a third party is authorised to act on behalf of an individual, you are not required to comply with the SAR. However, you should still respond to them explaining this.

In most cases, provided you are satisfied that the third party has the appropriate authority, you should respond directly to that third party. However, if you think an individual may not understand the nature of the information you are disclosing, and in particular you are concerned about disclosing excessive information, you should contact the individual first to make them aware of your concerns. If the individual agrees, you may send the response directly to them rather than to the third party. The individual may then choose to share the information with the third party after reviewing it. If you cannot contact the individual, you should provide the requested information to the third party (as long as you are satisfied that they are authorised to act on the individual's behalf). If you are processing health data, please see ['What about requests for health data from a third party?'](#)

There are cases where an individual does not have the mental capacity to manage their own affairs. There are no specific provisions which enable a third party to exercise subject access rights on behalf of such an individual 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 in the Adults with Incapacity (Scotland) Act 2000. However, as mentioned above, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual has the appropriate authority to make a SAR on their behalf. The same applies to a person appointed to make decisions about such matters in:

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

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

You may receive a SAR made on behalf of an individual through an online portal, for example a third party that provides services to assist individuals in exercising their rights.

To determine whether you must comply with such a request, you need to consider if you:

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

You are not obliged to take proactive steps to discover that a SAR has been made. Therefore, if you cannot view a SAR without paying a fee or signing up to a service, you have not ‘received’ the SAR and are not obliged to respond.

You should note that it is the portal’s responsibility to provide evidence that it has appropriate authority to act on the individual’s behalf. Mere reference to the terms and conditions of its service are unlikely to be sufficient for this purpose (see [‘Can a request be made on behalf of someone?’](#) above). The portal should provide this evidence when it makes the request (ie in the same way as other third parties).

When responding to a SAR, you are also not obliged to pay a fee or sign up to any third party service. If you are in this position you should instead provide the information directly to the individual.

If you have concerns that the individual has not authorised the information to be uploaded to the portal, you should contact the individual before you respond.

In some cases you may be unable to contact the individual directly, for example if you do not have their address details or are otherwise not satisfied with the ID information provided. If this is the case, you should contact the third party portal to advise them that you will not respond to the request until they have met each of the above requirements, and provided evidence that the individual has agreed to the information being uploaded to the portal. Until then, you have not received a valid SAR and the time limit does not start until you receive it.

If you have concerns about supplying the information via the portal for any reason, including security concerns, you should contact the individual first to make them aware. If the individual agrees, you should send the response directly to them rather than to the portal.

What about requests for information about children or young people?

The right to access information you hold about a child is the child’s right rather than anyone’s 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 should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident that the child can understand their rights, you should usually respond directly to the child. You may allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

If a child is competent, they may authorise someone else – other than a parent or guardian – to make a SAR on their behalf (please see the earlier section, ['Can a request be made on behalf of someone?'](#)). This could be an adult or a representative such as a child advocacy service, charity or solicitor. However, you should not consider a child to be competent if it is evident that they are acting against their own best interests. For example, if a child authorises a third party to make a SAR on their behalf, but you have reasonable concerns that the third party is pressurising the child to make the SAR.

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

If the child makes a SAR, or authorises another person to make a SAR on their behalf, what matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to understand what they are asking for and what they will receive or to understand the consequences of authorising someone to act on their behalf; and
- the nature of the personal data.

If a parent or guardian, or someone authorised by the child, makes a SAR on the child's behalf, you should also take into account:

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

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This does not apply in England, Wales or Northern Ireland but would be a reasonable starting point.

If you have regular contact with the child (which is likely to be the case for education or childcare settings), you should be in a position to assess the child's competence.

If you do not have regular contact with the child (this is likely to be the case with banks and building societies), you should take a common sense approach. For example, if the child is aged 12 or over, you correspond directly with them and they are likely to be aware of the nature of information you process about them. It is reasonable to conclude that the child is competent to make a SAR.

However, if you process sensitive information about a child or if you hold information they may not be aware of, you should make stronger efforts to check competence.

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

It is not uncommon for a request to mistakenly state that it is a freedom of information (FOI) request. If, in fact, it relates to the requester's personal data, you must treat it as a SAR.

Example

A local authority receives a letter from a council tax payer requesting a copy of any information the authority holds about a dispute over his eligibility for a discount. The letter states it is a 'freedom of information request'. It is clear that the request concerns the individual's own personal data and the local authority should treat it as a subject access request.

You may be more likely to receive a SAR in the form of an FOI request if your organisation is a public authority for the purposes of FOIA, FOISA, the Environmental Information Regulations 2004 (EIR) or the Environmental Information (Scotland) Regulations 2004 (EIRs). However, whether or not your organisation is a public authority, you must deal with the request appropriately. This depends on whether it relates only to the requester's personal data or to other information as well.

If it is clear that the requester is just asking for their own personal data, but they have cited FOIA/FOISA, you should follow certain actions:

- 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 individual to verify their identity.
- If your organisation is a public authority, the requested personal data is, in fact, exempt from disclosure under FOIA/FOISA or the EIR/EIRs. Strictly speaking, you should issue a formal refusal notice saying so. In practice, we do not expect you to do this if you are dealing with the request as a SAR. However, if you are a public authority in Scotland, you need to follow guidance issued by the [Scottish Information Commissioner](#).
- It is good practice for public authorities to clarify within 20 working days (the time limit for responding to FOI requests) 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 data and to other information, you should treat this as two requests:

- one for the requester's personal data, made under the UK GDPR; and
- another for the remaining information, made under FOIA/FOISA, or the EIR/EIRs.

It is important to consider the requested information under the right legislation. This is because a disclosure under FOIA/FOISA or the EIR/EIRs is to the world at large – not just the requester. If you mistakenly disclose personal data under FOIA/FOISA or the EIR/EIRs, this could lead to a personal data breach.

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

It is important to draw a practical distinction between formal requests for information and routine verbal enquiries and correspondence that you can deal with in the 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 an individual requests a high volume of information and you need to conduct a time-consuming search of your records in order to comply with the request.

For example, if an individual requests copies of letters which you have sent to them previously, it is unlikely that you need to deal with this as a formal SAR. You should consider these enquiries on a case by case basis. However, you should not use your normal business processes to restrict or delay an individual's right of access to 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 and it is not necessary to deal with the request as a SAR.

Example

A customer phones about a query they have about their account. You can discuss the matter on the call with the customer, including the personal data you process about them, in accordance with your normal business processes provided that you have verified the individual's identity.

Further Reading

 [Relevant provisions in the UK GDPR - see Articles 15 and Recitals 59, 63](#) 

External link

Further reading

- [Children and the UK GDPR](#)
- [Guide to freedom of information](#)
- [Guide to the Environmental Information Regulations](#)

What should we consider when responding to a request?

In more detail

- [How long do we have to comply?](#)
- [Can we extend the time for a response?](#)
- [When is a request complex?](#)
- [Can we clarify the request?](#)
- [Can we charge a fee?](#)
- [Do we need to make reasonable adjustments for disabled people?](#)
- [Can we ask for ID?](#)
- [What if the individual mentions other rights?](#)
- [How should we deal with bulk requests?](#)
- [Do we still need to comply if the requester dies before the response is provided?](#)

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 requested to confirm the requester's identity (see '[Can we ask for ID?](#)'); or
- a fee (only in certain circumstances – see '[Can we charge a fee?](#)').

You should calculate the time limit from the day you receive the request, fee or other requested information (whether it is a working day or not) until the corresponding calendar date in the next month.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

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

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always 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 individual – this can include other types of requests relating to individuals’ rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.

You should calculate the extension as three months from the original start date, ie the day you receive the request, fee or other requested information.

If you decide that it is necessary to extend the time limit by two months, you must let the individual know within one month of receiving their request and explain why.

When is a request complex?

Whether a request is complex depends upon the specific circumstances of each case. What may be complex for one controller may not be for another – the size and resources of an organisation are likely to be relevant factors. Therefore, you need to take into account your specific circumstances and the particular request when determining whether the request is complex.

The following are examples of factors that may, in some circumstances, add to the complexity of a request. However, you need to be able to demonstrate why the request is complex in the particular circumstances.

- Technical difficulties in retrieving the information – for example if data 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.
- Any specialist work involved in obtaining the information or communicating it in an intelligible form.
- Clarifying potential confidentiality issues around the disclosure of sensitive medical information to an authorised third party.
- Needing to obtain specialist legal advice. If you routinely obtain legal advice, it is unlikely to be complex.
- Searching large volumes of unstructured manual records (only applicable to public authorities).

Requests that involve a large volume of information may add to the complexity of a request. However, a request is not complex solely because the individual requests a large amount of information.

Also, a request is not complex just because you have to rely on a processor to provide the information you need in order to respond.

Can we clarify the request?

Yes. If you process a large amount of information about an individual, you may ask them to specify the information or processing activities their request relates to before responding to the request. The time limit for responding to the request is paused until you receive clarification. This is referred to as ‘stopping the clock’.

This means that you do not need to provide the individual with a copy of the information, or any of the supplementary information that you cannot reasonably provide, unless you have obtained clarification.

You should not seek clarification on a blanket basis. You should only seek it if:

- it is genuinely required in order to respond to a SAR; and

- you process a large amount of information about the individual.

It is up to you whether you request clarification of a request – as long as you are satisfied that you hold a large amount of information, and it is not clear what information the individual is requesting. You are not required to do so, and you may choose to perform a reasonable search instead. Please see [‘What efforts should we make to find information?’](#) for more information on what is a reasonable search and to what extent you must search for information.

Whether you hold a large amount of information about an individual will, to an extent, depend on your organisation’s size and the resources available to you. The volume of information held may be less of an issue for a big organisation with significant dedicated resources available to respond to a SAR. However a smaller organisation, processing the same amount of information but with fewer and less sophisticated resources at their disposal, is more likely to be able to argue that they hold a large amount of information.

