About this guidance

This guidance discusses the right of access to information processed for a law enforcement purpose under Part 3 of the Data Protection Act 2018 (DPA 2018) 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 under Part 3 in practice. It is aimed at 'competent authorities' who process personal data for any of the law enforcement purposes, and particularly at DPOs and those with specific data protection responsibilities in the context of law enforcement processing.

If you haven't yet read the 'in brief' page on the right of access under Part 3 of the DPA 2018 in the Guide to Law Enforcement processing, 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.

This guidance should be read alongside the detailed UK GDPR guidance on the right of access. You should read this guidance if you have specific questions about dealing with subject access requests (SARs) in the context of law enforcement processing.

You should also read the separate law enforcement guidance on 'manifestly unfounded and excessive requests', and you can access it **here [link to be added post-consultation]**.

Where your processing operations are for general purposes only, you should refer to the right of access guidance under the UK GDPR. You can access the UK GDPR detailed right of access guidance **here**.

Contents

How should we supply Part 3 information to the requester?

Can we restrict the right of access under Part 3?

What should we consider when acting as joint controllers?

What should we do if the Part 3 request involves information about other individuals?

What do we need to consider if personal data is processed by a court for law enforcement purposes?

Can the right of access be enforced under Part 3?

Is it a criminal offence to destroy and conceal information?

What is the right of access in Part 3 of the DPA 2018?

In detail

What is the right of access in the context of law enforcement processing?

The UK GDPR does not apply to personal data processed for any of the law enforcement purposes. There is a separate regime in Part 3 of the DPA 2018 which provides that individuals have a right to access their personal data processed for a law enforcement purpose. An individual is entitled to ask for their personal information under section 45(1).

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. Requests made under the right of access are usually called subject access requests (SARs).

The right of access 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. You must publicise the right of access using appropriate methods, for example, on your website, in your privacy statement, or in your other communications with individuals. For further details on privacy information, please see our Part 3 guidance on the right to be informed.

You should only use Part 3 for responding to SARs if you are a competent authority **and** you are processing for one of the law enforcement purposes. Please refer to the 'Guide to Law Enforcement Processing' to help you decide

if you are a competent authority. You may also find it helpful to refer to our guidance, 'Which regime'.

The law enforcement purposes are defined under section 31 as,

Quote

"…the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

So if you receive a SAR for personal data processed for one of these purposes, you should use Part 3 to deal with it.

What does "safeguarding against and the prevention of threats to public security mean?"

Whilst many competent authorities are responsible for protecting or preventing threats to public security, not all public security measures are linked to criminal law enforcement.

The language of section 31 makes it clear that the law enforcement purposes are for the prevention, investigation, and detection of criminal offences, or the execution of criminal penalties. This definition also **includes** actions and measures taken to prevent threats to public security. However, in order to be Part 3 processing, these threats to public security must fit broadly within the wider law enforcement purposes of preventing, investigating, detecting or prosecuting crime, or executing criminal penalties. For example, safeguarding against threats to public security may apply to covert surveillance or video surveillance for the purposes of prevention and detection of crime.

This distinction is important, because public security has much broader scope than criminal law enforcement. For example, it may also cover responses to major incidents, such as accidents or natural disasters, or policing large events. These matters are not usually linked to criminal offences or criminal penalties. Personal data collected for the purposes of dealing with these types of public security incidents should therefore be processed under the UK GDPR and not Part 3. For further details, see 'How do we decide which SARs regime applies?'

What information is an individual entitled to under Part 3?

The right of access under Part 3 gives individuals the right to obtain the following from a controller:

- confirmation that you are processing their personal data;
- access to their personal data; and
- other supplementary information.

You should provide the individual with a copy of their personal data, and other supplementary information, in writing, where practicable. For further details on the supplementary information see, 'What other information is an individual entitled to under Part 3?'

In most cases, you can confirm whether you are processing an individual's personal data in general terms. However, this will depend on the nature of the request. If the request is for a specific piece of information, you should generally be able to confirm or deny whether you are processing the information unless a restriction applies – see 'Can we restrict the right of access under Part 3?'. However, depending on the circumstances, and due to the sensitivities of law enforcement processing, you may not be able to be fully transparent with the individual about the nature of the processing or whether you hold the data - see 'When can we neither confirm nor deny we hold the information?'.

You should ensure that your processing is lawful and fair, and you should aim to be as open and transparent as possible with individuals about how you process their personal data.

However, in some circumstances transparency can undermine your law enforcement activities, and you may be unable to confirm or deny whether you are processing personal data. However, you may only restrict an individual's right of access, if one of the restrictions listed in section 45(4) applies. See, 'Can we restrict the right of access under Part 3?'

What other information is an individual entitled to under Part 3?

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 and lawful basis for processing;
- categories of personal data you're processing;
- recipients or categories of recipient you have disclosed 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 of the data being processed;
- the individual's right to lodge a complaint with the Information Commissioner's Office (ICO);
- communication of the personal data being processed; and
- any available information about the source of the data.

When responding to a SAR, you must remember to supply this information in addition to a copy of the personal data itself, even if the individual does not specifically ask for it. If you provide this information in your privacy notice, you may provide a link to or a copy of your privacy notice. Please see our Part 3 guidance on the right to be informed for further details.

You should provide the exact retention period for storing the personal data if you can. You should only provide the criteria for determining how long you will store the information instead, if it is not possible to provide the exact period. This may be the case if your retention policy does not cover the requested information, or you have restricted the individual's right of access to their information. You should keep a record of the reasons why you were unable to provide details of the exact retention period.

In processing personal data for a law enforcement purpose, you are required to make a distinction, where possible, between the different categories of individuals whose data you process. You may process personal data for a law enforcement purpose about a suspect, offender, complainant, victim, witness, informant, or any other person. It is important to remember that how you categorise an individual may have a bearing on what information

you are able to provide, how you search for information (eg if it is held in different contexts), or if you need to restrict an individual's right of access to their data. See 'Does the categorisation of data subjects impact what information we should provide them with?' and 'How should we deal with requests from individuals who fall within multiple categories?' For further details, see our guidance on 'Categorisation'.

Are individuals only entitled to their own personal data?

In most circumstances 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; or
- they are exercising another individual's right of access on their behalf.

Before you can respond to a SAR, you need to decide whether the information you hold is personal data and, if so, who it relates to. For information to be personal data, it must relate to a living person who is identifiable from that information (directly or indirectly). The context in which you hold information, and the way you use it, can have a bearing on whether it relates to an individual and therefore if it is the individual's personal data.

In most cases, it is obvious whether the information is personal data, but we have produced guidance on 'What is personal data?' to help you decide if it is unclear.

The same information may be the personal data of two (or more) individuals. You may be able to restrict the individual's right of access to their information, if it contains personal data relating to another person. Please see 'What should we do if the Part 3 request involves information about other individuals?' for further details.

Who is responsible for responding to a request?

Controllers are responsible for complying with SARs, not processors. If you use a processor, you need to have contractual arrangements in place to guarantee that you can deal with SARs properly, irrespective of whether they are sent to you or the processor. The processor must help you meet your obligations for SARs and you should make this clear in the agreement between your two parties. Our UK GDPR guidance on contracts between controllers and processors provides further relevant information.

In some cases the processor may hold personal data on your behalf. If so, you should be able to require the processor to search for this data and, if necessary, give you a copy. However, it is still your responsibility to decide how the request is dealt with and responded to.

If you are a joint controller, you need to have an arrangement in place with your fellow joint controller(s) which sets out each of your responsibilities, including how you deal with SARs. Under Part 3, you **must** specify a central point of contact for individuals, which **must** be one of the joint controllers. See, 'What should we consider when acting as joint controllers?'.

When do we need to take action to enable an individual to make a SAR?

Individuals have a right to be informed about how you are processing their personal data and you should, where possible, be open and transparent about what data you process about them, and why you are processing it. By letting individuals know that you are processing their personal data, this will greatly assist them in exercising their right of access under Part 3.

There may be circumstances in which individuals are unlikely to be aware that you process data about them, or have enough information to be able to make a SAR, should they wish. This is likely to be the case where you obtain the information from a source other than from the individual themselves.

