Right of access

Table of contents

About this detailed guidance

This guidance discusses the right of access in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you apply the right of access in practice. It is aimed at data protection officers (DPOs) and those with specific data protection responsibilities in larger organisations.

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.

What is the right of access?

In more detail

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

The right of access, commonly referred to as subject access, gives 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.

Commented [redacted]: The language "their personal data" implies the data subject has ownership of the data. I would suggest more neutral language (the right under Article 15 GDPR refers to "personal data concerning him or her" and the definition of "personal data" is "any information relating to an identified or identifiable natural person").

This comment applies to all usage of "their personal data" and related terms throughout this document.

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) or another supervisory authority;
- information about the source of the data, if it was not obtained directly from the individual;
- the existence of 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 provide a link to or a copy of your privacy notice.

Are individuals only entitled to their own personal data?

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

Commented [[redacted]]: I would remove this sentence. It is confusing, and oversimplifies the exemption for third party personal data.

Commented [[redacted]]: See above comment about the use of language which implies that personal data is "owned by" or "belongs to" the data subject.

The General Data Protection Regulation (GDPR) provides that, for information to be personal data, it must relate to a living person who can be identified from that information (directly or indirectly). The context in which information is held, and the way it is used, 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. If responding to a SAR involves providing information that relates both to the individual making the request and to another individual, an exemption may apply. 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 ensuring that SARs are complied with. 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.

If you use a processor, you need to have contractual arrangements in place to guarantee that SARs are dealt with properly, irrespective of whether they are sent to you or to the processor. Please read our guidance on contracts between controllers and processors for more information.

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 data processor to retrieve any personal data that relates to the member of staff.

Relevant provisions in the GDPR

See Articles 4(1), 4(7), 4(8), 15, 26, 28 and Recitals 30, 63, 79, 81

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?

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

- comply with your legal obligations under the 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 may prepare:

- **Awareness –** Make information available about how individuals can make a SAR (eg on your website, in leaflets, 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 there is resilience against absence.

- **Asset registers –** Maintain information asset registers which state where and how personal data is stored. This helps speed up the process of locating the information required to respond to SARs.

- **Checklists –** Produce a standard checklist that staff can use to ensure a consistent approach is taken to SARs.

- **Logs -** Maintain a log of SARs you have received and update it to monitor progress. The log may include copies of information supplied in response to a SAR, together with copies of any material 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 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 by enabling you to easily locate and extract personal data. Your systems should also be designed to 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. For example:

- 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.

Relevant provisions in the GDPR

See Articles 5(1)(c), 5(2), 25, 30, 32, 26, 28 and Recitals 39, 78, 82, 83

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)?

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 GDPR.

Are there any formal requirements?

The GDPR does not set out formal requirements for a valid request. Therefore, an individual can make a SAR verbally or in writing. It can also be made to any part of your organisation (including by social media) and does not have to be directed to a specific person or contact point.

Commented [redacted] "Verbally" means "in words". It would be helpful to clarify they can be made orally (by speech).

A request does not have to include the phrases 'subject access request', 'right of access' or 'Article 15 of the GDPR', as long as it is 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. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. 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. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted it.

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, although 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 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 it is submitted 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.

Commented [[redacted]]: Same comment as above.

Can a request be made via social media?

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.

Can a request be made on behalf of someone?

An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. The 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 evidence of this. This might be a written authority to make the request or a more general power of attorney.

Example

A building society has an elderly customer who visits a particular branch to make weekly account withdrawals. Over the past few years, she has always been accompanied by her daughter who is also a customer of the branch. The daughter makes a SAR on behalf of her mother and explains that her mother does not feel up to 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 had a general power of attorney, the society would be happy to comply. They ask the daughter whether she has such a power, but she does not.

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

If there is no evidence that a third party is authorised to act on behalf of an individual, you are not required to respond to the SAR. However, if you are able to contact the individual, you should respond to them directly to confirm whether they wish to make a SAR.

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 what information would be disclosed, 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 in the 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 which enable a third party to exercise subject access rights on behalf of such an individual. 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. 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 exercising their rights under Article 15;
- are able to verify the identity of the individual, if this is in doubt (see 'Can we ask for ID?'); and
- are satisfied the third party portal is acting with the authority of, and on behalf of, the individual.