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

Essentially, it is unlikely to be reasonable or necessary to seek clarification if you process a large volume of information in relation to the individual but can obtain and provide the requested information quickly and easily.

You can ask the requester to provide additional details about the information they want to receive, such as the context in which you may have processed their information and the likely dates of when you processed it. However, you cannot force an individual to narrow the scope of their request, as they are still entitled to ask for ‘all the information you hold’ about them. If an individual responds to you and either repeats their request or refuses to provide any additional information, you must still comply with their request by making reasonable searches for the information.

Example

An individual writes to their local GP practice and asks for ‘all the information you hold about me.’ The practice employed the individual as a receptionist for a number of years and they are currently registered as a patient. As the individual is now a carer for their elderly parent, the practice also holds personal data relating to them within their parent’s file.

The practice is of the view that they process a large volume of information about the individual. However, it is not clear from the request what information the individual wants. If the practice performs a reasonable search of their records, they will be able to provide some of the information held about the individual, but would need to perform a much more extensive search in order to provide all the information they hold.

In these circumstances, it is reasonable to ask the individual to clarify their request. The practice should explain to the individual that whilst they are entitled to request all the information held about them, the practice is only required to conduct a reasonable search of their records. This means that the individual may only receive some of the information held about them. It is important to explain to the individual that by clarifying their request, the practice will be able to focus their searches on locating

the specific information that the individual wants.

The individual could clarify the request by, for example, asking for details of their employment from 1993 to 2008; their medical records which relate to an accident in 2018; and 'everything else you hold about me'. The practice should focus their searches on the first two enquiries and then perform a reasonable search for the rest of the information.

It is likely that you will be able to provide certain information without seeking clarification, although this may depend on the circumstances. For example, in many cases you will be able to provide a general confirmation that you hold personal data about the individual. In addition, you should be able to provide some of the supplementary information set out in Article 15(1) of the UK GDPR, in particular details of:

- the individual's right to request rectification, erasure or restriction, or to object to processing; and
- the individual's right to lodge a complaint with the ICO or another supervisory authority.

If you can reasonably provide any of the supplementary information without clarification, you should provide it within one month. If your privacy notice already contains this supplementary information, it is sufficient to provide the individual with a link to it.

Example

A supermarket receives a SAR from a long-standing employee for all the data the supermarket holds about them. The employee has recently had a complaint made about them by another employee.

The supermarket asks the employee if they only want information relating to the complaint or if the employee is looking for information between particular dates. The supermarket also asks if the employee would like information unrelated to their employment, eg information linked to the employee's reward account as a customer.

Until the supermarket receives clarification, they will be unable to perform a reasonable search, or provide a copy of the information, as they do not know what information the request relates to. Furthermore, they will not be able to provide some of the supplementary information, including the purposes of processing, categories of personal data and the retention period. However, they can provide some information, including details of the individual's right to lodge a complaint with the ICO. The supermarket sends the individual a copy of their privacy notice as it already contains these details.

You should ensure the process of seeking and obtaining clarification is quick and easy for the individual, and as far as possible you should provide advice and assistance to help them clarify their request. You should explain that the clock stops from the date that you request clarification and will resume once the individual responds. You should also specify whether the individual needs to reply by a certain time.

Where possible, you should contact the individual in the same format they made the request, eg if they have emailed the SAR, you should email them to ask for clarification.

If you receive a request where it is genuinely unclear whether an individual is making a SAR, then the time limit does not begin until you have clarified whether the individual is making a SAR, and what personal data they are requesting. In such cases, you are expected to contact the individual as quickly as possible (eg by phone or email where this is appropriate). You should keep a record of any conversation with an individual about the scope of their request and the date when you sought and received any further explanation.

In all circumstances, you should explain to the individual 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 requester clarifies the request and will resume on the date you receive clarification from the requester. You should calculate the timescale as follows:

- When you receive a request, you should 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 from the same day. You will have one month to reply which means you should respond 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 provides you with clarification on 18 May, the timing will resume on that date.

The clock was therefore stopped from 15 May until 18 May. This means that you can extend the original one month deadline by three days and you should provide a response by or on 17 June.

You should request clarification promptly and without undue delay after receiving the request. This will enable you to focus on searching for the information the individual wants at the earliest possible stage and ensure that you have sufficient 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 individual 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 is unable to comply by the deadline as they did not leave themselves enough time to search for the information after obtaining clarification.

If it only becomes apparent during the course of a search that you need further information in order to respond, you should record why it was not possible to request clarification at an earlier stage.

If you seek clarification and receive it on the same day, the clock will not stop – you should calculate the 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, by close of business at 5:00pm, you cannot stop the clock and extend the time limit by one day. The original deadline of one month will still apply.

The clock only stops where you seek 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

An individual requests a copy of their medical records from 5 February 2001 until 9 August 2007. They specifically ask that the practice forwards the records by email. However, due to security concerns, it is not possible to email the records but the practice is able to provide the individual with remote access to their information. The practice decides to ask the individual whether they are happy with this. The clock does not stop when they ask for clarification and the usual time limit of one month still applies. Since the time limit is not paused whilst they wait for a response, the practice should begin searching for information as soon as possible.

Where 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 an individual might have difficulty in providing additional details within a specified timeframe, you should try and accommodate the individual as much as possible. For example where complex issues are involved or when there are accessibility issues.

If you need to request both clarification and proof of ID, you should do so as soon as possible. You should not wait until the individual provides clarification before asking for ID documents, unless there is a risk of disclosing personal data to the individual before you have checked their identity. You must not deter or delay individuals from exercising their subject access rights.

You may be able to extend the time limit by two months if the request is complex or the individual 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. For further information on complex requests, see the earlier section, [‘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
- an individual requests further copies of their data following a request.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request. For information about when a request may be manifestly unfounded or excessive, please see [‘When can we refuse to comply with a request?’](#).

When determining a reasonable fee, you can take into account 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 individual, including contacting the individual to inform them that you hold the requested information (even if you are not providing the information).

As there may be substantial overlap across these activities, you should ensure that the fee you charge is reasonable and that you do not ‘double-charge’ the individual. For example, the process of locating, retrieving and extracting information may be performed in one action, depending on the context in which you hold the information and the nature of the search you perform.

A reasonable fee may include the costs of:

- photocopying, printing, postage and any other costs involved in transferring the information to the individual (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 2018 allows for the Secretary of State to specify limits on the fees that controllers may charge to deal with a manifestly unfounded or excessive request by way of regulations.

However, at present there are no regulations in place. As such, it is your responsibility as a controller to ensure that you charge a reasonable rate.

You should ensure that you charge fees in a reasonable, proportionate and consistent manner. Therefore, it is good practice to establish an unbiased set of criteria for charging fees which explains:

- the circumstances in which you charge a fee;
- your standard charges (including a costs breakdown where possible eg the costs per A4 photocopy); and

- how you calculate the fee – explaining the costs you take into account including the costs of staff time.

Your criteria should be clear, concise and accessible. You should make this criteria available on request, but you do not need to publish it online.

When requesting a fee you should explain the costs to the individual. You should include a copy of this criteria in your request for a fee and explain any charge that is unclear (see '[Do we need to explain the information supplied?](#)'). You should also advise the individual if you intend to charge a fee even if you are not providing the information.

You must be able to justify the costs you have charged in the event that an individual complains to the ICO.

If you choose to charge a fee, you do not need to comply with the request until you have received the fee. However you should request the fee promptly and at the latest within one month of receiving the SAR. This means you must request the fee as soon as possible. You must not unnecessarily delay requesting it until you are nearing the end of the one month time limit.

If you are unable to request the fee as soon as reasonably possible, you should document the reasons why this was not possible and be able to provide your reasons to the ICO, if asked. You should not ask for a fee as a way of extending the period of time you have to respond to the request.

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

Do we need to make reasonable adjustments for disabled people?

Yes. Some disabled people may experience communication difficulties, and may therefore have difficulty making a SAR. You have a legal duty to make reasonable adjustments if they wish to make a request. If the request is not straightforward, you should document it in an accessible format and send it to the disabled person to confirm the details of the request.

What is a reasonable adjustment will depend on the specific needs of the individual. Before responding to a SAR you should talk to the person to find out how best to meet their needs. This may be by providing the response in a particular format that is accessible to the person, such as large print, audio formats, email or Braille. If an individual thinks you have failed to make a reasonable adjustment, they can make a claim under the Equality Act 2010 or the Disability Discrimination Act 1995 (NI). Further information about your legal obligations and 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 data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that:

- you know the identity of the requester (or the person the request is made on behalf of); and
- the data you hold relates to the individual in question (eg when an individual has similar identifying details to another person).

You can ask for enough information to judge whether the requester (or the person the request is made on

behalf of) is the person that the data is about. The key point is that you must be reasonable and proportionate about what you ask for. You should not request more information if the requester's identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

Example

You have received a written SAR from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your 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 you know the person making the request.

You should also not request formal identification documents unless necessary. First you should think about other reasonable and proportionate ways you can verify an individual's identity. You may already have verification measures in place which you can use, for example a username and password.

However, you should not assume that on every occasion the requester is who they say they are. In some cases, it is reasonable to ask the requester to verify their identity before sending them 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 site for some time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, before responding to the request it is reasonable to gather further information, which could simply be to ask the customer to confirm other account details, such as a customer reference number.

The level of checks you make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual 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. The potential risk to the former patient of sending their health records to the wrong person is high, so the practice is right to be cautious. They

could ask the requester to provide more information, such as a passport or driving licence or another document confirming their identity.

When you receive a SAR, you should determine what information you require to verify identity and explain to the individual what they need to provide. You will sometimes need to request more information than usual, depending on the circumstances. You should not request ID documents if you are aware that it might not be sufficient, or if you believe that you will need to request further proof at a later stage.