You must provide the individual with the following information – unless you have a legitimate reason for withholding it:

- your lawful basis for processing;
- your retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- if applicable, recipients or categories of recipient you have disclosed the personal data to (including recipients or categories of recipients in third countries or international organisations); and
- any other information the individual needs to be able to make a SAR.

You should engage with the individual as appropriate, eg by contacting them directly or directing them to the privacy information on your website.

However, if you are processing information for law enforcement purposes, in some instances you may not be able to be fully transparent with individuals about what information you are processing about them. This does not mean you do not need to provide privacy information at all, as you are still under an obligation to inform the individual of the processing, unless you are able to lawfully restrict the individual's right to be informed.

You can only restrict an individual's right to be informed in certain circumstances. For further details on when you may restrict the individual's right to their privacy information, please follow the approach outlined in the chapter, 'Can we restrict the right of access under Part 3?'

Any decision on whether you can restrict the individual's right to any of their privacy information should be considered on its own merits, and separately from any decision about whether you need to confirm the information is held, or restrict the individual's right of access. However, the relevant provisions under section 44(4) which permit you to restrict access to the individual's privacy information, are broadly similar to the relevant provisions which allow you to restrict the individual's right to access their personal information.

In deciding whether to restrict the individual's right to be informed, you also need to carefully consider the impacts this measure may have on the rights and freedoms of the individual. See 'What is a necessary and proportionate measure?, and 'What rights and freedoms may be impacted by restricting an individual's right of access?'.

Where possible, you should provide the individual with as much of their privacy information as you can. As circumstances change throughout the lifecycle of a criminal case, you may be able to provide the individual with more information than you were able to at the start. Sometimes you will only need to restrict the right for a specified period of time – for further details, see, 'Can we restrict the right of access for a specified period of time?'

Relevant provisions in the legislation

See DPA 2018 Sections 43-45; 55-59; and 64-65

Further reading – ICO guidance/European Data Protection Board

UK GDPR guidance on 'contracts between controllers and processors'
UK GDPR guidance on 'controllers and processors'
UK GDPR guidance on DPIAs
Guide to Law Enforcement Processing
Part 3 guidance on the 'right to be informed'
Part 3 guidance on 'Categorisation'

How do we recognise a Part 3 subject access request (SAR)

In detail

What is a Part 3 subject access request (SAR)?

A Part 3 SAR is a request made by or on behalf of an individual for the information they are entitled to ask for under section 45(1).

Are there any formal requirements?

No. Part 3 does not set out formal requirements for a valid request. Therefore, an individual can make a SAR verbally or in writing, including by social media. They can make it to any part of your organisation. They do not have to direct it to a specific person or contact point, or tell you why they are making the request, or what they intend to do with the information. However, it is generally good practice to have a single contact point for SARs. If you are a joint controller, you **must** ensure that you designate a "contact point" for individuals who wish to make SARs. This should be covered in your joint controllership arrangements. See 'What should we consider when acting as joint controllers?'

It is good practice to have a policy for recording details of all the requests you receive. We recommend that you keep a log of any verbal requests you receive as these will also be considered valid SARs.

A request does not have to include the phrases "subject access request", "right of access", or "section 45(1) of the DPA 2018". It just needs to be clear that the individual is asking for their own personal data. Indeed, a

request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) or the Freedom of Information (Scotland) Act 2002 (FOISA).

Do we have to respond to the SAR if the individual has an alternative means of accessing their information?

In most cases, yes. A request may still be valid even if the individual has the option of using another statutory or legal route to obtain their information. Bear in mind that individuals do not have to tell you their reason for making the request or what they intend to do with the information. However, if you are aware that an individual is seeking their data for a specific purpose, eg for court proceedings, it is good practice to remind them that they will only be able to obtain their own personal data by making a SAR, and not information about other individuals.

You may explain to the individual what other routes may be available to them for obtaining their information. However, you cannot refuse to comply with a SAR just because an individual has an alternative means of accessing their personal data.

Example

An individual who was injured in a road traffic collision makes a SAR to the police for the purposes of pursuing a civil claim for damages against the driver responsible for the accident.

The police are aware that the individual will be able to obtain this information through other legal mechanisms once they bring a claim. In responding to the SAR, the police are aware they will need to redact the personal data of other individuals before disclosing it. As the information will be redacted, the police expect that it may have limited use as evidence at court.

However, the police cannot refuse to comply with the SAR just because there is an alternative route of access open to the individual.

The police contact the individual and explain that they will need to redact some of the information. They also suggest that it would be a good idea for the individual to discuss the matter with their solicitor, as there may be other legal methods of obtaining the information they need. However, they also make it clear that the individual is entitled to make a SAR for this information.

If the individual still wants to make a SAR, the police should respond within one month of first receiving the request.

If they are the subject of a criminal case, it is likely that information about the defendant will be provided under an alternative statutory process. For example, in England, Wales, and Northern Ireland, information may be disclosed under the Criminal Procedure and Investigations Act 1996, or in Scotland, under the Criminal Justice and Licensing (Scotland) Act 2010.

However, just because the individual's personal data has **already been disclosed** under another process does not mean you do not need to comply with the SAR. Under statutory disclosure rules, an individual may not have received all of the personal data held about them, or only have had an opportunity to inspect their data, and may not have received a copy. If the

individual makes a SAR, you should consider their request under Part 3, and, where possible, provide them with a copy of their information. If it's not possible to provide a copy, you should give them an opportunity to re-inspect the data you hold about them. Inspecting information for the purposes of defending a criminal case is a very different endeavour to inspecting information to verify the lawfulness of the processing. See 'What information must we supply under Part 3?'

You may also hold additional information about the individual which was not required to be disclosed under another statutory process or relevant guidelines, or new information about the individual which did not exist at the time of the criminal proceedings. This information is potentially disclosable further to a SAR, particularly as the individual did not already receive it under another disclosure mechanism.

Also bear in mind that alternative disclosure mechanisms may not involve direct disclosure to the individual themselves, as the information may be provided to the individual's lawyers. Whilst lawyers are generally under an obligation to make their client aware of all material information in their possession, you should not assume that the individual has been able to access any or all of their information just because it has been made available to their lawyer through another process. You should carefully consider the circumstances of the request, particularly where an individual may have changed their legal representative.

However, if you have already provided a copy of the data to the individual through an alternative disclosure mechanism, this may be a factor to consider in deeming a SAR as manifestly unfounded or excessive. For further details, see our guidance on 'manifestly unfounded and excessive requests.

For more information about when you may be able to restrict an individual's right of access, see 'Can we restrict the right of access under Part 3?'

Can an individual ask a third party to make a SAR on their behalf?

An individual may prefer a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. In the context of criminal justice and law enforcement, it will not be uncommon for individuals to ask their solicitor to act on their behalf. Part 3 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. Please follow the recommendations in our UK GDPR detailed

right of access guidance – 'Can an individual make a request on behalf of someone?'

If a third party makes a SAR on behalf of an individual, you should respond to the request as if you were responding directly to the individual themselves.

Example

A requester makes a SAR to the Planning Service on behalf of their mother, who is being prosecuted for failure to comply with an Enforcement Notice to remove an illegal house extension. The requester is appropriately authorised to act on their mother's behalf, and to obtain the information. The Planning Service is satisfied that it is appropriate to release the information to the requester.

However, the information contains some personal data of the requester who is acting on behalf of their mother. The requester's personal data contains important context about the circumstances of the prosecution. However, the Planning Service must deal with the SAR as if it had been made by the individual themselves. As it is releasing the information directly to the requester, it contacts them to enquire whether they are happy for their personal data to be disclosed in the response.

However, if the Planning Service sends the response directly to the mother, it should redact the personal data of the requester, as it would have done if the mother had made the SAR themselves. If the Planning Service is unable to contact the requester to check their preference, it should err on the side of caution and redact the requester's personal data.

In circumstances where an individual has appointed a legal representative or other professional to act on their behalf, you may receive repeat requests for information which you have previously disclosed, for example, if the individual changes their representative. How you respond may depend on the circumstances, and on any other laws or policies you are subject to. It is important that you document the reasons for your decision.