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.

Commented [redacted]: This implies that the request has to refer to "Article 15". I would suggest instead "have been made aware that a particular individual is requesting information".

Commented [redacted]: I'm not sure if it's accurate to suggest the third party portal is "acting". Rather, I would suggest a third party portal is a tool used by the applicant (in the same way as an email provider is providing a service and not "acting on behalf of" the sender).

I would therefore suggest "are satisfied that the request has been made with the individual's knowledge and agreement".

Commented [redacted]: I would clarify that this includes clicking a link to view the request.

If you have concerns that the individual has not authorised the information to be uploaded to the portal or may not understand what information would be disclosed to the portal, you should contact the individual to make them aware of your concerns.

What about requests for information about children or young people?

Even if a child is too young to understand the implications of the right of access, it is still their right. Even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them, it is still the right of the child rather than anyone else's.

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 you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, 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.

Commented [redacted]: I appreciate the sentiment here, but this is not the correct legal position, and best interests should **not** be considered (unless this is a specific factor in the exemption, e.g. child abuse data).

In relation to Scotland, s208 DPA 2018 provides the circumstances where children have capacity to make a SAR. If the child has capacity, then their parents do not. If a parent does not have capacity to make the request on behalf of their child, this cannot be overridden by the fact that the data controller considers it might be in the child's best interests to respond.

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 make decisions like this;
- the nature of the personal data;
- 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 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 cannot access this information; and
- any views the child or young person has on whether their parents 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.

Commented [redacted]: I suggest clarifying that this does not mean younger children do not have capacity. The rule is that **all** children aged 12+ have capacity unless shown otherwise, but **most** 10 year olds will indeed be capable of making a SAR.

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, however, we do not expect you to do this if you are dealing with the request as a SAR.

- It is good practice for public authorities to clarify within 20 working days (the time limit for responding to FOI requests) that the request is being dealt with as a SAR under the GDPR, and that the one month time limit for responding applies.

If you are a public authority and the request relates to both the personal data of the requester, and to other (non-personal) information, you should treat this as two requests:

Commented [redacted]: By contrast, the Scottish Information Commissioner **does** expect a formal refusal notice to be issued, and has decided against authorities who have failed to do so. I would suggest noting this, or contacting OSIC for their comments on what to include in this guidance.

Commented [redacted]: "Non-personal" isn't the best description, as personal data about third parties can still be disclosed under FOI.

- one for the requester's personal data made under the GDPR; and
- another for the remaining, non-personal 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 personal data is mistakenly disclosed 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 correspondence that you can deal with in the normal course of business. 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 such correspondence on a case by case basis.

Relevant provisions in the GDPR

See Articles 15 and Recitals 59, 63

Further reading

Children and the 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?

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.

Example

An organisation receives a request on 3 September. The time limit starts from the same day. This gives the organisation until 3 October to comply with the request.

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 the request is made.

Commented [redacted]: It is misleading to say "The time limit starts from the same day". The first day of the one month period is the day after the response is received, and the last day to respond is the calendar day corresponding to the date the request was received.

For the request received on 3 September, the one month period is 4 September to 3 October.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

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?

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.

Commented [redacted]: Same comment as above. It is not helpful to say "The time limit starts from the same day".

Example

An organisation receives a request on 7 August. The time limit starts from the same day. The request is complex so the organisation extends the period by two months.

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

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.

Commented [redacted]: Perhaps also add that the information is held by a wide range of individuals within the organisation.

- 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 redacting information or communicating it in an intelligible form.

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 has requested 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 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 reasonable 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 what fee is reasonable you can take into account administrative costs such as:

- photocopying;
- printing; and
- postage.

You cannot charge for the time taken to deal with the request.

You must be able to justify the costs you have charged in the event that a complaint is made to the ICO. It is good practice to explain the costs to the individual.

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

Do we need to make reasonable adjustments for disabled people?

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.

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?

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). You also need to be satisfied that 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 about what you ask for. You should not request more information if the identity of the requester 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.

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.

Commented [redacted]: You should have a separate, more detailed, section on whether the requester has the authority to make the request on behalf of the data subject.