Example

A local authority is aware that a father and son living at the same address have the same name – John Smith. When they receive a request from a John Smith at this address, it is reasonable for them to request proof of identity that reveals the requester’s date of birth, even if they would not usually ask for ID which confirms date of birth.

The timescale for responding to a SAR does not begin until you have received the requested information. However, you should request ID documents promptly. This means you must request the documents as soon as possible. You must not unnecessarily delay requesting the documents until the end of the one month time limit.

If the requested information is not sufficient and you need to take further steps to verify the individual’s identity, the timescale for responding begins once you have completed the verification. However, this only applies in exceptional circumstances, and generally the timescale for responding to a SAR begins once you receive the requested information. Please see [‘How long do we have to comply?’](#) for more information about timescales.

For example, the ID documents may not be sufficient if an individual supplies information which raises doubts about their identity, or you have reasonable concerns that the ID is fraudulent or the individual has obtained it fraudulently.

Example

After a company has received a SAR, they ask for proof of ID. However, when this is provided the name on the ID document is different from the name they have on record for the individual concerned, and 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 individual’s identity by asking for alternative ID or evidence that explains why the names are different. The timescale does not begin until they have received sufficient information to verify the requester’s identity.

Whilst you do not need to keep copies of ID documents, it might be helpful to keep a note of:

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

Before supplying any information in response to a SAR, you should also check that you have the correct details to send the response (eg the correct email address).

What if the individual mentions other rights?

If you have received a number of simultaneous requests from an individual, which relate to other rights under the UK GDPR (eg the right to erasure and the right to data portability), you should deal with each request separately. You should refer to our published guidance relevant to each of the rights they want to exercise. However, certain steps will be common to each request, for example:

- establishing proof of ID;
- ensuring that a third party has authority to act on behalf of the data subject; and
- determining what information the request relates to.

If you receive a number of requests from an individual relating to their UK GDPR rights, you may be able to extend the time limit to respond by a further two months. See ['Can we extend the time for a response?'](#) for further information.

How should we deal with bulk requests?

Depending on the size of your organisation and the nature of your business, you may receive a number of SARs in a short period of time. In the financial services sector, for example, it is not uncommon for claims management companies to make bulk requests on behalf of multiple individuals.

You must consider each SAR within a bulk request individually and respond appropriately. The ICO acknowledges the potential resource implications of this duty but recommends you bear in mind 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 an individual making a SAR.
- The purpose for which an individual makes a SAR does not affect its validity, or your duty to respond to it (unless it is a manifestly unfounded or excessive request).
- If a third party makes a request on behalf of an individual, the third party's behaviour should not be taken into account in determining whether a request is manifestly unfounded or excessive.
- You must satisfy yourself that the third party is authorised to make the request.
- You must satisfy yourself as to the identity of the individual concerned.
- You must respond to the request even if you hold no information about the individual (your response may obviously be very brief in such cases).

In considering a complaint about a SAR, the ICO will have regard to the volume of requests received by an organisation and the steps they have taken to ensure they deal with requests appropriately, even when facing a high volume of similar requests. The organisation's size and resources are also likely to be relevant factors. As we explain in ['Can the right of access be enforced?'](#), the ICO has discretion as to whether to take



enforcement action, and we would not take such action if it is clearly unreasonable to do so.

Do we still need to comply if the individual dies before we provide a response?

No. The definition of personal data covers information which relates to a living individual. If you receive a SAR, but are aware that the individual has died before you have provided the response, you are not obliged to respond to the request because the data ceases to be personal data once the individual has died.

It is important to note that this does not mean that from the moment of a person's death, any information relating to them is freely available to anyone requesting access to that information. You need to consider other legal rules protecting a deceased person's information, such as the common law duty of confidentiality.

Further Reading

 [Relevant provisions in the UK GDPR - see Articles 12, 15 and Recitals 58, 59 63, 64](#) 

External link

How do we find and retrieve the relevant information?

In more detail

- [What efforts should we make to find information?](#)
- [What about electronic records that aren't easily available?](#)
- [What about archived information and back-up records?](#)
- [What about deleted information?](#)
- [What about information contained in emails?](#)
- [What about information stored in different locations?](#)
- [What about information stored on personal computer equipment?](#)
- [What about other records?](#)
- [What about personal data in big datasets?](#)
- [Can we amend or delete data following receipt of a SAR?](#)

What efforts should we make to find information?

The UK GDPR places a high expectation on you to provide information in response to a SAR. You should 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 must consider:

- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

The burden of proof is on you to be able to justify why a search is unreasonable or disproportionate.

Even where searching for certain information may be unreasonable or disproportionate, you must still search for any other information within the scope of a request. You should also consider whether further information from the individual will help you find the information they have requested. Please see the previous section for more information about clarifying a request.

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 data. For more information please 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 is very difficult to truly erase all electronic records, you may hold data that you do not have ready access to and

that requires technical expertise to retrieve.

You are likely to have removed information from your 'live' systems in a number of different ways, by:

- archiving it to storage;
- copying it to back-up files; or
- deleting it.

Each of these is discussed in further detail below.

What about archived information and back-up records?

You may archive or backup information for a number of reasons. For instance, under Article 32 you must be able to restore availability and access to personal data in the event of an incident. Please read our [guidance on security](#) for more information.

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

Search mechanisms for electronic archive and back-up systems might not be as sophisticated as those for 'live' 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 data 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 longer than you need it. You should have defined retention periods setting out how long you keep archived or backed-up data. Please 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. The ICO's view is that, if you delete personal data 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 must go to such efforts to respond to a SAR.

The ICO will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously 'deleted' personal data 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.

For more information please see our [guidance on deleting personal data](#).

What about information contained in emails?

The contents of emails you store on your computer systems are a form of electronic record to which the general principles above apply. For the avoidance of doubt, you should not regard the contents of an email as deleted merely because a user has moved it to their 'Deleted items' folder.

It may be particularly difficult to find information related to a SAR if it is contained in archived emails that you have removed from your 'live' systems. Nevertheless, the right of access is not limited to personal data that is easy for you to provide. You may, of course, ask the requester to give you some context that would help you find what they want, if you process a large amount of information about them.

It can sometimes be difficult to determine whether an email contains an individual's personal data. This depends on the contents of the email, the context of the information it contains, and what it is being used for. Ultimately it is for you to determine whether any of the information in the email is the individual's personal data. However, you should remember:

- The right of access only applies to the individual's personal data contained in the email. This means you may need to disclose some or all of the email to comply with the SAR.
- Just because the contents of the email are about a business matter, this does not mean that it is not the individual's personal data. This depends on the content of the email and whether it relates to the individual.
- Just because the individual receives the email, does not mean that the whole content of the email is their personal data. Again, the context of the information and what it is being used for is key to deciding this. However, their name and e-mail address is their personal data and you should disclose this information to them.

Example

An employee makes a SAR for all of the information you hold about them. During your search for their personal data, you find 2000 emails which the employee is 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 the employee's personal data.

You do not have to provide the employee with a copy of each email (with the personal information of third parties redacted). Since the only personal data which relates to them is their name and email address, it is sufficient to advise them that you identified their name and email address on 2000 emails and disclose to them the name contained on those emails, eg John Smith, and the email address contained on those emails, eg [\[email protected\]](#). Alternatively you could provide one email with other details redacted as a sample of the 2000 emails you hold. You should also clearly explain to the individual why this is the only information they are entitled to under the UK GDPR, but remember to provide them with supplementary information concerning the processing, eg retention periods for the emails.

However, if any of the content within the email relates to the individual, you should provide them with a copy of the email itself, redacted if necessary.

For further information on this, see our guidance on ['What is personal data?'](#).

What about information we store in different locations?

The right of access applies irrespective of whether the personal data you process is stored in one location

or in many different locations. Consolidating disparate data stores may assist you, not just for subject access but in other ways. However, whether this is appropriate for you depends on your circumstances.

What about information stored on personal computer equipment?

You are only obliged to provide personal data in response to a SAR if you are a controller for that data. In most cases, therefore, you do not have to supply personal data if someone else is storing it on their computer systems rather than your own (the exception being where that person is a processor). However, this may not be the case if the requester's personal data is stored on equipment belonging to your staff (such as smartphones or home computers) or in private email accounts or private instant messaging applications.

It is good practice to have a policy restricting the circumstances in which staff may hold information about customers, contacts or other employees on their own devices, in private email accounts or on private instant messaging applications. Some organisations enable staff to access their systems remotely (eg via a secure website), but most are likely to prohibit the holding of personal data on equipment the organisation does not control. Nevertheless, if you do permit staff to hold personal data on their own devices, they may be processing that data on your behalf, in which case it is within scope if you receive a SAR. The purpose for which you hold the information, and its context, is likely to be relevant. We do not expect you to instruct staff to search their private emails, personal devices or private instant messaging applications in response to a SAR, unless you have a good reason to believe they are holding relevant personal data.

What about other records?

If you hold information about the requester in non-electronic form (eg in paper files or on microfiche records), you need to decide whether it is covered by the right of access. You need to make a similar decision if you have removed electronic records from your live systems and archived them in non-electronic form.

Whether the information in hard-copy records is personal data accessible via the right of access 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 data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

However, under the DPA 2018, personal data held in unstructured manual records processed 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 please see ['Unstructured manual records'](#).

What about personal data in big datasets?

The volume and variety of big data, coupled with the complexity of data analytics, could 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 data from a range of data sources, including unstructured data, this can pose difficulties when producing all of the data you hold on one individual. This can be further complicated if you make use of observed data or inferred data - data that an individual does not provide to you directly. For example, if you generate insights about an individual's behaviour based on their use of your service, where this data is identified or identifiable (directly or indirectly) then it is personal data and subject to the right of access.

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

- adequate metadata;
- the ability to query your data to find all the information you have on an individual; and
- knowledge of whether the data you process has been truly anonymised, or whether it can still be linked to an individual.