Depending on the circumstances, you may also consider such requests to be manifestly unfounded or excessive. For details on responding to manifestly unfounded or excessive requests, please see our Guide to Law Enforcement processing – 'Manifestly unfounded or excessive requests'.

Example

A solicitor makes a SAR to the prosecution service on behalf of an individual who was convicted of assault occasioning actual bodily harm. The prosecution service discloses the information. Several weeks later, the individual changes their solicitor who makes a request for the same information.

The prosecution service considers the SAR as if it had been made by the individual themselves. This means that it may view the SAR as a repeat request, which means the manifestly excessive provisions may apply to the information which has already been disclosed. However, depending on the circumstances, the prosecution service may still decide to provide this information. For example, it may consider any relevant legislation, policies, or other matters, including any difficulties the individual might have in obtaining the information, or the impact on the individual if it does not provide the information.

However, if it has obtained any new information since responding to the previous request, it should provide it unless a restriction applies. It is important that the prosecution service documents the reasons for its decision.

In cases where information has been disclosed through another statutory process – see the previous section, 'Do we have to respond to the SAR if the individual has an alternative means of accessing their information?'

You may also receive requests for information made on behalf of an individual through an online portal. For further details on how to respond to these types of requests, please refer to our UK GDPR detailed right of access guidance – 'Do we have to respond to requests made via a third party online portal?'

If you receive requests by or on behalf of children or young people, please refer to our UK GDPR detailed right of access guidance – 'What about requests for information about children or young people?'

How do we decide which SARs regime applies?

Before responding to a SAR, you need to determine whether you are processing the personal data for general purposes or for any of the law enforcement purposes. Identifying the correct regime is important as there are many key differences between the UK GDPR and Part 3. You may also process information for more than one reason.

If your primary purpose for processing the information is for one of the law enforcement purposes, you should deal with the SAR under Part 3. If you are processing the information for general purposes, you should deal with the SAR under the UK GDPR (the general processing regime).

As a competent authority, it is very likely that you are also processing personal data for general purposes, eg HR information that you hold about your employees. In many cases, although you are a competent authority, you may be required to carry out public functions for purposes other than law enforcement. In these circumstances, the processing of personal data will come within the UK GDPR and not Part 3. For example, police and other agencies may be required to deal with public emergencies or disasters such as floods, fires or industrial accidents. They may also need to deal with incidents linked to safeguarding and mental health.

Example

A seaside town regularly experiences flooding. The police work with other agencies in developing an incident response plan, which explores how to prevent future floods, and how best to protect human life and property should future incidents occur.

Whilst dealing with such emergencies is an important policing function, it is not criminal law enforcement. Any of the personal data police collect in relation to this matter should therefore be processed under the UK GDPR. If police receive a SAR from an individual whose data they process for this purpose, they should deal with it under the UK GDPR – not Part 3.

For discussion on the types of public security matters covered by Part 3, see 'What does "safeguarding against and the prevention of threats to public security mean?".

If you process the same personal data for more than one purpose, eg for a law enforcement purpose and for general purposes, you will need to identify your **primary purpose** for processing the information.

What is the 'primary purpose' for processing?

The term 'primary purpose' is not defined in the legislation but will generally mean your principal objective for the processing. It does not necessarily mean your original purpose for collecting the data, although it can mean this.

Usually, it will be obvious what your primary purpose is. You cannot process personal data under either the UK GDPR or Part 3 unless you have identified an appropriate lawful basis. If you collect personal data to investigate a crime, then you are likely to be processing it under Part 3. If you process personal data about an employee's health condition, it is likely to fall within the general processing regime.

Your principal objective for processing the information may change over time. You may begin processing information under one regime, but as circumstances progress and the purpose changes, the processing of the data will come under another regime or take place under both simultaneously.

You may initially be processing data for general administrative purposes, but as the situation changes you may identify elements of criminality. The processing would then come under Part 3. It may be easier to identify a change in regime if the data is passed to a specialist team or department to continue the processing for a specific purpose. For example, a dedicated fraud unit may obtain information originally collected under the general processing regime to use for the purposes of an investigation under Part 3.

In general, any information you obtain in connection with your law enforcement purposes is likely to be processed under Part 3. This can include (but is not limited to):

- information you discover, seize, or download as part of an investigation;
- expert reports (eg medical or forensic);
- legal advice; or
- information provided to you by third parties.

If your primary purpose for processing the information is for any of the law enforcement purposes, you should use Part 3 to respond to the SAR, even if you also process the data for another non-law enforcement purpose.

Example

Police process information about a disciplinary matter between two civilian staff members in the course of their employment. There is an ongoing dispute between the individuals, which has resulted in numerous arguments and allegations of harassment and bullying by both parties. The police are processing this information under the UK GDPR, and dealing with it in accordance with standard policies.

However, whilst investigating the matter, the police identify potential criminal issues. Following this, the investigation into the matter becomes a criminal investigation.

Both individuals make a SAR for the personal data held about them in relation to this matter. As it is now being treated as a criminal investigation, the SARs should be dealt with under Part 3.

However, you should take a practical, common-sense approach. If your employee's human resources file becomes part of your criminal investigation, the primary purpose for processing the data which is clearly relevant to your investigation, is likely to be law enforcement.

You may need to consider your original purpose for processing the data to determine the primary purpose for processing information which is not relevant to your criminal investigation.

Example

The police receive a SAR from a civilian staff member for details of their medical absences within the last 3 years. The individual's human resources file contains information relevant to a criminal investigation.

However, the police decide that details about the individual's medical absences is not relevant to the current investigation.

As the requested data is not being processed for a law enforcement purpose, the police consider their original purpose for processing the data. The primary purpose for processing details of the individual's medical absences, is for human resources reasons. The police deal with the SAR under the UK GDPR.

However, if your original purpose for collecting the information was for any of the law enforcement purposes, and you don't have an underlying lawful basis under Article 6(1) of the UK GDPR for processing the data, you may not be able to process the data under the UK GDPR.

Section 36(4) states,

Quote

"Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law."

If you want to repurpose law enforcement data to use for general processing, you must have appropriate 'authorisation' in law for doing so. In addition, you must ensure that your further processing is lawful under the UK GDPR.

For further details, please refer to our guidance on Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR and Part 2 DPA 2018 – Part 3 to Part 2 DPA 2018 data sharing.

If you collect bulk information for a law enforcement purpose, eg to investigate a crime, you may incidentally collect some irrelevant information.

However, just because some of the information you collected may not be relevant to your criminal investigation, does not mean you will automatically be processing it for general purposes. You can only process personal data under the general processing regime if you have a lawful basis for doing so under Article 6(1) of the UK GDPR. As you obtained the information for the purposes of a criminal investigation, you do not have an underlying lawful basis under the UK GDPR for processing it. Since you collected the data under Part 3, you are therefore still processing it under Part 3.

While you may not have any use for this irrelevant data, you are still required to store it in line with your retention and disposal schedule (at least until you have completed sifting it to determine if it is relevant or not). In general, if information is irrelevant for your law enforcement purposes, you should, where possible, limit its further processing, and ensure you don't keep it longer than necessary. You may also need to consider other regulations governing the use and retention of law enforcement data.

You will need to comply with SARs, and other requests by individuals in the exercise of any of their lawful rights under the data protection legislation. So in these circumstances, if the individual makes a SAR "for all the information you hold about me", you should deal with their entire request under Part 3 – not just those elements of the SAR that relate to your criminal investigation. This is because all the data, including the irrelevant data, was collected for a law enforcement purpose. Obviously, if you already process data about the individual under the UK GDPR, you will need to provide that information under the general processing regime.

Example

Police seize a number of laptops and phones from an individual for the purpose of investigating allegations that the individual possesses images depicting child sexual abuse. Having determined that it is strictly necessary to do so, police extract the data stored on the devices. On reviewing the extracted material, they find some incriminating evidence, but also a large amount of personal data, including the individual's own bank and credit card details, some health information, along with photographs of the individual, their friends and family. Some of this information may not be relevant to the offences under investigation.

The individual makes a SAR for all the information the police have extracted from their devices. However, the police have not finished sifting the data, to decide what is or is not relevant to the investigation. They decide that disclosing any of the personal data relevant to the suspected crimes could be prejudicial to the investigation. Therefore, they decide to restrict the individual's right of access to the relevant information.