Commented [redacted] "the data subject".

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 such that the practice is right to be cautious. They could ask the requester to provide more information, such as a document providing evidence of their 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 upon receipt of the requested information. Please see 'How long do we have to comply?' for more information about timescales.

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).

Commented [redacted]: I would add a passage saying that this should be done by computer not by sight, as a visually similar email address can be used to impersonate someone (e.g. [redacted]@GMAIL.COM and [redacted]@GMAIL.COM)

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 that is made as part of a bulk request has the same legal status as a SAR that is made individually;

- the purpose for which a SAR is made does not affect its validity, or your duty to respond to it (unless it is a manifestly unfounded or excessive request);
- if a request is made by a third party on behalf of an individual, the behaviour of the third party 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; and
- 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 requests are dealt with 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 would not take such action if it is clearly unreasonable to do so.

Relevant provisions in the GDPR

See Articles 12, 15 and Recitals 58, 59 63, 64

How do we find and retrieve the relevant information?

In more detail

What efforts should we make to find information?

The GDPR places a high expectation on you to provide information in response to a SAR. Whilst it may be challenging, you should make extensive efforts to find and retrieve the requested information.

You should ensure that your information management systems are well-designed and maintained, so you can efficiently locate and extract information requested by the data subjects whose personal data you process and redact third party data where it is deemed necessary. For more information please see 'What about our information management systems?'.

Can we clarify the request?

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. However, this does not affect the timescale for responding - you must still respond to their request within one month. 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?').

You cannot ask the requester to narrow the scope of their request, but you can ask them to provide additional details that will help you locate the requested information, such as the context in which their information may have been processed and the likely dates when processing occurred.

However, a requester is entitled to ask for 'all the information you hold' about them. If an individual refuses to provide any additional information or does not respond to you, you must still comply with their request by making reasonable searches for the information covered by the request. The time limit is not paused whilst you wait for a response, so you should begin searching for information as soon as possible. You should ensure you have appropriate records management procedures in place to handle large requests and locate information efficiently.

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. Whilst the supermarket is waiting for a response it starts to search for information that may be covered by the request.

The employee confirms that their request is for all the information held by the supermarket relating to their employment, and is not limited to information about the complaint. However, the employee does not want to receive information about their relationship with the supermarket as a customer.

If you receive a request where it is genuinely unclear whether a SAR is being made, 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).

What about electronic records that aren't easily available?

In most cases, information stored in electronic form can easily be found and retrieved. 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 back up 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 has been 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. 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 held in electronic form by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated 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 organisations to use time and

effort reconstituting information that they have deleted as part of their general records management.

For more information please see our guidance on deleting personal data.

What about information contained in emails?

The contents of emails stored 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 it has been moved to a user's 'Deleted items' folder.

It may be particularly difficult to find information related to a SAR if it is contained in emails that have been archived and 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.

What about information stored 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 it is stored on someone else's 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.

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 or in private email accounts. 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 the scope of a SAR you receive. The purpose for which the information is held, and its context, is likely to be relevant. We do not expect you to instruct staff to search their private emails

Commented [redacted]: I would avoid language that suggests employees are data processors.

or personal devices 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 such 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 GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'.

Commented [redacted]: I suggest emphasising that it is a very low bar to being considered a 'filing system' – Grand Chamber case C-25/17.

Quote

'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 those 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 has not provided 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 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 data following receipt of a SAR?

It is our view that a SAR relates to the data held at the time the request was received. 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.

Relevant provisions in the GDPR

See Articles 4(6), 5(1)(e), 15, 32 and Recitals 39, 63, 83

Relevant provisions in the DPA 2018

See Part 2, Chapter 3 and Part 6, section 173

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?

The focus of a SAR is usually the supply of 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 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 approach is likely to be appropriate 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 have located and retrieved the personal data that is relevant to the request, you must provide the requester with a copy.

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

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

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. 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 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 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; or

- depending on the source, it may pose a security risk to those individuals.

Example

An individual makes a subject access request for their personal data. The organisation provides a copy of this data using what it considers 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 copy in a 'commonly used' format due to the availability of that software package.