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




It is our view that a SAR relates to the data you held at the time you received the request. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it is reasonable for you to supply the information you hold when you respond, even if this is different to what you held when you received the request.

However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under the DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure.

Further Reading

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

Further reading

- [Security](#)
- [Storage Limitation](#)
- [Deleting personal data](#) 
- [Bring your own device \(BYOD\)](#) 
- [Big data, artificial intelligence, machine learning and data protection](#) 

How should we supply information to the requester?

In more detail

- [What information must we supply?](#)
- [How do we decide what information to supply?](#)
- [In what format should we provide the information?](#)
- [What is a commonly used electronic format?](#)
- [Do we need to provide remote access?](#)
- [Can we provide the information verbally?](#)
- [How do we provide the information securely?](#)
- [What if we have also received a data portability request?](#)
- [Do we need to explain the information supplied?](#)

What information must we supply?

The focus of a SAR is usually a copy of the requester's personal data. However, you should remember that the right of access also entitles an individual to other supplementary information (eg the purposes of processing). For a full list of the other information that you must provide please see ['What other information is an individual entitled to?'](#).

This information might be contained in the copy of the personal data you supply. However, if it is not, you must remember to supply this information in addition to a copy of the personal data itself.

How do we decide what information to supply?

Documents (including draft documents), or files may contain a mixture of information that is the requester's personal data, personal data about other people and information that is not personal data at all. This means that sometimes you need to consider each document within a file separately, and even the content of a particular document, to assess the information they contain.

It may be easier (and more helpful) to give a requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it is their personal data. This is an appropriate approach where none of the information is particularly sensitive, contentious or refers to third-party individuals.

In what format should we provide the information?

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

How you do this, and the format you use, depends upon how the requester submitted their request (ie electronically or otherwise):

- If the individual submitted the SAR electronically (eg by email or via social media), you must provide a copy in a commonly used electronic format. You may 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 individual submitted the SAR 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. However, where the information is sensitive, you should ensure that you transfer it to the requester using an appropriately secure method. Please see [‘How do we provide the information securely?’](#) for further details.

Remember that the onus is on you to provide the information to the individual (or their appointed representative). An individual should not have to take action to receive the information (eg by collecting it from your premises), unless they agree to do so.

The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents containing their personal data. You may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out of the relevant information from your computer systems. While it is reasonable to supply a transcript if it exists, we do not expect controllers 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”. However, this means the format in which you supply the requester with their personal data. When determining what format to use, you should consider both the circumstances of the particular request and whether the individual has the ability to access the data you provide in that format.

You should note that the UK GDPR does not require individuals to take any specific action in order to access the data you provide in response to a SAR. You should not expect them to download software, particularly because:

- it may involve individuals having to buy that software;
- depending on the source, it may pose a security risk to those individuals; and
- it is not providing them with ‘direct access’ to their personal data.

Example

An individual makes a subject access request for their personal data. The organisation provides a copy of this data using what they consider to be a commonly used electronic format.

When the individual receives the files, some of them are in a proprietary format and the individual does not have the software package needed to access these files. The organisation considers that they have provided the data in a “commonly used” format due to the availability of that software package.

However, as the UK GDPR does not require individuals to purchase specific software packages merely to

access a copy of their data, the organisation has not fulfilled their obligations to provide a copy as the individual cannot access it.

Therefore, it is good practice to establish with the individual their preferred format, prior to fulfilling their request.

However, if you were to send the individual their information in an encrypted format, and then separately send them a secure code that they can use to access the encrypted information, you will have provided them with direct access to their data.

Alternatives can also include allowing the individual to access their data remotely and download a copy in an appropriate format. See ['Do we need to provide remote access?'](#) for more information.

Do we need to provide remote access?

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

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

You should note, however, that although you provided the individual with access to their personal data, it does not necessarily mean that you provided them with a copy of their data. This depends on whether they are able to download a copy of the requested information. If an individual can download a copy of their personal data in a commonly used electronic format, then this satisfies the requirement to provide a copy, as long as the individual does not object to the format.

Can we provide the information verbally?

Yes. If an individual asks, you can provide the response to their SAR verbally, provided that you have confirmed their identity by other means. You should keep a record of:

- the date the individual made their request;
- the date you responded;
- details of who provided the information; and
- what 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 are responsible for taking all reasonable steps to ensure its security. Whilst there are many different ways to send the requested information to the individual, 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:

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

For more on this see the [‘How should we prepare?’](#) section above.

The method you use to provide the information to the individual will, in part, be guided by any request they have made about what format they would like to receive it (see [In what format should we provide the information?](#) above).

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

If this is not possible, but you are seeking to provide the information electronically, you may wish to consider providing it in an encrypted form, followed up by sending the passphrase to the individual separately (eg via email). This depends on the nature and sensitivity of the information (in particular if it is special category or criminal offence data).

If the individual asks for you to provide the information in hard copy, in many circumstances the postal service is a secure method of sending the information. However, depending on the nature and sensitivity of the information, you may need to consider sending it by special delivery or via a courier service.

Providing remote access to a secure system can be one method to ensure you provide the information securely. You should however note that you need to apply appropriate technical measures to this system so that both it and any information it holds are secure. A good baseline may be the security measures you already apply to your existing systems. (See [Do we need to provide remote access?](#) above).

Please 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 implement encryption effectively.

What if we have also received a data portability request?

If an individual makes a SAR and a request for data portability at the same time, you need to consider what information comes under the scope of which request.

An easy way of considering this is to remember that:

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

Also, whilst 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 individuals the right to receive personal data 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 data directly to another controller.

Therefore, the required format for providing the information depends on which right applies to the data in question.

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 why the individual may have difficulty understanding it.

The UK GDPR requires that the following information is provided to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language:

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

This means that this information should:

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

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

For more information about how to provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, please see our [guidance on the right to be informed](#).

You are expected to give the individual additional information to aid their understanding, if the requested personal data is not in a form that they can easily understand. However, this is not meant to be onerous and you are not expected to translate information or decipher unintelligible written notes.

Example

An individual makes a request for their personal data. 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 this 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 it is good practice to do so, you are not required to decipher the poorly written notes, as the UK GDPR does not require you to make information legible.

Example

You receive a SAR from someone with poor English comprehension skills. You send a response which can be understood by the average person but they ask you to translate the information you sent them into French. In these circumstances, you are not required to do this, even if the person who receives the data cannot understand all of it. However, it is good practice for you to help individuals understand the information you hold about them.

Further Reading

 [Relevant provisions in the UK GDPR - see Articles 12, 15, 20 and Recitals 58, 63, 68](#) 

External link

Further reading

- [Right to data portability](#)
- [Right to be informed](#)

When can we refuse to comply with a request?

In more detail

- [Can we refuse to comply with a request?](#)
- [What does manifestly unfounded mean?](#)
- [What does manifestly excessive mean?](#)
- [What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?](#)
- [What are exemptions and how do they work?](#)
- [What should we do if we refuse to comply with a request?](#)

Can we refuse to comply with a request?

Yes. If an exemption applies, you can refuse to comply with a SAR (wholly or partly). Not all exemptions apply in the same way and you should look at each exemption carefully to see how it applies to a particular request.

You can also refuse to comply with a SAR if it is:

- manifestly unfounded; or
- manifestly excessive.

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual:
 - explicitly states, in the request itself or in other communications, that they intend to cause disruption;
 - makes unsubstantiated accusations against you 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 must consider a request in the context in which it is made. If the individual genuinely wants to exercise their rights, it is unlikely that the request is manifestly unfounded.

Whilst aggressive or abusive language is not acceptable, the use of such language does not necessarily

make a request manifestly unfounded.

Example

An individual makes a subject access request to an online retail company for their personal data. They state that they are making a SAR in accordance with the UK GDPR and that if the company credits the individual's 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 manifestly excessive mean?

To determine whether a request is manifestly excessive you need to consider whether it is clearly or obviously unreasonable. You should base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request.

This will mean taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship between you and the individual;
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual;
- your available resources;
- whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a completely separate set of information it is unlikely to be excessive).

A request is not necessarily excessive just because the individual requests a large amount of information. As stated above, you must consider all the circumstances of the request. You should also consider asking the individual for more information to help you locate the information they want and whether you can make reasonable searches for the information. Please see ['Can we clarify the request?'](#) and ['What efforts should we make to find information?'](#)

You should consider the following when deciding whether a reasonable interval has elapsed:

- the nature of the data – this could include whether it is particularly sensitive; and
- how often you alter the data – if it's unlikely that the information has changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request, you should inform the individual of this.

What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?

You must take the following into account when determining whether a request is manifestly unfounded or excessive:

- consider each request individually – you should not have a blanket policy;
- do not presume that a request is manifestly unfounded or excessive just because an individual has previously submitted a manifestly unfounded or excessive request;
- the inclusion of the word “manifestly” means there must be an obvious or clear quality to unfoundedness/excessiveness; and
- ensure you have strong justifications for why you consider a request to be manifestly unfounded or excessive, which you can clearly demonstrate to the individual and the ICO.

What are exemptions and how do they work?

The UK GDPR and DPA 2018 recognise that, in some circumstances, you might have a legitimate reason for not complying with a SAR, so there are a number of exemptions from the right of access. Where an exemption applies to the facts of a particular request, you may refuse to provide all or some of the requested information, depending on the circumstances.

Not all of 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 data in question, eg information contained in a confidential reference. Others apply because disclosure of the information is likely to prejudice your purpose, ie it would have a damaging or detrimental effect on what you are doing.

If an exemption does apply, sometimes you are obliged to rely on it (for instance, if complying with UK GDPR would break another law), but sometimes you can choose whether to or not.

You should not routinely rely on exemptions or apply them in a blanket fashion, and should consider each one on a case-by-case basis.