The information which was collected incidentally (such as bank details, health data and family photos) is still being processed under Part 3, as the primary purpose for collecting the information was for a law enforcement purpose.

Just because some of the data is unlikely to be relevant to the investigation does not bring it within the remit of the UK GDPR. The primary purpose of processing the information is clearly for law enforcement – the investigation of crime. Therefore, the police do not have a lawful basis for processing the information under the UK GDPR, and should deal with the SAR under Part 3 of the DPA 2018.

It is for the controller to determine which SARs regime is appropriate to use, depending on the circumstances. There may be occasions where you receive requests which cover personal data being processed separately under both

regimes. In these circumstances, you will need to consider the SAR under both the general processing regime under the UK GDPR, and also Part 3 – see 'How do we deal with requests for information processed for different purposes?'

If your processing under any of the law enforcement purposes is 'sensitive processing', see our guidance on 'What is sensitive processing?'

What if the primary purpose is not obvious?

In some circumstances, your primary purpose for processing the information may not be entirely clear. Therefore, you may need to exercise your discretion in order to identify what your primary purpose is. It may be helpful to consider the following factors:

- your reasons for collecting or obtaining the information;
- any legislation that forms the basis of your processing, and whether it has an underlying law enforcement purpose;
- whether your purpose for processing has changed;
- any relevant policies; and
- any other relevant circumstances.

In such cases, it is very important that you document the reasons for your decision.

Example

A suspect is being detained in a custody suite on suspicion of having committed an offence. The suspect has a pre-existing medical condition which requires them to take medication at regular intervals.

The custody officer has been provided with medical information about the suspect's medical condition in order to enable them to self-administer their medication. The suspect makes a SAR for all the information held about them.

Whilst the information relating to the criminal offence will clearly be dealt with under Part 3, the controller needs to decide whether their primary purpose for processing the medical data is under the UK GDPR, or Part 3. They may consider any relevant legislation or policies (eg regarding the care and welfare of detainees at police stations), or any other matter. They should also document the reasons for their decision.

At what point do we decide which SARs regime applies?

You should usually consider the SAR under the regime you are using to process the information at the time the request is received.

For example, if you receive a SAR for data you collected for a law enforcement purpose several years ago but have since repurposed it under the general processing regime, then it will usually be appropriate to consider the request under the UK GDPR, and not Part 3. However, this may depend on the circumstances, and you should adopt a pragmatic and flexible approach. You should also document the reasons for your decision. For further details about how to deal with SARs under the UK GDPR see our UK GDPR guidance on the right of access.

If your primary purpose for processing changes after you receive the request and before you respond to the individual, it will usually be appropriate to consider the SAR under the processing regime which applied on the date the request was received. It may be impractical to change SARs regimes after you have received and logged the request. However, you should be prepared

to take a flexible approach and have regard to the specific circumstances of the request.

Example

A financial regulator is processing an application for registration. It receives a SAR from the applicant on 9 March for "all the information you hold about me." The regulator logs the SAR. On 16 March it discovers evidence of fraudulent activity by the applicant.

The staff processing the application send the file to their enforcement department. The file then becomes part of a criminal investigation. While the original purpose for processing the application was for general purposes, as soon as the file passes to the enforcement department to launch a criminal investigation, the primary purpose for processing becomes for one of the law enforcement purposes – the investigation of crime.

However, the regulator must still comply with the SAR they received on 9 March. It should generally consider the SAR under the UK GDPR – which was the relevant regime at the time the request was received. It may also consider whether it would be appropriate to apply a UK GDPR exemption, eg crime and taxation, in respect of the data now being processed for a criminal investigation. The regulator should consider liaising with the enforcement department before responding to the request, if there is a risk that disclosing the information may, for example, prejudice the investigation.

Depending on the circumstances, the regulator may decide that it would be appropriate to deal with the request under Part 3 instead. If it does take this approach, it must be able to justify why it is taking this approach.

Please also see our detailed right of access guidance in Our Guide to the GDPR: 'What other exemptions are there? – Crime and Taxation'.

Relevant provisions in the legislation

See UK GDPR Article 6 and Recitals 40-41, 44-49, and 50
See DPA 2018 sections 36(4) and 45

Further reading – ICO guidance

UK GDPR detailed right of access guidance:
'Do we have to respond to requests made via a third party online portal?';
'What about requests for information about children or young people?'

Guide to Law Enforcement Processing:
Manifestly unfounded and excessive requests;
Law Enforcement Processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR and Part 2 DPA 2018.

What should we consider when responding to a Part 3 request?

In detail

How long do we have to comply?

You must comply with a Part 3 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 (you should follow the UK GDPR right of access guidance, '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 first day after 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

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

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 public holiday, you have until the next working day to respond. This means that the exact number of days you have to comply with a request varies, depending on the month in which an individual makes the request.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may also be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

As the time limits are different in the UK GDPR, you may if you wish, apply the shorter time limit (under the UK GDPR) to all SARs you receive.

For further details on how to calculate the time limit when you receive a SAR under the UK GDPR, see the UK GDPR detailed right of access guidance – 'How long do we have to comply?'

Can we extend the time for a response?

Unlike the UK GDPR, Part 3 does not allow you to extend the period for responding to complex requests, or if you have received a number of requests from an individual.

Section 54(2) allows for the Secretary of State to specify a longer time period for responding to SARs by way of regulations. However, at present there are no regulations in place. As such, you must respond to Part 3 SARs within one month.

If both the UK GDPR and Part 3 data is covered by the SAR, can we deem the request complex and extend the deadline?

You may only consider a mixed data SAR (ie one that contains both UK GDPR, and Part 3 information) to be complex in respect of the data you process under the UK GDPR. You should therefore not consider a request to

be complex on account of the fact it contains information processed under both SAR regimes.

You should provide the Part 3 information within the one month deadline, even if you have extended the time limit for responding to information processed under the UK GDPR. See above, 'How long do we have to comply?'

However, if you wish to provide all the information at the same time, you should ensure that you comply with the request under the normal time limits for responding to a Part 3 SAR. See 'How long do we have to comply?'

How do we deal with requests for information processed for different purposes?

There may be circumstances in which you will need to consider requests for information processed under both the UK GDPR and Part 3. For example, where an individual requests "all the information you hold about me", some of the data you process may be for a law enforcement purpose, eg a criminal investigation, and some of it may be for general purposes, eg human resources reasons.

You may need to separately consider the information you hold under both regimes in order to respond. As the time limits differ between the two SAR regimes (and there are no provisions in Part 3 to extend the time to respond), there may be circumstances in which you will need to provide separate responses.

However, you are not required to provide the information separately, as long as your cover letter clearly explains which regime you have used to disclose each specific piece of information (although this may not always be possible if you need to restrict the individual's right of access to this information). In most cases, it will be appropriate to provide all the information to the individual at the same time. However, you should bear in mind that SARs under the UK GDPR, and Part 3, will be subject to different time limits.

Example

A local authority receives a SAR from an individual for "all the information you hold about me". In order to respond to the request, it needs to provide the information it processes about the individual under both the UK GDPR, and Part 3 SARs regimes.

The authority has deemed the UK GDPR information to be complex, as it processes a large quantity of data about the individual, and it is unclear, from the request, what information the individual is actually looking for. As such, it extends the time limit for responding to this element of the request by two months. However, the authority is aware it must provide the Part 3 information within one month.

The authority holds a number of documents which contain personal data that it processes about the individual under both the UK GDPR, and Part 3 of the DPA 2018. The authority considers that it would be very impractical, and costly, to extract the UK GDPR and Part 3 information from the documents to respond to the SAR. It would be much more efficient to provide the individual with copies of the documents.

In the circumstances, the authority decides to provide the individual with copies of the documents. However, while the deadline for responding to the request has been extended in relation to the UK GDPR information, the authority must ensure it provides copies of all the personal data contained in the documents within the Part 3 timeframe.

If you are providing information processed under both regimes at the same time, you should respond within the shorter time limit, to ensure that you are complying with the statutory time limits in respect of both UK GDPR and Part 3 information. Also see above, 'How long do we have to comply?'