However, as the GDPR does not require individuals to purchase specific software packages merely to access a copy of their data, the organisation has not fulfilled its obligations to provide a copy as the individual cannot access it.

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

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 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 have provided them with access to their personal data, it does not necessarily mean that you have provided them with a copy of their data. This depends on whether they are able to download of copy of the information they have requested. 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?

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 you responded 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.

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 the SAR and what information comes under the scope of the data portability 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 supplied?

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 it cannot be understood.

The 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 the information is addressed 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.

When providing a copy of the personal data requested, you are expected to give the individual additional information to aid understanding if the 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 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.

Relevant provisions in the GDPR

See Articles 12, 15, 20 and Recitals 58, 63, 68

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?

If an exemption applies, you can refuse to comply with a SAR (wholly or partly). Not all of the 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
- excessive.

You should consider each request on a case-by-case basis in order to decide if it is manifestly unfounded or excessive. You should not have a blanket policy.

You must be able to demonstrate to the individual why you consider that the request is manifestly unfounded or excessive and, if asked, explain your reasons to the ICO.

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 purposes other than to cause disruption. For example:

- the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated accusations against you or specific employees;
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual 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, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request is manifestly unfounded.

What does excessive mean?

A request may be excessive if it:

- repeats the substance of previous requests and a reasonable interval has not elapsed; or
- overlaps with other requests.

However, it depends on the particular circumstances. It is not necessarily excessive just because the individual:

- requested a large amount of information, even if you might find the request burdensome (instead you should consider asking them for more information to help you locate what they want to receive, please see 'Can we clarify the request?');
- wanted to receive a further copy of information they have requested previously (instead you can charge a reasonable fee for the administrative costs of providing this information again);

- made an overlapping request relating to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

When deciding whether a reasonable interval has elapsed you should consider:

- the nature of the data – this could include whether it is particularly sensitive;
- the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed; and
- how often the data is altered – if information is unlikely to have 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 are exemptions and how do they work?

The 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 information requested, depending on the circumstances.

Not all of the exemptions apply in the same way, and 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 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 or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

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, if it is appropriate to do so, you should be transparent about your reasons for withholding information.

Relevant provisions in the GDPR
See Articles 12, 15 and Recitals 58, 63

What should we do if the request involves information about other individuals?

In more detail

What is the basic rule?

Responding to a SAR may involve providing information that relates both to 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 to do so would mean disclosing information about another individual who can be identified from that information, 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 in respect of 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.

Commented [redacted]: I would change this to "you should do so".

What approach should we take?

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

Step 1 – Does the request require the disclosure of 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 individual.

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

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

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

Step 2 – Has the other individual consented?

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

Commented [redacted]: I would suggest highlighting that 'consent' under the GDPR is restrictive and an organisation cannot usually obtain valid consent from its employees due to the imbalance of power.

However, you are not obliged to ask for consent. Indeed, in some circumstances, it may not be appropriate to do so, for instance if it would involve a disclosure of personal data about the requester to the third party.

Step 3 – 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 individual;
- any steps you have taken to try to get the third-party individual's consent;
- whether the third-party individual is capable of giving consent; and
- any stated refusal of consent by the third-party individual.

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 information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed to you with the expectation it remains confidential. This expectation might result from the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence:

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

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

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

What about health, educational and social work data?

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

For health workers, the 'health data test' is met if:

- the information is contained in a health record; and
- the other individual is a health professional who:
    - compiled the record;
    - contributed to the record; or
    - has been involved in the diagnosis, care or treatment of the requester.

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.

For social workers, the 'social work data test' is met if:

- the other individual is:
    - a children's court officer;
    - a person employed by a body in connection with its 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).

For education workers, the 'education data test' is met 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 employed by an education authority in Scotland (as defined by the Education (Scotland) Act 1980) in connection with its 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.

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 social worker is employed by the council 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 requester with the social worker's personal data 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.** If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it is more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, 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. The need to preserve confidentiality for a third party must be weighed 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 has withheld consent.

Do we need to respond to the request?

You need to respond to the requester whether or not you decide to disclose information about a third party. If the third party has given 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 have not got the consent of the third-party 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.