In line with the accountability principle, you should justify and document your reasons for relying on an exemption so you can demonstrate your compliance.

The following sections look at the exemptions most likely to occur in practice.

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

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

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

If you believe a request is manifestly unfounded or excessive, you must be able to demonstrate this to the individual. Where an exemption applies, the reasons you give to an individual for not complying with a request may depend upon the particular case. For example, if telling an individual 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.

Further Reading

 [Relevant provisions in the UK GDPR - see Articles 12, 15 and Recitals 58, 63](#) 

Information about other individuals

In more detail

- [What is the basic rule?](#)
- [What approach should we take?](#)
- [What about confidentiality?](#)
- [What about health, educational and social work data?](#)
- [Are there any other relevant factors?](#)
- [Do we need to respond to the request?](#)

What is the basic rule?

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

Example

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

There is an exemption in the DPA 2018 that says you do not have to comply with a SAR, if doing so means disclosing information which identifies another individual, except where:

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

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

What approach should we take?

To help you decide whether to disclose information relating to a third party, follow the three-step process described below. You may also find it helpful to read our guidance on ['Access to information held in complaint files'](#). Whilst it is FOI and EIR guidance, it also covers SARs.

Step one – Does the request require disclosing information that identifies another individual?

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

Example

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

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

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

Step two – Has the other individual provided consent?

In practice, the clearest basis for justifying the disclosure of third-party information in response to a SAR is that the third party has given their consent. It is therefore good practice, where possible, to ask relevant third parties for their consent to the disclosure of their personal data 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 data of the requester to the third party that they were not already aware of; or
- it would be inappropriate for the third party to know that the requester has made a SAR.

Step three – Is it reasonable to disclose without consent?

In practice, it may sometimes be difficult to get third-party consent; for example, the third party might refuse or be difficult to find. If so, you must consider whether it is reasonable to disclose the information about the other individual anyway.

The DPA 2018 says that 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 taken by you to try to get the third party's consent;

- whether the third-party individual is capable of giving consent; and
- any stated refusal of consent by the third-party individual.

This is a non-exhaustive list, and ultimately it is for you to make this decision, taking these factors into account, along with the context of the information.

What about confidentiality?

Confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where an individual 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 data. For example, if it reveals that the third party is the subject of an ongoing disciplinary investigation; or
- from 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).
 - Trade Unions (trade union representative and member).

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

What about health, educational and social work data?

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

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

- a health record contains the information; and
- the third-party individual 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 data concerning health; and
- is made by or on behalf of a health professional (eg a doctor, dentist or nurse) in connection with an individual's diagnosis, care or treatment.

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

- the other individual 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 individual 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, or was supplied by the other individual in their capacity as an employee of an education authority.

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

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

Example

An individual makes a subject access request to their local council for a copy of all the information it holds on them. The information held includes several social services reports. The reports contain the personal data of the individual, 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 data to the requester in response to the subject access request. However, the council must either have the consent of the family member, or consider whether it is reasonable to disclose their personal data without consent. If the council does not have consent, it is likely that it needs to reconcile the individual's right of access in respect of any duty of confidence owed to the family member.

Are there any other relevant factors?

In addition to the factors listed in the DPA 2018, the following points are likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

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

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

- **Circumstances relating to the individual making the request.** The importance of the information to the requester is also a relevant factor. You need to weigh the need to preserve confidentiality for a third party against the requester's right to access information about their life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party withholds consent.

Do we need to respond to the request?

Yes. You need to respond to the requester whether or not you decide to disclose information about a third party. If the third party gives their consent, or if you are satisfied that it is reasonable to disclose it without consent, you should 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 is reasonable to disclose the third-party information, then you should withhold it. However, you are still obliged to communicate as much of the requested information as you can, without disclosing the third-party's identity. Depending on the circumstances, it may be possible to provide some information, having edited or 'redacted' it to remove information that identifies the third-party individual.

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

Further Reading

 [Relevant provisions in the UK GDPR - see Article 15 and Recital 63](#) 

External link

 [Relevant provisions in the DPA 2018 - see Part 7, section 205 and schedule 2, Part 3, Paragraphs 16 and 17](#) 

External link

Further reading

- [Personal data of both the requester and others \(FOI guidance\)](#)
- [Access to information held in complaint files \(FOI guidance\)](#)

What other exemptions are there?

In more detail

- [Crime and taxation: general](#)
- [Crime and taxation: risk assessment](#)
- [Legal professional privilege](#)
- [Functions designed to protect the public](#)
- [Regulatory functions relating to legal services, the health service and children's services](#)
- [Other regulatory functions](#)
- [Judicial appointments, independence and proceedings](#)
- [Journalism, academia, art and literature](#)
- [Research and statistics](#)
- [Archiving in the public interest](#)
- [Health, education and social work data](#)
- [Child abuse data](#)
- [Management information](#)
- [Negotiations with the requester](#)
- [Confidential references](#)
- [Exam scripts and exam marks](#)
- [Other exemptions](#)

Crime and taxation: general

There are two parts to this exemption. Firstly, personal data processed for crime and taxation-related purposes is exempt from the right of access. These purposes are:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of a tax or duty or an imposition of a similar nature.

However, the exemption applies only to the extent that complying with a SAR is likely to prejudice the crime and taxation purposes set out above. You need to judge whether or not this is likely in each case. You should not use the exemption to justify denying access to whole categories of personal data, if its disclosure is unlikely to prejudice the crime and taxation purposes.

Example

A bank conducts an investigation into one of their customers for suspected financial fraud. During their

investigation, the bank receives a subject access request for all of the personal data they hold from the customer in question. The bank decides that they will withhold information about the investigation, because it would be likely to prejudice the investigation as the individual may abscond or destroy evidence. However, the bank is able to provide other information in response to the request which would not prejudice the investigation (for example the individual's account details and transactions).

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

Note that if you are a competent authority processing personal data for law enforcement purposes (eg the police conducting a criminal investigation), your processing is subject to the rules of Part 3 of the DPA 2018. See [our guidance on law enforcement processing for information](#) on how individual rights may be restricted when competent authorities process personal data for law enforcement purposes. If you are an intelligence service under Part 4 of the DPA 2018, please see [our guidance on intelligence services processing](#).

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) - see Schedule 2, Part 1, Paragraph 2](#) 
External link

[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 \(4\)](#) 
External link

Crime and taxation: risk assessment

Personal data is exempt from the right of access if it is in a classification applied to an individual as part of a risk assessment system.

A government department, local authority or another authority administering housing benefit must operate the risk assessment system, for the purposes of:

- 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.

However, the exemption only applies to the extent that complying with a SAR would prevent the risk assessment system from operating effectively.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 1, Paragraph 3](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#)



External link

Legal professional privilege

Personal data 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) could be maintained in legal proceedings; or
- in respect of which a professional legal adviser owes a duty of confidentiality to his client.

This exemption covers the two branches of legal professional privilege: litigation privilege and legal advice privilege. The English law concept of legal professional privilege encompasses both 'litigation' privilege and 'legal advice' privilege. In broad terms, the former applies to confidential communications between a client, professional legal adviser or a third party, but only where litigation is contemplated or in progress. The latter applies only to confidential communications between a client and professional legal adviser for the purpose of seeking or obtaining legal advice.

The Scottish law concept of confidentiality of communications provides protection for both communications about the obtaining or providing of legal advice and communications made in connection with legal proceedings. You may withhold information that comprises confidential communications between client and professional legal adviser under the legal privilege exemption, in the same way that you may withhold information attracting English law 'legal advice' privilege. Similarly, the Scottish law doctrine that a litigant is not required to disclose material they have brought into existence for the purpose of preparing their case protects information that, under English law, enjoys 'litigation' privilege.

Legal professional privilege is only available for communications that are:

- confidential in nature;
- except where litigation is in contemplation, made solely between client and professional legal adviser acting in a professional capacity; and
- made for the dominant purpose of obtaining or providing legal advice or being used by lawyers in possible or probable litigation.

A communication is a document that conveys information and 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, eg with the intention of putting them before a legal adviser.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 4, Paragraph 19](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#)



External link

Functions designed to protect the public

Personal data is exempt from the right of access if you process it for the purposes of discharging one of six functions designed to protect the public. However, this exemption only applies to the extent that complying with a SAR would be likely to prejudice the proper discharge of any of these functions. If you can comply with a SAR without causing prejudice to any of these functions, then you must do so.

The first four functions are to:

1. protect the public against financial loss due to the seriously improper conduct (or unfitness or incompetence) of financial services providers, or in the management of bodies corporate, or due to the conduct of bankrupts;
2. protect the public against seriously improper conduct (or unfitness or incompetence);
3. 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
4. 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, for a controller to rely upon this exemption, one of the functions above must be:

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

The fifth function is to:

5. 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.

A controller may rely on this exemption only where one of the above functions has been conferred on the:

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

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

6. 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.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 2, Paragraph 7](#) [↗](#)

External link

[↗ 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\(1\)](#) [↗](#)

External link

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

Personal data is exempt from the right of access if you process it for the purposes of discharging 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 be likely to prejudice the proper discharge of your functions. If you can comply with a SAR and discharge your functions as normal, you cannot rely on the exemption.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 2, Paragraph 10](#) [↗](#)

External link

[↗ 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\(1\)](#) [↗](#)

External link

Other regulatory functions

Personal data is exempt from the right of access if an organisation processes it for the purpose of discharging a regulatory function. The exemption is only available to the following bodies and persons:

- 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;
- a consumer protection enforcer (other than the Competition and Markets Authority);
- 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.

The exemption only applies to the extent that complying with a SAR would be likely to prejudice the proper discharge of your functions. If you can comply with a SAR and discharge your functions as normal, you cannot rely on the exemption.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 2, Paragraphs 11-12](#) 
External link

 [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\(1\)](#) 
External link

Judicial appointments, independence and proceedings

Personal data is exempt from the right of access if you process it:

- for the purposes of assessing a person’s suitability for judicial office or the office of Queen’s Counsel;
- as an individual acting in a judicial capacity; or
- as a court or tribunal acting in its judicial capacity.