If you need to withhold or restrict an individual's right of access to their information, you should explain your reasons to the individual, unless providing reasons would undermine the purpose of the relevant provision you rely on. See, 'Do we need to tell individuals why their rights have been

restricted?' and for UK GDPR SARs, see the UK GDPR right of access guidance – 'What should we do if we refuse to comply with a request?'

Can we clarify the request in Part 3?

Yes. You may ask an individual to specify the information or processing activities their request relates to before responding to the SAR. For example, you may wish to seek clarification if you process a large volume of data about an individual, or where it is not clear what information the individual is requesting. It is good practice to check with the individual if you are not sure.

You can ask the requester to provide additional details about the information they want to receive, such as the context in which it may have been processed and the likely dates when processing occurred. However, you cannot require an individual to narrow the scope of their request, as they are 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. Please see our UK GDPR guidance on the right of access – 'What efforts should we make to find information?' for details about the extent to which you must search for information.

However, unlike under the UK GDPR, **the time limit is not paused** while you wait for a response, so you should ask for clarification as soon as possible.

Under Part 3, you must make, where relevant and as far as possible, a clear distinction between different categories of personal data, such as people who are suspects, convicted offenders, complainants, victims, witnesses or informants. How you categorise individuals may help you to target your searches appropriately. See, 'Does the categorisation of individuals impact what information we should provide them with?' and also refer to the Part 3 guidance on 'Categorisation'.

If both UK GDPR and Part 3 data is covered by the SAR, can we stop the clock and request clarification under the UK GDPR?

If you process information under both the UK GDPR and Part 3, you may only pause the time limit whilst you ask for clarification in respect of the UK GDPR information. For further details, see our UK GDPR right of access guidance – 'Can we clarify the request?'

As the clock does not stop in relation to the Part 3 information, you should try to provide it, or if relevant, make the individual aware that you have restricted access to it, within the one month time limit.

If the Part 3 information is inextricably linked to, or otherwise not separately searchable from the rest of the information, eg if it is contained within the same document, you can only still stop the clock in relation to the data processed under the UK GDPR (provided that you genuinely need to, and you process a large volume of information about the individual).

However, if you have stopped the clock in respect of data processed under the UK GDPR, but you wish to provide all the information at the same time, you should ensure that you comply with the request under the normal time limits for responding to a Part 3 SAR. See 'How do we deal with requests for information processed for different purposes?', and 'How long do we have to comply?'

Example

An employee of the Land Registry makes a SAR "for all the information you hold about me concerning disputes or investigations".

The Land Registry processes a large volume of information about the individual, who was involved in a number of disputes and investigations, some of which are still ongoing. They were involved in a property dispute with their next-door neighbour several years ago. There was a grievance between the individual and other employees, and the individual made a complaint to the Land Registry about its handling of a freedom of information request. The individual is currently in the process of buying a house and the Land Registry is investigating allegations of fraudulent activity on the part of the vendor. The fraud investigation is being processed under Part 3 of the DPA 2018 and the file contains personal data about the individual. It also contains various complaints from the individual about the handling of the case.

As it is not clear what information the individual wants, and since the Land Registry processes a large volume of information and believes it is genuinely necessary to seek clarification, it decides to stop the clock under the UK GDPR, to ask the individual to specify what information they are looking for.

The clock does not stop in relation to the Part 3 information, so the Land Registry must try and ensure it provides a response within the time limit. However, since there is a mix of data on the fraud file, including various complaints from the individual, it decides that the Part 3 data is not separately searchable from the UK GDPR data. The Land Registry provides the information relating to the fraud matter within the usual Part 3 timescale for responding.

Can we charge a fee under Part 3?

In most cases, you cannot charge a fee to comply with a SAR – you should provide the information free of charge.

However, you can charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. Alternatively, you can refuse to comply with a manifestly unfounded or excessive request. You may also charge a reasonable administrative fee for providing further copies of a SAR response. For further details, see our guidance on Part 3 manifestly unfounded and excessive requests.

Section 53(4) allows for the Secretary of State to specify limits on the fees that controllers may charge to deal with a manifestly unfounded or excessive request by way of regulations. However, at present there are no regulations in place. As such, it is your responsibility as a controller to ensure that you charge a reasonable rate.

For further guidance on the factors that you should consider when determining a reasonable fee you should follow our UK GDPR right of access guidance – 'Can we charge a fee?'.

Do we need to provide information processed for logging purposes?

If you process personal data on automated systems for any of the law enforcement purposes you must keep logs of certain operations, including the collection, alteration, consultation, disclosure, combination and erasure of data. See our guidance on 'Logging' for further details.

Logs of information may only be used for the purposes specified in section 62(4). These are:

- to verify the lawfulness of processing;
- to enable controllers to monitor and audit their data processing internally;
- to ensure the integrity and security of personal data; and
- for the purposes of criminal proceedings.

As logs of information may be used to "verify the lawfulness of processing", in some circumstances, you may need to consider whether such information is disclosable further to a SAR.

Individuals have a general right to be informed about what information you hold about them, including your purposes for processing it. You will usually be able to provide individuals with information, in general terms, about the collection, alteration, disclosure, or other processing operations you carry out on their information. This comes within your duty to provide individuals with certain supplementary information, which largely corresponds with the information you are required to provide in your privacy notice. See 'What other information is the individual entitled to under Part 3?'

However, logs of information are likely to contain specific metadata about your processing activities, including exact times and dates on which certain processing actions were performed. You need to consider, in the circumstances, whether this is the personal data of the individual whose record the log relates to. For further details, see our guidance on 'What is personal data?'

Logs of information create an audit trail of the data processing operations carried out by your employees. Therefore, they are likely to include the personal data of employees, including their name, and the date and time on which they consulted a particular piece of information. As your employees are likely to be aware their actions will be logged on a system, they may on occasion make a request for this information.

Example

The police suspect that a civilian staff member has inappropriately accessed the Police National Computer for the purpose of stalking and threatening another individual. The individual makes a SAR for all the information held about them. As the logs of information includes their personal data, this information is potentially disclosable further to the SAR.

However, as logs of information may be used for the purpose of criminal proceedings, the police consider whether they need to restrict the individual's right of access to avoid prejudicing the investigation.

For further information about when you may restrict the right of access, see 'Can we restrict the right of access under Part 3?'

Which SARs regime do we use to respond to requests for logs of information?

If you receive a SAR for logs of information, you should use Part 3 to deal with it. For example, you may keep logs for the purpose of auditing and monitoring the activities of your employees.

Example

An employee makes a SAR, and asks for "all the personal data you hold about me." Most of their personal information is contained within their human resources records, which you are processing under the UK GDPR. However, you also hold information about them in other databases and in your information logs.

The information logs contain the employee's name, the dates and times on which they accessed electronic criminal records, and details of any amendments the employee made to the records.

As the information logs therefore contain the employee's personal data, you should consider disclosing this information to comply with the SAR. However, it may be necessary to redact any personal data about third party individuals, eg information relating to the individual whose records were accessed by the employee.

Whilst your purpose for processing this information is not specifically for a law enforcement purpose, you are doing so to comply with the logging requirement under section 62 of the DPA 2018. As such, your underlying purpose is for law enforcement. Therefore, you must deal with this element of the SAR under Part 3.

How do we deal with requests for unstructured manual records?

Unstructured personal data is manual information that is not, or is not intended to be part of a "filing system".

A filing system should be interpreted broadly. It can cover the personal data you collect for your law enforcement purposes, if the data is structured

according to specific criteria. This means it should be ordered in a way that allows you to easily retrieve the information. However, it does not have to include data sheets, specific lists or other search methods.

Most of the manual information you process for any of the law enforcement purposes will be structured, and therefore form part of a filing system, eg witness statements, police notebooks, and any other evidence used for criminal proceedings. In general, unstructured manual data is only likely to include paper records such as loose written notes or post-it notes.

Example

Police seize large volumes of paper records for the purposes of a money laundering investigation. Personal data is contained in notebooks, folders, and in the form of loose pages. The police store this data in boxes marked with reference numbers which relate to the investigation.

As the information is clearly referenced, the information forms part of a filing system, even though some of the documents are in the form of loose notes, and the police have yet not had an opportunity to review it fully. This information is not unstructured manual data because it is clearly referenced and linked to a specific investigation.