Relevant provisions in the GDPR

See Article 15 and Recital 63

Relevant provisions in the DPA 2018

See Part 7, section 205 and schedule 2, Part 3, Paragraphs 16 and 17

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

There are two parts to this exemption. Firstly, personal data processed for purposes related to crime and taxation 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 the crime and taxation purposes are unlikely to be prejudiced by its disclosure.

Example

A bank conducts an investigation into one of its customers for suspected financial fraud. During its investigation the bank receives a subject access request for all of the personal data it holds from the customer in question. The bank decides that it will withhold information in relation to 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 personal data is processed for law enforcement purposes by competent authorities. If you are an intelligence service under Part 4 of the DPA 2018, please see our guidance on intelligence services processing.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 1, Paragraph 2

Relevant provisions in the 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)

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.

The risk assessment system must be operated by a government department, local authority or another authority administering housing benefit, 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 a SAR would prevent the risk assessment system from operating effectively.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 1, Paragraph 3

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

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 duty of confidentiality is owed by a professional legal adviser to his client.

The English law concept of legal professional privilege encompasses both 'legal advice' privilege and 'litigation' privilege. In broad terms, the former applies only to confidential communications between client and professional legal adviser, and the latter applies to confidential communications between client, professional legal adviser or a third-party, but only where litigation is contemplated or in progress.

The Scottish law concept of confidentiality of communications provides protection both for communications relating to the obtaining or providing of legal advice and for communications made in connection with legal proceedings. Information that comprises confidential communications between client and professional legal adviser may be withheld under the legal

privilege exemption in the same way that information attracting English law 'legal advice' privilege may be withheld. Similarly, the Scottish law doctrine that a litigant is not required to disclose material he or she has brought into existence for the purpose of preparing their case protects information that, under English law, would enjoy 'litigation' privilege.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 4, Paragraph 19

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

Functions designed to protect the public

Personal data is exempt from the right of access if it is processed 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 your functions. If you can comply with a SAR and discharge your functions as normal, you must do so.

The first four functions are:

1. to 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. to protect the public against seriously improper conduct (or unfitness or incompetence);

3. to 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. to 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:

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

The only controllers who can rely upon this are 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:

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

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 2, Paragraph 7

Relevant provisions in the 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)

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

Personal data is exempt from the right of access if it is processed 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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 2, Paragraph 10

Relevant provisions in the 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)

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 2, Paragraphs 11-12

Relevant provisions in the 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)

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 2, Paragraph 14

Relevant provisions in the 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)

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 the exemption is required 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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 5, Paragraph 26

Relevant provisions in the 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

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 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 individual concerned (ie the person the child abuse data relates to).

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

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 5, Paragraph 21

Relevant provisions in the GDPR (the exempt provisions)

See Article 15(1)-(3)

Management information

An exemption applies to personal data that is processed for management forecasting or management planning in relation to 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 plans are revealed 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).

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 4, Paragraph 22

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

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 it should pay. An internal paper sets out the company's position on these matters including the maximum sum it is willing to pay to avoid the claim going to court. If the individual makes a subject access request to the insurance company, it does not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 4, Paragraph 23

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

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 its 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 not assume that a reference is confidential, you must be able to justify why this is the case.

Commented [redacted]: I would suggest further guidance on what should be considered to determine whether a reference is confidential.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 4, Paragraph 24

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 2, Part 4, Paragraph 25

Relevant provisions in the GDPR (the exempt provisions)

See Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3)

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

The GDPR does not cover non-automated information which is not, or is not intended to be, part of a 'filing system'. However, under the DPA 2018 unstructured manual information processed by public authorities constitutes personal data. This includes paper records that are not held 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
- it is estimated 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. Please note that in Scotland the appropriate maximum is £600 for all 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.

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;
- service in any office or employment under the Crown or under any public authority;
- service in 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).

Relevant provisions in the DPA 2018

See Part 2, Chapter 3, sections 21 and 24

Credit files

In the DPA 2018 there are special provisions about the access to personal data held by credit reference agencies. 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.

Relevant provisions in the DPA 2018

See Part 2, Chapter 2, section 13

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?
- Is there a restriction if you are not a health professional?
- 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 his or her health status.