Additionally, even if you do not process personal data for the reasons above, you are also exempt from the right of access to the extent that complying with a SAR would be likely to prejudice judicial independence or judicial proceedings.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 2, Paragraph 14](#) 
External link

[↗ 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\(1\) ↗](#)
External link

Journalism, academia, art and literature

Personal data is exempt from the right of access if you process it for:

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

Together, these are known as the 'special purposes'.

However, the exemption only applies to the extent that:

- as controller for the processing of personal data, you reasonably believe that compliance with a SAR would be incompatible with the special purposes (this must be more than just an inconvenience);
- the processing is being carried out with a view to the publication of some journalistic, academic, artistic or literary material; and
- 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 to harm individuals.

When deciding whether it is reasonable to believe that publication would be in the public interest, you must (if relevant) have regard to the:

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

If you rely upon this exemption and the individual makes a complaint to the ICO, we expect you to be able to explain why you require the exemption in each case, and how and by whom this was considered at the time. The ICO does not have to agree with your view – but we must be satisfied that you had a reasonable belief.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 5, Paragraph 26 ↗](#)
External link

[↗ 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 ↗](#)
External link

Research and statistics

There is an exemption from the right of access if you process personal data 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 the purposes for processing;
- if the processing is subject to appropriate safeguards for individuals' rights and freedoms (see Article 89(1) of the UK GDPR) – among other things, you must implement data minimisation measures;
- if the processing is not likely to cause substantial damage or substantial distress to an individual;
- if the processing is not used for measures or decisions about particular individuals, except for approved medical research; and
- if the research results are not made available in a way that identifies individuals.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemptions\) See Schedule 2, Part 6, Paragraph 27](#) 

External link

[Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5\(1\)\(b\) and \(e\), and 15\(1\)-\(3\)](#) 

External link

[Relevant provisions in the UK GDPR \(the appropriate safeguards\) See Article 89\(1\) and Recital 156](#) 

External link

[Relevant provisions in the DPA 2018 \(safeguards\) See Section 19](#) 

External link

Archiving in the public interest

There is an exemption from the right of access if you process personal data 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 the purposes for processing;
- if the processing is subject to appropriate safeguards for individuals' rights and freedoms (see Article 89(1) of the UK GDPR) – among other things, you must implement data minimisation measures;
- if the processing is not likely to cause substantial damage or substantial distress to an individual; and
- if you are not using the processing for measures or decisions about particular individuals, except for approved medical research.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemptions\) See Schedule 2, Part 6, Paragraph 28 ↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5\(1\)\(b\) and \(e\), and 15\(1\)-\(3\) ↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the appropriate safeguards\) See Article 89\(1\) and Recital 156 ↗](#)

External link

[↗ Relevant provisions in the DPA 2018 \(safeguards\) See Section 19 ↗](#)

External link

Health, education and social work data

The exemptions that may apply when a SAR relates to personal data included in health, education and social work data are explained in detail in [‘What should we do if the request involves information about other individuals?’](#), [‘Health data’](#), [‘Education data’](#) and [‘Social work data’](#).

Child abuse data

Child abuse data is personal data consisting of information about whether the data subject 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, an individual aged under 18.

You are exempt from providing child abuse data 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 an individual aged under 18; or
- appointed by a court to manage the affairs of an individual 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.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 5, Paragraph 21 ↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the exempt provisions\) See Article 15\(1\)-\(3\) ↗](#)

External link

Management information

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

Example

The senior management of an organisation are 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 subject access request. In responding to that request, the organisation does not have to reveal their plans to make the employee redundant, if doing so would be likely to prejudice the conduct of the business (perhaps by causing staff unrest before the management's plans are announced).

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 4, Paragraph 22](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#)

External link

Negotiations with the requester

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

Example

An individual makes a claim to his insurance company. The claim is for compensation for personal injuries he sustained in an accident. The insurance company disputes the seriousness of the injuries and the amount of compensation they should pay. An internal paper sets out the company's position on these matters, including the maximum sum they are willing to pay to avoid the claim going to court. If the individual makes a subject access request to the insurance company, they do not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

The exemption does not set out any limits regarding the timing of negotiations, nor does it say that 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 justify why disclosure would be likely to prejudice negotiations. This may be most relevant where you can demonstrate that disclosure would prejudice your position in future negotiations.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 4, Paragraph 23](#) [↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#)



External link

Confidential references

From time to time you may give or receive references about an individual. The personal data included in a confidential reference is exempt from the right of access for the purpose of prospective or actual:

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

The exemption applies regardless of whether you have given or received the reference.

Example

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

It is important to note that this exemption only applies to references given in confidence. You should make it clear to individuals, 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. For more information see our [guidance on the right to be informed](#).

You should bear in mind that it is good data protection practice to be open as possible with individuals about information which relates to them. They should be 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.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 4, Paragraph 24](#) [↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#) [↗](#)

External link

Exam scripts and exam marks

There is an exemption from the right of access relating to information about the outcome of academic, professional or other examinations, but it only applies to the information recorded by candidates. This means candidates do not have the right to copies of their answers to the exam questions.

The information recorded by the person marking the exam is not exempt. However, if an individual makes a SAR for this information before the results are announced, special rules apply to how long you have to comply with the request. You must provide the information within:

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

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 2, Part 4, Paragraph 25](#) [↗](#)

External link

[↗ Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\)](#) [↗](#)

External link

Other exemptions

The exemptions mentioned in this chapter are those most likely to apply in practice. However, the DPA 2018 contains additional exemptions that may be relevant when dealing with a SAR. For more information please see [our guidance about exemptions](#).

Further reading

- [Guide to Law Enforcement Processing](#)
- [Guide to Intelligence Services Processing](#)
- [Exemptions](#)

Are there any special cases?

In more detail

- [Special cases](#)
- [Unstructured manual records](#)
- [Credit files](#)

Special cases

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

- [unstructured manual records](#);
- [credit files](#);
- [health data](#);
- [educational data](#); and
- [social work data](#).

These are each covered in this section and the following sections.

Unstructured manual records

In general, the UK GDPR does not cover non-automated information which is not, or you do not intend to be, part of a 'filing system'. However, under [Article 2\(1A\) of the UK GDPR](#), unstructured manual information that public authorities process constitutes personal data. 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 data; or
- they estimate that the 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 can 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; and
- extracting the requested information from records.

The biggest cost is likely to be staff time. You should 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 to your public authority. For further information, please see the [Fees Regulations](#) made under Section 12(5) of FOIA 2000. 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.

Public authorities are also not obliged to comply with requests for unstructured paper records if the personal data is about appointments, removals, pay, discipline, superannuation or other personnel matters in relation 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:
 - Her Majesty;
 - a Minister of the Crown;
 - the National Assembly for Wales;
 - the Welsh Ministers;
 - a Northern Ireland Minister (within the meaning of the Freedom of Information Act 2000); or
 - an FOI public authority (as defined in FOIA or FOISA).

Further Reading

 [Relevant provisions in the DPA 2018 See Part 2, Chapter 3, sections 21 and 24](#) 

External link

 [Relevant provisions in the UK GDPR – see Article 2\(1A\)](#) 

External link

Credit files

In the DPA 2018 there are special provisions about the access to personal data that credit reference agencies hold. Unless otherwise specified, a SAR to a credit reference agency only applies to information relating to the individual's financial standing. Credit reference agencies must also inform individuals of their rights under s.159 of the Consumer Credit Act 1974.

Further Reading

 [Relevant provisions in the DPA 2018 See Part 2, Chapter 2, section 13](#) 

External link

Health data

In more detail

- [What is health data?](#)
- [Can I charge a fee for providing access to health data?](#)
- [Is health data ever exempt from the right of access?](#)
- [Is health data exempt if it is processed by a court?](#)
- [Is health data exempt if disclosure goes against an individual's expectations and wishes?](#)
- [Is health data exempt if disclosure could cause serious harm?](#)
- [What are the restrictions on disclosing health data?](#)
- [What about requests for health data from a third party?](#)

What is health data?

The DPA 2018 defines 'data concerning health' as personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about their health status.

Further Reading

 [Relevant provisions in the DPA 2018 See Part 7, section 205\(1\)](#) 

External link

Can I charge a fee for providing access to health data?

No. There are no special rules which allow you to charge fees if you are complying with a SAR for health data. For more information about when you can charge a fee please see ['Can we charge a fee?'](#).

Is health data ever exempt from the right of access?

The exemptions and restrictions that apply to other types of personal data also apply to personal data concerning health. So, for example, if health data contains personal data relating to someone other than the requester (such as a family member), you must consider the rules about third-party data before disclosing it to the requester. However, you should not normally withhold information that identifies a health professional, such as a doctor, dentist or nurse, carrying out their duties for this reason. See ['What should we do if the request involves information about other individuals?'](#) for more information.

There are also further exemptions and restrictions that apply to health data in particular. These are explained in the next sections.

Is health data exempt if a court processes it?

There is an exemption from the right of access for health data if the data is:

- processed by a court;
- supplied in a report or given to the court as evidence in the course of proceedings; and
- certain specific statutory rules apply to those proceedings that allow the withholding of the data from the individual it relates to.

If you think this exemption might apply to your processing of personal data, see paragraph 3(2) of Schedule 3, Part 2 of the DPA 2018 for full details of the statutory rules.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 2, Paragraph 3](#) [↗](#)

External link

[↗ 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\(1\)](#) [↗](#)

External link

Is health data exempt if disclosure goes against an individual'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 data from someone:

- with parental responsibility for an individual aged under 18 (or 16 in Scotland); or
- appointed by the court to manage the affairs of an individual 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 individual had provided to you in the expectation that it would not be disclosed to the requester, unless the individual has since expressly indicated that they no longer have that expectation;
- was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or
- the individual has expressly indicated should not be disclosed in this way.