If the police receive a SAR for this information, they should deal with it under Part 3.

It is important to apply good record-keeping practices to all the information you process – including manual data – in order to comply with the principles of data minimisation and storage limitation. For further details, see our Guide to Law Enforcement – 'What are principles three, four and five about?'

However, you should not use the Part 3 SARs regime for responding to requests for unstructured manual data obtained for law enforcement purposes. You should use the UK GDPR SARs regime to deal with **all** requests for unstructured manual data, even if you've obtained the information in connection with your law enforcement purposes.

Part 3 only covers information that:

- is processed wholly or partly by automated means; or
- is, or is intended to, form part of a filing system.

This means that unstructured manual data obtained for law enforcement purposes, is not included in the Part 3 processing regime. However, it **automatically** comes within scope of the UK GDPR – provided the controller is a public authority.

Article 2(1A) of the UK GDPR provides that,

Quote

"This Regulation [the UK GDPR] also applies to the manual unstructured processing of personal data held by an FOI public authority."

Therefore, unstructured manual data obtained for law enforcement purposes is automatically caught by this provision.

Example

An individual makes a SAR to their local authority for "all the information you hold about me".

In performing a search of its records, the authority finds handwritten notes prepared by an employee. The notes were made by the employee to assist them in typing up a penalty notice, which was served on the individual several weeks ago, and required them to pay a fine. The notes contain the individual's name, and various other personal details about them which were not included in the typed up penalty notice provided to the individual.

As the note is unstructured, it should not be considered under the Part 3 SAR regime. Instead, the local authority deals with the SAR under the UK GDPR. However, the authority also takes into account the fact the note relates to an ongoing criminal matter. The authority should consider whether any of the exemptions under the UK GDPR are relevant. For example, it may be necessary to apply the crime and taxation exemption.

See our guidance on the UK GDPR right of access – 'Unstructured manual records' for further details. For more information on the UK GDPR exemptions, see 'What other exemptions are there?'

Bear in mind that you may have to provide unstructured manual records to comply with another statutory or common law obligation.

Do we need to make reasonable adjustments for disabled people?

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

What is a reasonable adjustment will depend on the specific needs of the individual. Before responding to a SAR you should talk to the person to find out how best to meet their needs. This may be by providing the response in a particular format that is accessible to the person, such as large print, audio formats, email or Braille. If an individual thinks you have failed to make a reasonable adjustment, they can make a claim under the Equality Act 2010 or the Disability Discrimination Act 1995 (NI). Further information about your legal obligations and how to make effective reasonable adjustments is available from the Equality and Human Rights Commission or from the Equality Commission for Northern Ireland.

Relevant provisions in the legislation

See DPA 2018 sections 38(3), 54(2) and 62

Further reading – ICO guidance
'What is personal data?'

Guide to Law Enforcement:
'Categorisation'.
'Logging'

UK GDPR detailed right of access guidance:
'How long do we have to comply?'
'Can we ask for ID?'
'Can we clarify a request?'
'What should we do if we refuse to comply with a request?'
'Can we deal with a request in our normal course of business?'
'What efforts should we make to find information?'

How should we supply Part 3 information to the requester?

In detail

What information must we supply under Part 3?

You must make it easy for individuals to exercise their right of access. You should take reasonable steps to ensure that you provide the information in a concise, intelligible and easily accessible form, using clear and plain language.

Once you locate and retrieve the relevant personal data for the request, you should provide individuals with a copy of their information where possible. Whilst you should usually be able to provide the information in writing, it may not be reasonable to provide it in writing where it does not convey the true context or content of the information, for example, a transcript of a video recording. In these circumstances, you should provide the information in its existing format.

If you are unable to provide a copy of the information, you must still ensure that the individual is able to access their data. For example, you could make arrangements with the individual to enable them to view the data you hold. See 'In what circumstances can we provide an individual with access to their information but not a copy?'

Example

An individual was captured on CCTV footage and as a result of the footage, was arrested for a public order offence. The individual was then interviewed under caution and released without charge. The individual writes to the police to request a copy of the CCTV footage.

As the information does not exist in written form, the police provide the individual with a copy of the recording, having redacted the personal data of other individuals. Alternatively, they might have chosen to make arrangements to allow the individual to view the footage at a mutually convenient time. Depending on the circumstances, it may be necessary to redact the personal data of other individuals, before providing the individual with access to the footage.

Bear in mind that an individual will need a reasonable amount of time to review and assess the information you hold about them. So if they attend your premises in person, you should, where possible, provide them with enough time to consider the information you hold.

If you process information electronically, you should ensure that your software has been built with accountability and security measures in mind. As controller, you must ensure you are able to comply with all your data protection obligations. This includes the right of access, and any of the other individual's rights. For example, you may need to redact the personal data of third party individuals before disclosing information in response to a SAR. This is particularly important where the data concerns children or vulnerable people. So it is important that your software can perform this function.

Redacting visual and audio data, eg in the case of CCTV or body worn video, may require the use of specialist software. Where processing is likely to result in high risk, it is important that you carry out a DPIA in relation to any software or technology you use, to ensure it is fit for purpose. For further information about how to carry out a DPIA, please see our guidance on data protection impact assessments. Also see sections 64 and 65 of the DPA 2018 which deal with DPIAs for law enforcement purposes.

In what format should the information be provided?

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

- If the individual submitted the SAR electronically (eg by email or via social media), you must provide a copy in a commonly used electronic format. You may choose the format, unless the requester makes a reasonable request for you to provide it in another commonly used format (electronic or otherwise). (See our detailed right of access guidance for further information on, 'What is a commonly used electronic format?')

- If the individual submitted the SAR by another means (eg by letter or verbally), you must provide the information in the same format used by the individual to make the request, but only if it is practicable to do so.

- If an individual makes a reasonable request for you to provide the information in a commonly used format, you should comply with their request if it is practicable to do so, even if they have made the request in a different format.

Example

A prisoner writes a letter to the police, asking for copies of their personal data. The police collected the personal data for a law enforcement purpose and they decide that they can disclose the information.

The police would normally send the information by electronic means. However, since the individual has made the request by letter, they must print out the requested information and either hand deliver it to the prison or ensure that it is delivered securely by post.

Whilst you are not required to contact every individual who makes a SAR to ask them about their preferred format, you should contact them if it is not possible for you to provide the information in the same format as the request or in the format they have specified.

Many individuals within the criminal justice system may not be able to access information in certain formats. For example, prisoners may not be able to access electronic systems, or have only limited access to electronic systems. On the other hand, they may not have a secure method of storing paper copies of their information. Bear in mind that you **must**, where possible, help individuals exercise their right to access their information.

You may provide the information in any format, but you should give reasons if you are unable to provide the information in the same format as the request or in the individual's preferred format. You should document the efforts you make to ensure the information you provide is accessible, including contacting the individual where appropriate. You must be able to provide evidence of your efforts to the ICO, if asked to.

However, you are not required to create new information (eg transcripts) in order to respond to a SAR. In circumstances where it is not possible to provide a copy of the data, you must still ensure that the individual is able to access their information.

It may not always be practicable to provide the information in the same format as the request or in the individual's preferred format – for example, where you have concerns about security. In particular, if the information is sensitive, you should ensure that you transfer it to the requester using an appropriately secure method. Please see our UK GDPR right of access guidance 'How do we provide the information securely?' for further details.

You should take reasonable steps to ensure that the information you provide in response to a SAR is in an accessible and intelligible form using clear and plain language. For further information, please refer to our UK GDPR guidance on the right of access 'Do we need to explain the information we supply?', and also our Part 3 guidance on the right to be informed.

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.

What should we do if the information exists in different forms?

If the information exists in different forms, you should generally provide the information in writing where possible, although you are not required to create transcripts if you would not normally do so. Bear in mind that audio or

visual recordings are likely to contain further context and meaning which cannot be communicated in a transcript. This may include information about the individual's emotions. For example, their tone of voice may display sarcasm, anger or fear.

In these circumstances, it is good practice to discuss with the individual their preferred format, before responding to the request. If an individual believes that the response you have provided in writing is incomplete and they ask for the information to be provided in its original format, you should deal with the matter as part of their original request. This means you should respond as soon as possible, and either:

- provide a copy of the information in the alternative format (eg audio recording); or

- allow the individual an opportunity to access their information in the alternative format, by inviting them to your premises to listen to or view the information.