Relevant provisions in the DPA 2018
See Part 7, section 205(1)

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

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 data concerning health 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 it is processed by a court?

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 evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the data to be withheld 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.

Relevant provisions in the DPA 2018 (the exemption)
See Schedule 3, Part 2, Paragraph 3

Relevant provisions in the 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)

Is health data exempt if disclosure goes against an individual's expectations and wishes?

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 2, Paragraph 4

Relevant provisions in the 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)

Is health data exempt if disclosure could cause serious harm?

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 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.

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

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.

Relevant provisions in the DPA 2018 (the exemption)
See Schedule 3, Part 2, Paragraph 5

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

Is there a restriction if you are not a health professional?

This is a restriction rather than an exemption. It restricts you from disclosing health data in response to a SAR if you are not a health professional 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 health data has already been seen by, or is known by, the individual it is about.

'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).

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

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

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 a SAR cannot be used 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?

The DPA 2018 defines 'education data' as:

- personal data which consists of information that forms part of an educational record; but

- is not health data.

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 kept by a teacher 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 about the pupil provided by the parent of another child is not part of the educational record.

Relevant provisions in the DPA 2018

See Schedule 3, Part 4, paragraphs 13-17

How can education data be accessed?

There are two distinct rights to information held about pupils by schools:

- the pupil's right of access under Article 15 of the GDPR; and

- 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 is only concerned with the right of access under the 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 personal data processed by a school 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 regulatory responsibilities of the ICO, but we refer to it here for completeness.

Unlike the parent's right of access to their child's educational record, the right to make a SAR is the pupil's right. Parents are only entitled to 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?

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?'.

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 it is processed by a court?

This exemption can apply to education data processed by a court.

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

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the education data to be withheld 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.

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

Relevant provisions in the 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)

Is education data exempt if disclosure could cause serious harm?

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 4, Paragraph 19

Relevant provisions in the GDPR (the exempt provisions)

See Articles 15(1)-(3)

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 his 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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 4, Paragraph 20

Relevant provisions in the GDPR (the exempt provisions)

See Articles 15(1)-(3)

Social work data

In more detail

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.

Relevant provisions in the DPA 2018

See Schedule 3, Part 3, paragraph 7-8

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

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, information that identifies a professional, such as a social worker, carrying out their duties should not

normally be withheld 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 it is processed by a court?

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

- processed by a court;
- supplied in a report or evidence given 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.

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

Relevant provisions in the 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)

Is social work data exempt if disclosure goes against an individual's expectations and wishes?

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
- someone 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 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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 3, Paragraph 10

Relevant provisions in the 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)

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

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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 3, Paragraph 11

Relevant provisions in the GDPR (the exempt provisions)

See Articles 15(1)-(3)

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

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 his or her 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.

Relevant provisions in the DPA 2018 (the exemption)

See Schedule 3, Part 3, Paragraph 12

Relevant provisions in the GDPR (the exempt provisions)

See Articles 15(1)-(3)

Can the right of access be enforced?

In more detail

What enforcement powers does the ICO have?

Anyone has the right to make a complaint to the ICO about an infringement of the data protection legislation 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 have failed to comply with data protection legislation. For example, we could issue a controller or processor with a warning, a reprimand, an 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 there must be a contract in place between the controller and processor. The contract must state that the processor will assist the controller with its 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 SAR be enforced by a court order?

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 rights under the data protection legislation – including, of course, by failing to comply with a SAR – they are entitled to claim compensation from you. This right can only be enforced through the courts. You will not be liable if you can prove that you are not in any way responsible for the event giving rise to the damage.

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

It is a criminal offence to require an individual to make a SAR, in certain circumstances and in relation to certain information.

Is it a criminal offence to destroy and conceal information?

It is a criminal offence, in certain circumstances, 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.

Relevant provisions in the GDPR

See Articles 77, 82 and Recitals 141, 146

Relevant provisions in the DPA 2018

See Part 6 and Part 7, section 184

Further reading

Regulatory Action Policy
Contracts and liabilities between controllers and processors

Commented [redacted]: I would suggest more detail on this.

Commented [redacted] I would specify these circumstances.