Further Reading

[↗ Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 2, Paragraph 4](#) [↗](#)

External link

[↗ 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\(1\)](#) [↗](#)

External link

Is health data exempt if disclosure could cause serious harm?

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

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

- you are a health professional; or
- within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health data is met. Even if you have done this, you still cannot rely on the exemption if it would be reasonable in all the circumstances to re-consult the appropriate health professional.

This means that if you are not a health professional, you cannot rely on this exemption and refuse to provide the health data in response to a SAR, unless you have obtained an opinion that the serious harm test for health data is met. Bear in mind that you may also need to obtain an opinion even if you do not intend to rely on this exemption (see [What are the restrictions on disclosing health data?](#)).


The appropriate health professional is the health professional most recently responsible for the diagnosis, care or treatment of the individual. You can appoint a health professional with the necessary experience and expertise, if the most recent health professional no longer practices.

If you think this exemption might apply to a SAR you have received, see paragraph 2(1) of Schedule 3, Part 2 of the DPA 2018 for full details of who is considered the appropriate health professional.

However, if you are not a health professional, you may only disclose health data in specific circumstances. Please see the next section (['What are the restrictions on disclosing health data?'](#)) if you intend to disclose health data.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 2, Paragraph 5](#) 
 External link

[Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 
 External link

What are the restrictions on disclosing health data?

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

- within the last six months you have obtained an opinion from the appropriate health professional that the serious harm test for health data is not met. Even if you have done this, you must re-consult the appropriate health professional if it would be reasonable in all the circumstances; or
- you are satisfied that the individual it is about has already seen, or knows about, the health data.

The individual is likely to be aware of the health data if they have provided the information to you, or it is obvious that they know about the information.

Example

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

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

'Health professionals' include registered medical practitioners, dentists and nurses. The DPA provides a full list of the types of professional that fall within the definition (see section 204 of the DPA 2018).

If you need to consult with an appropriate health professional, you may consider the request to be complex. If so, you can extend the time limit to respond by a further two months. Please see ['When is a request complex?'](#) and ['Can we extend the time limit for a response?'](#) for further information.

When you receive the SAR, you should make all reasonable efforts to obtain an opinion from the appropriate health professional as soon as possible. However, if you are unable to obtain an opinion within the time limit for responding to the request, you should withhold the health data.

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

You should note that because of the nature of this exemption (and the potential nature of the data in question) you may not be able to tell the individual why you have extended the time limit to respond or why you have withheld the information. However, this will depend on the circumstances and in general you should be as transparent as you possibly can. Please see ['What should we do if we refuse to comply with a request?'](#).

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Part 7, section 204\(1\) and Schedule 3, Part 2, Paragraph 6](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 

External link

What about requests for health data from a third party?

A third party can make a SAR on behalf of an individual, provided that the third party is entitled to act on the individual's behalf. Therefore, a solicitor may make a SAR on behalf of a client. It is the solicitor's

responsibility to provide evidence that they are entitled to make a SAR on their client's behalf. Please see ['Can a request be made on behalf of someone?'](#) for more information.

If you have a genuine concern that a solicitor (or other third party) has requested excessive information, you should contact the individual first to make them aware of your concerns. If the individual agrees, you may send the response directly to the individual rather than to the third party.

The individual may then choose to share the information with the third party after reviewing it. If you cannot contact the individual, you should provide the requested information to the third party (as long as you are satisfied that they are authorised to act on the individual's behalf).

A SAR is not appropriate in situations where the third party's interests are not aligned with the individual's, for example an insurance company needing to access health data to assess a claim. In such circumstances, with an individual's consent, an insurer can apply to an individual'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). AMRA does not lie within the regulatory responsibilities of the ICO, but we refer to it here for completeness.

Remember that the definition of personal data only relates to living individuals, so individuals cannot use a SAR to obtain information about a deceased individual. However, 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 data

In more detail

- [What is education data?](#)
- [How can education data be accessed?](#)
- [Can I charge a fee for providing subject access to education data?](#)
- [How long do we have to comply if a SAR is received in school holidays?](#)
- [Is education data ever exempt from subject access?](#)
- [Is education data exempt if it is processed by a court?](#)
- [Is education data exempt if disclosure could cause serious harm?](#)
- [Is there a restriction if you are an education authority in Scotland?](#)

What is education data?


The DPA 2018 defines 'education data' as:

- personal data which consists of information that forms part of an educational record; and
- is not data concerning health.

The definition of 'educational record' in the DPA 2018 differs between England and Wales, Scotland and Northern Ireland. Broadly speaking, however, the expression has a wide 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.

However, information a teacher keeps solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil forms part of the pupil's educational record. However it is possible that some of the information could fall outside the educational record, eg information a parent of another child provides about the pupil is not part of the educational record.

Further Reading

[Relevant provisions in the DPA 2018 See Schedule 3, Part 4, paragraphs 13-17](#) 

External link

How can individuals access education data?

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

- The pupil's right of access under Article 15 of the UK GDPR.
- The parent's right of access to their child's 'educational record'. In England, Wales and Northern Ireland this right of access is only relevant to maintained schools (all grant aided schools in Northern Ireland – not independent schools, academies or free schools). However, in Scotland the right extends 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

Although this guidance only concerns the right of access under the UK GDPR, it is important to be aware of a parent's right to access their child's educational records. This is because the information you provide may differ depending on which right applies, ie the parent's right is only to access their child's educational record, whereas a SAR also enables access to the personal data a school processes that does not fall into the definition of an educational record. The two rights also have different time limits for compliance. You must respond to a parent's right of access to their child's educational records within 15 school days, whereas you must comply with a SAR within one month. The law on a parent's right to their child's educational records does not lie within the ICO's regulatory responsibilities, but we refer to it here for completeness.

Unlike the parent's right of access to 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 and young people?'](#) If it is not clear whether a requester has parental responsibility for the child or is acting on their behalf, you should clarify this before responding to the SAR. If the school is in England, Wales or Northern Ireland, the school should deal with the SAR. If the school is in Scotland, the relevant education authority or the proprietor of an independent school should deal with the SAR.

Can I charge a fee for providing subject access to education data?

No. There are no special rules which allow you to charge fees if you are complying with a SAR for education data. For more information about when you can charge a fee please 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 which allow you to extend the time period for dealing with a SAR you receive it during school holidays. Regardless of whether a school is closed, if you receive a SAR then you have the normal time period to comply. Please see ['How long do we have to comply?'](#) for more information.

Is education data ever exempt from subject access?

The exemptions and restrictions that apply to other types of personal data also apply to education data. So, for example, if an educational record contains personal data relating to someone other than the requester (such as a family member), you must consider the rules about third-party data before disclosing it to the requester. However, you should not normally withhold information that identifies a teacher. See ['What should we do if the request involves information about other individuals?'](#) for more information.

There are also further exemptions and restrictions that apply to education data in particular. These are explained in the next sections.

Is education data exempt if a court processes it?

This exemption can apply to education data that a court processes.

You are exempt from providing education data in response to a SAR if the education data is:

- supplied in a report or given as evidence to the court in the course of proceedings; and
- certain specific statutory rules apply to those proceedings that allow the withholding of the data from the individual it relates to.

If you think this exemption might apply to your processing of personal data, see paragraph 18(2) of Schedule 3, Part 4 of the DPA 2018 for full details of the statutory rules.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 4, Paragraph 18](#) 

External link

[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\(1\)](#) 

External link

Is education data exempt if disclosure could cause serious harm?

Yes. In most circumstances, you are exempt from providing education data in response to a SAR to the extent that complying with the request would be likely to cause serious harm to the physical or mental health of any individual. This is known as the “serious harm test” for education data. However, this exemption does not apply to independent schools in Scotland.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 4, Paragraph 19](#) 

External link

[Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 

External link

Is there a restriction if you are an education authority in Scotland?

This is a restriction rather than an exemption. It applies if you process education data as an education authority in Scotland (as defined by the Education (Scotland) Act 1980), and you receive a SAR for that data.

It restricts you from disclosing education data in response to a request if:

- you believe that the data came from the Principal Reporter (as defined by the Children’s Hearings (Scotland) Act 2011) in the course of their statutory duties; and
- the individual whom the data is about is not entitled to receive it from the Principal Reporter.

If there is a question as to whether you need to comply with a SAR in this situation, you must inform the Principal Reporter within 14 days of the question arising.

You may only disclose the education data in response to the request if the Principal Reporter has told you they think the serious harm test for education data is not met.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 4, Paragraph 20](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 

External link

Social work data

In more detail

- [What is social work data?](#)
- [Can I charge a fee for providing access to social work data?](#)
- [Is social work data ever exempt from subject access?](#)
- [Is social work data exempt if it is processed by a court?](#)
- [Is social work data exempt if disclosure goes against an individual's expectations and wishes?](#)
- [Is social work data exempt if disclosure could cause serious harm?](#)
- [Is there a restriction if you are a local authority in Scotland?](#)

What is social work data?

The DPA 2018 defines 'social work data' as personal data which:

- paragraph 8 of Schedule 3, Part 3 of the DPA 2018 applies to (generally this includes particular bodies processing personal data in connection with their social services functions or to provide social care); but
- is not education data or health data.

Further Reading

 [Relevant provisions in the DPA 2018 See Schedule 3, Part 3, paragraph 7-8](#) 

External link

Can I charge a fee for providing access to social work data?

No. There are no special rules which allow you to charge fees if you are complying with a SAR for social work data. For more information about when you can charge a fee please see ['Can we charge a fee?'](#).

Is social work data ever exempt from subject access?