In deciding what response is appropriate, you should carefully consider the circumstances of the request. For example, you may consider the following factors:

- Whether it would be reasonable to ask the individual to attend your premises to view or listen to the recording rather than provide them with a copy. For example, this may depend on how far they would have to travel.

- The nature of the disparity between the transcript and the alternative format. If the transcript is vague, or lacks some crucial detail, you should, where possible, provide a copy of the recording. However, if the transcript is generally comprehensive (but does not include some contextual information eg tone of voice or facial expressions), it may be reasonable to provide the individual with an opportunity to view or listen to the recording in order to check the accuracy of the transcript.

- Whether providing a copy of the recording would be manifestly unfounded or excessive.

Bear in mind that you should not deem a request as excessive just because you have already provided the information in writing. If the response is incomplete, it may be reasonable for the individual to ask you to provide it in

an alternative format, as part of their original request. For further details about manifestly unfounded or excessive SARs, see our guidance on manifestly unfounded and excessive requests.

Example

An individual was interviewed under caution at a police station. The interview was recorded with the individual's knowledge and the police decided not to charge the individual. The individual later makes a SAR for a copy of the recording. The police respond to the request by providing a transcript of the interview.

The individual contacts the police after receiving the transcript and asks for a copy of the audio recording, because they do not believe the transcript is accurate. As the police believe that any inconsistencies are likely to be minor, they invite the individual to attend the police station so they can listen to the audio recording for the purpose of checking the accuracy of the transcript.

You should ensure that the information you hold about individuals is accurate and up-to-date. Remember that if an individual thinks you hold inaccurate data about them, they can ask for it to be rectified. For further information on this see our law enforcement guidance on 'The right to rectification', and 'What are principles three, four and five about?'.

Can we provide remote access?

You may provide the individual with remote access to their personal data via a secure system **if they agree**. If you are providing an individual with remote access to their personal data, it may be necessary to redact information about third party individuals, before making the information available to them.

You should note that although you provided the individual with remote access to their personal data, it does not necessarily mean that you provided them with a copy of their data. This depends on whether they are able to download a copy of the requested information. If the individual has been able to download their personal data from the remote access system, then you have provided them with a copy.

See above, 'What information must we supply under Part 3?' Also see the next section, 'In what circumstances can we provide an individual with access to their information but not a copy?'.

In what circumstances can we provide an individual with access to their information but not a copy?

If an individual makes a SAR, in most cases you should provide them with a copy of their personal data. However, in certain circumstances, it may be appropriate to provide them with access to their information rather than providing a copy, for example, where:

- one of the section 45(4) restrictions apply to the provision of a copy of the data;
- because the cost of providing a copy of the information may be deemed as manifestly excessive; or
- the individual agrees.

This is not an exhaustive list, and there may be other reasons why you may be unable to provide a copy of the information. You should keep a record of your reasons, and be able to justify your decision, if required.

For further details about when you may restrict an individual's right of access to their information, see the next chapter, 'Can we restrict the right of access under Part 3?'.

Relevant provisions in the legislation

See DPA 2018 section 52

Further reading – ICO guidance

UK GDPR right of access guidance – 'How do we provide the information securely?' and 'What is a commonly used electronic format?'
UK GDPR guidance on DPIAs
Part 3 guidance on the right to be informed

Can we restrict the right of access under Part 3?

In detail

Can we restrict access to the information we provide under Part 3?

Yes – but only in very specific circumstances.

An individual has a right to obtain confirmation of whether or not you process their information, and to access their personal data. You may restrict these rights, in full or in part, if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;

- avoid prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

You should only restrict an individual's right to access their information to the extent necessary to achieve one of these purposes, and you must provide them with any information you do not need to restrict access to.

If you are restricting any of the individual's rights to their information, you may still need to provide them with certain details – see, 'Do we need to tell individuals why their rights have been restricted?'

In some circumstances, you may restrict an individual's right to be provided with specific privacy information, in circumstances in which they may not be aware of the processing – see 'When do we need to take action to enable an individual to make a SAR?'

What is a "necessary and proportionate measure"?

The right of access to personal data is a fundamental right for individuals. If you are processing an individual's information for a law enforcement purpose, in many cases, it will be more likely that their rights and freedoms are engaged. This includes their rights and freedoms under the Human Rights Act 1998, and the European Convention on Human Rights (ECHR). For example, an individual may require the information to obtain legal advice.

The relevant provisions require you to demonstrate that restricting the individual's right of access is "necessary" to achieve a specific purpose. This means that you should only restrict access if you really have to. You need to show that you have identified a reasonable possibility of a potential risk. It must be more than speculative, but does not have to be a foregone conclusion.

If you can reasonably achieve the same purpose by another means you should do that instead, eg by redacting the sensitive data and providing the individual with the rest of the information. This links to the principle that processing must be lawful and fair, as this includes not unreasonably restricting an individual's right to access their information.

You must also demonstrate that your decision to restrict access is "proportionate". This means that your reasons for restricting access must be sufficiently important to merit any restriction, particularly when considered against any impacts that restricting access will have on the individual.

In considering whether restricting the right of access, or refusing to confirm or deny whether you hold the information, is a necessary and proportionate measure, you must have regard to the fundamental rights and legitimate interests of the individual. This does not simply mean acknowledging and recognising that restricting the right of access may impact an individual's rights (although it is important that you can identify what rights may be affected) but also requires you to seriously consider the actual consequences, including any potential adverse impacts the individual may experience as a result of your restricting access to their information. You should only infringe the individual's rights to the minimum extent necessary to achieve your purpose.

In general, you should consider all relevant factors and carefully balance the individual's right of access against your reasons for restricting access. The legislation does not require you to perform a balancing exercise, although, in many circumstances, this approach may be appropriate. The amount of weight you should attach to the individual's right of access will depend on how compelling their need to have access to the information is.

You may restrict access to some or all of the information depending on the circumstances. As you should only restrict access to the extent necessary to achieve your purpose, you should generally provide the individual with as much information as you can.

In certain circumstances, restricting access will have such an adverse impact on an individual's rights, that you may not be able to justify it as "a necessary and proportionate measure". In other cases, it will be reasonable to restrict an individual's right of access even where their rights are adversely impacted, if the underlying purpose of the restriction is so compelling, and there are no other means by which to mitigate the risks you have identified.

What rights and interests may be impacted by restricting an individual's right of access?

The rights, freedoms and interests of individuals should be considered broadly. Restricting access to personal data can impact any aspect of an individual's life, and not just in the context of criminal proceedings.

For example, refusal to provide the information may impact fundamental rights and freedoms, such as:

- the right to a fair trial;
- the right to liberty and security;
- the right to respect for private and family life;
- freedom to choose an occupation and the right to engage in work; or
- freedom to conduct a business.

Which of the individual's rights and interests are impacted may vary depending on the circumstances, and how you have categorised them – see 'Does the categorisation of individuals impact what information we can provide them with?'

You may receive a SAR from any individual whose data you process for a law enforcement purpose. You should carefully consider the rights and freedoms that may be engaged in the specific circumstances, whether the individual provides you with these details or not.

It is important to balance the rights of the individual against the harm disclosure may cause. The amount of weight you should attach to any of an individual's rights, freedoms or legitimate interests may depend on how compelling or trivial they are, and on how compelling the need to restrict the right of access is.

Example

An employee is injured at work and the health and safety regulator launches a criminal investigation. The employee makes a SAR to the regulator asking for all the information held about them. They want to use the information to obtain legal advice about their chances of bringing a successful personal injury claim against their employer.

The regulator is concerned that disclosure of the information may be prejudicial to the investigation. Also, if some of the information were to reach the media, this may have an impact on the fairness of any future trial. However, the individual has a legitimate interest in wanting to access the information, as this may help them decide whether or not to make a claim.

The regulator decides it must balance the individual's fundamental rights and legitimate interests against the possible prejudice to the investigation in disclosing the data. The regulator documents the impacts of disclosure, against the impacts on the individual of restricting access, in order to reach its decision. It carefully considers any relevant factors and records how it has reached its decision.