The exemptions and restrictions that apply to other types of personal data also apply to social work data. So, for example, if social work data contains personal data relating to someone other than the requester (such as a family member), you must consider the rules about third party data before disclosing it to the requester. However, you should not normally withhold information that identifies a professional, such as a social worker, carrying out their duties for this reason. See ['What should we do if the request involves information about other individuals?'](#) for more information.

There are also further exemptions and restrictions that apply to social work data in particular. These are explained in the next sections.

Is social work data exempt if a court processes it?

You are exempt from the right of access if the social work data is:

- processed by a court;
- supplied in a report or given as evidence to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the social work data to be withheld from the individual it relates to.

If you think this exemption might apply, see paragraph 9(2) of Schedule 3, Part 3 of the DPA 2018 for full details of the statutory rules.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 3, Paragraph 9](#) 

External link

 [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\(1\)](#) 

External link

Is social work data exempt if disclosure goes against an individual'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 social work data concerning an individual from someone:

- with parental responsibility for an individual aged under 18 (or 16 in Scotland); or
- appointed by court to manage the affairs of an individual 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 individual provided in the expectation that it would not be disclosed to the requester, unless the individual has since expressly indicated that they no longer have that expectation;
- was obtained as part of an examination or investigation that the individual consented to, in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or
- the individual has expressly indicated should not be disclosed in this way.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 3, Paragraph 10](#) 

External link


 [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\(1\)](#) 


External link

Is social work data exempt if disclosure could cause serious harm?

Yes. You are exempt from complying with a SAR for social work data to the extent that complying with the request would be likely to prejudice carrying out social work because it would be likely to cause serious harm to the physical or mental health of any individual. This is known as the “serious harm test” for social work data.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 3, Paragraph 11](#) 
External link

[Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 
External link

Is there a restriction if you are a local authority in Scotland?

Yes. This is a restriction rather than an exemption. It applies if you process social work data as a local authority in Scotland (as defined by the Social Work (Scotland) Act 1968), and you receive a request for that data.

It restricts you from disclosing social work data in response to a SAR if:


- the data came from the Principal Reporter (as defined by the Children’s Hearings (Scotland) Act 2011) in the course of their statutory duties; and
- the individual whom the data is about is not entitled to receive it from the Principal Reporter.

If there is a question as to whether you need to comply with a SAR in this situation, you must inform the Principal Reporter within 14 days of the question arising.

You may only disclose the social work data in response to the SAR if the Principal Reporter has told you they think the serious harm test for social work data is not met.

Further Reading

[Relevant provisions in the DPA 2018 \(the exemption\) See Schedule 3, Part 3, Paragraph 12](#) 
External link

[Relevant provisions in the UK GDPR \(the exempt provisions\) See Articles 15\(1\)-\(3\)](#) 
External link

Can the right of access be enforced?

In more detail

- [What enforcement powers does the ICO have?](#)
- [Can a court order be used to enforce a SAR?](#)
- [Can an individual be awarded compensation?](#)
- [Is it a criminal offence to force an individual to make a SAR?](#)
- [Is it a criminal offence to destroy and conceal information?](#)

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 in relation to their personal data. For example, if a controller fails to comply with a SAR.

In appropriate cases, the ICO may take action against a controller or processor if they fail to comply with data protection legislation. For example, we could issue a controller or processor with a:

- warning;
- reprimand;
- enforcement notice; or
- penalty notice.

The ICO will exercise these enforcement powers in accordance with our [Regulatory Action Policy](#).

Whilst a processor does not have any obligations under Article 15, under Article 28 the controller and processor must have a contract in place. The contract must state that the processor will assist the controller with their obligations to comply with a SAR by taking appropriate technical and organisational measures, as far as this is possible (taking into account the nature of the processing). For more information please read our guidance on [contracts 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. It is a matter for the court to decide, in each particular case, whether to make such an order.

Can an individual be awarded compensation?

If an individual suffers damage or distress because you have infringed 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 first 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 giving rise to the damage.

Is it a criminal offence to force an individual to make a SAR?

Usually. It is a criminal offence to require an individual to make a SAR, in certain circumstances and in relation to certain information. For more information please see [‘Can we force an individual 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 would have been entitled to receive.

You can defend this offence if you prove that:

- the alteration, defacing, blocking, erasure, destruction or concealment of the information would have happened regardless of whether the individual made a SAR; or
- you acted in the reasonable belief that the person making the SAR was not entitled to receive the information requested.

Further Reading

[Relevant provisions in the UK GDPR See Articles 77, 82 and Recitals 141, 146](#) 

External link

[Relevant provisions in the DPA 2018 See Part 6 and Part 7, section 184](#) 

External link

Further reading

- [Regulatory Action Policy](#)
- [Contracts and liabilities between controllers and processors](#)

Can we force an individual to make a SAR?

In more detail

- [What is an enforced SAR?](#)
- [When does it apply?](#)
- [What is a relevant record?](#)
- [What does require mean?](#)
- [Are there any exemptions?](#)
- [What are the penalties?](#)

What is an enforced SAR?

An enforced SAR is when someone requires an individual to make a SAR to gain access to certain information about them (eg their convictions, cautions or health records). They then use this information, for example, as supporting evidence regarding a job application or before entering into a contract for insurance. Forcing an individual to make a SAR in such circumstances is a criminal offence.

Example

An individual applies for a position as a waiter at a restaurant, but is told that they cannot be offered the position until they provide a copy of their criminal record. The employer states that they must make a SAR in order to gain this information and they will only be appointed if it is supplied. The employer is likely to have committed a criminal offence.

Example

An individual makes an application for private health insurance to an insurance provider. The provider agrees to insure the individual but explains that it is a condition of the insurance that the individual must make and provide the results of a SAR for their medical records. The insurance company is likely to have committed an offence.

There are appropriate ways of accessing information such as criminal records and health records, ie through the criminal disclosure regime or under the provisions of the Access to Medical Reports Act 1988 (AMRA). An individual providing the results of a SAR, rather than using such appropriate channels, runs the risk of greater, and sometimes excessive disclosure. This is because a SAR requires the disclosure of all personal information (subject to some exemptions), and does not distinguish, for instance, between spent

and unspent convictions.

When does it apply?

It is a criminal offence for an individual or legal person (person 1) to require another person to make and provide the results of a SAR for a 'relevant record' in connection with:

- an employee's recruitment by person 1;
- the person's continued employment by person 1; or
- a contract for the provision of services to person 1.

The use of the words 'in connection with' means that there is a broad scope.

It is also a criminal offence for an individual or legal person (person 2) to require another person to make and provide the results of a SAR for a 'relevant record' if:

- person 2 is 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.

Providing the opportunity for individuals to do voluntary work is caught by the provision of goods, facilities or services.

Example

An individual applies to do voluntary work with a charity. The charity explains that the individual 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.

Further Reading

[Relevant provisions in the UK GDPR See Article 15 and Recital 63](#)

External link

[Relevant provisions in the DPA 2018 - See Part 7, section 184, Paragraph 6 and Schedule 18](#)

External link

What is a relevant record?

A 'relevant record' is a record which has been, or is to be, obtained by an individual exercising their right of access and:

- is a health record;
- contains information relating to a conviction or caution; or

- contains information relating to a statutory function in relation to that individual.

A 'health record':

- consists of data 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 individual it relates to.

'Information relating to a conviction or caution':

- consists of data 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 an individual.

'Information relating to a statutory function':

- consists of data processed in connection with certain statutory functions of the Secretary of State, Department for Communities in Northern Ireland, the Department of Justice in Northern Ireland, the Scottish Ministers or the Disclosure and Barring Service; 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 (for example, 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; or
 - the vetting and barring of those who wish to work with children or vulnerable adults.

Example

An individual applies for a job as an office receptionist. The employer offers the individual 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.

Further Reading

[Relevant provisions in the UK GDPR See Article 15 and Recital 63](#)

External link

[Relevant provisions in the DPA 2018 - see Part 7, section 184, Paragraph 6 and Schedule 18](#)

What does require mean?

A person has 'required' another person to make a SAR if they:

- 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.

You should look at a requirement in a wider context than simply an individual not receiving a job if they do not make a SAR. For instance, it would be considered a requirement if an individual would:

- be left in a detrimental position by not making a SAR; or
- miss out on an incentive by not making a SAR.

Example

An individual 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 at a reduced rate than that advertised. This would obviously leave the individual in a detrimental position if they did not make a SAR.

The offence is the act of requiring an individual to make a SAR. The requirement is enough, and is not dependent on the withdrawal of the offer of employment or the provision of goods, facilities or services.

Also, you will have required an individual to make a SAR, even if you give them the option that either you will access the information through an appropriate and lawful channel or they should make a SAR.

Further Reading

[Relevant provisions in the UK GDPR See Article 15 and Recital 63](#)

External link

[Relevant provisions in the DPA 2018 See Part 7, section 184, paragraph 5](#)

External link

Are there any exemptions?

It is not a criminal offence for you to require an individual 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 court order; 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, there needs to be an extremely strong justification that enforced subject access is in the public interest, supported by clear, specific and cogent evidence. This may be difficult to achieve as there is already clear public policy and laws about criminal record checking and access to medical records.

The defence that an enforced SAR is in the public interest cannot be used when the justifying argument is that the public interest relates to the prevention or detection of crime. This is because Part 5 of the Police Act 1997 defines in what circumstances certain types of criminal records check can be made. Given that the Police Act 1997 outlines the circumstances for criminal records checking, it is not possible to justify enforced subject access on the basis that it would assist with the prevention or detection of crime.

Further Reading

 [Relevant provisions in the UK GDPR See Article 15 and Recital 63](#) 

External link

 [Relevant provisions in the DPA 2018 See Part 7, section 184, paragraphs 3 and 4](#) 

External link

What are the penalties?

An individual 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. 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).

Further Reading

 [Relevant provisions in the UK GDPR See Article 15 and Recital 63](#) 

External link

 [Relevant provisions in the DPA 2018 See Part 7, section 196](#) 

External link