For example, refusing to provide the information will not prevent the individual from obtaining legal advice. However, the legal advice will be based on more limited information. It also considers that it will only be necessary to restrict access for a certain length of time, and once the investigation has ended, the regulator will be able to provide the information.

Ultimately, you need to make a reasoned and sensible decision based on genuine risks. You should document and keep a record of your decision, and be able to justify your position and provide details to the ICO if asked to. You should explain your reasons to the individual where possible.

When can we neither confirm nor deny we hold the information?

If you decide to restrict an individual's right to access their personal data, in many cases, you will still be able to comply with your duty to confirm whether or not you are processing their information.

However, in certain circumstances, you may decide to restrict the individual's right to know whether you process information about them. If you refuse to confirm or deny whether you hold the information, this is often called a "neither confirm nor deny" (NCND) response. This response may be appropriate if disclosing the fact you hold, or do not hold the information, may undermine the purpose of restricting the right of access in the first place.

You can only refuse to confirm or deny you hold the information in specific circumstances. You may provide a NCND response if, having regard to the fundamental rights and legitimate interests of the individual, you believe that withholding the information is a necessary and proportionate measure to achieve one of the purposes set out in the relevant provisions in section 45(4).

However, the decision to neither confirm nor deny is separate from a decision to restrict the right of access, and needs to be taken entirely on its own merits. There may be circumstances in which a NCND response may not be a necessary or proportionate measure. See 'What is a 'necessary and proportionate measure'?'

Example

The police are investigating a murder. They suspect the involvement of an individual and place them under surveillance without their knowledge.

The individual makes a SAR to the police for any information held about them relating to the murder investigation. Taking into account the rights and legitimate interests of the individual, and the seriousness of the offence, the police decide that restricting access to the information is a reasonable and proportionate measure because disclosure is likely to prejudice a murder investigation.

The police must separately consider whether to confirm or deny they hold the individual's personal data. Since the individual is not aware they are under surveillance, confirming any information is held is likely to undermine the purpose of restricting access to it in the first place. This is because the police have reasonable concerns that the individual may alter their behaviours and movements if they fear they may be under investigation. They may also attempt to conceal evidence or take action which could prevent the apprehension of a suspect.

As confirming the information is held would undermine the purpose of restricting the individual's right of access, the police respond to the request and provide a NCND response.

Avoid obstructing an inquiry, investigation or procedure

You may restrict access to some or all of the information you hold if disclosing it would obstruct an official or legal inquiry, investigation or procedure. This can include any public investigation or inquiry, and not just criminal investigations or proceedings, but only if you are processing the information for a law enforcement purpose. For example, depending on the specific context and circumstances, it may apply if disclosing the information would obstruct an ongoing or future coroner's inquiry.

"Obstructing" in this context, is not specifically defined, but it can generally be interpreted to mean preventing or delaying an inquiry, investigation or proceedings from taking place or progressing within a reasonable time.

You may restrict the individual's right of access, if you believe that complying with the SAR may frustrate, or cause difficulties or impediments in progressing an inquiry, investigation, or other official or legal procedure.

For example, if you are investigating complex criminal activity, you may have concerns that if you disclose information to a suspect, they may alert their accomplices who are still at large, and this may allow them an opportunity to cover their tracks. In these circumstances, you may consider that you need to restrict access to avoid obstructing the investigation.

Example

An individual is arrested and questioned by police in connection with a public order offence. The police believe the individual is a member of a violent gang under investigation for numerous offences. The police do not have enough information to detain the individual in custody but investigations are ongoing. The individual requests all the personal data held about them by the police.

The police are concerned about releasing some of the information to the individual, in case they share it with other gang members, who are potential suspects. The information might alert them to what the police already know about their activities, which could allow them to evade capture or cause them to engage in further criminal activity.

The police want to restrict access to the information on the basis that disclosure could obstruct the ongoing investigation. They decide that the impact to the individual is minimal as they have not been charged with an offence due to lack of evidence, and so failure to disclose the information does not impact their fundamental rights and freedoms.

The individual is therefore only entitled to the information that has not been restricted. The police document their reasons for restricting access, and explain their reasons to the individual, by advising that disclosure of the information would harm ongoing investigations, but do not provide any specific details as this would undermine the purpose of restricting access.

Avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

You may restrict access to some or all of the information you hold if providing it may prejudice:

- the prevention or detection of crime,
- the investigation and prosecution of criminal offences, or
- the execution of any criminal penalty.

In the context of criminal justice, “prejudice” can have different meanings depending on the context and circumstances.

In the context of the prevention, detection, and investigation of crime, prejudice may occur where disclosing the information may undermine an inquiry. For example by revealing details about a covert policing operation. It may also be relevant where controllers have reasonable grounds to believe that disclosing information to a suspect could lead to them taking steps to conceal a crime.

Prejudice, in this context, can also mean preventing an investigation from being conducted independently or fairly, eg where disclosure of the information would impair or damage the rights of any individual under investigation or charged with an offence. This could happen if, for example, prosecutors disclose information to a witness, which may not be admissible at trial, and which may damage the suspect’s rights if it reaches the media before the trial.

Prejudice can also apply in the context of the execution of criminal penalties. This term is not specifically defined in the legislation but generally means any measure or process used to determine an appropriate penalty for an offender. This may include sentences handed down by a judge, or out of court disposals. For example, it may be relevant where a judge is deciding whether to sentence an offender to a term in prison, or community service. However, it does not only apply to sentences handed down by a judge and may also apply in the context of a police caution or conditional discharge, for example.

In the context of court proceedings, including sentencing proceedings, prejudice can occur where decision-makers reach a conclusion or determine a matter before considering the evidence in full, and enabling due process, or if they make a decision based on irrelevant or inadmissible evidence. Unfair or preconceived opinions or irrelevant circumstances may also prevent an individual from having a fair trial, or receiving a fair sentence.

Example

The victim in a high profile criminal trial requests all the personal data held about them by the prosecution service. The information held about them includes witness statements and other evidence gathered by the police, including notes and the opinions of senior officers about the facts or circumstances.

Some of this evidence will not be admissible in court. However, some of the evidence will be admissible but will need to be properly tested during the course of the trial.

If the prosecutor provides the information to the victim they cannot control what they do with it. If it reaches the media, it could prevent the defendant from having a fair trial as potential jurors may be unfairly influenced by the media coverage, and they may have a biased opinion about the case before they hear the evidence at court.

As the victim will be compelled to testify at court, there is also a risk that providing them with this information may affect their testimony, as they may use the information they receive to help them reconstruct their version of events rather than basing their testimony on their recollection of the incident in question.

The prosecution service considers the fundamental rights and legitimate interests of the victim in deciding whether to provide them with access to this information. However, they decide that restricting access to some of the information is a necessary and proportionate measure to ensure that the defendant is tried fairly. They decide that the balance weighs against disclosure in these circumstances.

Protect public security

You can restrict an individual's right of access to their information if you consider it to be a necessary and proportionate measure to protect public security.

"Public security" is not specifically defined. It generally concerns the welfare and protection of the public at large. It may cover the protection of life, institutions and organisations against public threats, crime, disasters and other threats to life, safety and well-being. For example, it may include:

- use of intelligence to address possible threats;
- policing large events; and
- investigating drugs offences, human trafficking, or institutional child abuse.

Public security can encompass most major public policy issues, or anything that threatens public order. If you choose to restrict the right of access based on the need to protect public security, you should document your reasons why. In particular, you should record why providing the individual with access to their information would threaten public security or present a risk to the welfare and safety of the general public.

You should also document the level of the risk you perceive and ensure that you only restrict access in a proportionate way, and only to the extent necessary, taking into account the rights of the individual.

Example

The police are investigating the activities of a criminal gang operating in the local area. This includes violent crime, drugs, and human trafficking offences. One evening, they arrest an individual on suspicion of affray. The police have in their possession CCTV footage of the incident. The individual wants to view this footage, and makes a request for "all the data you hold about me."

However, the police also hold on their records, information which suggests the individual is connected to the criminal gang they are currently investigating. They do not have sufficient evidence to establish the individual's involvement. They are concerned that if they disclose this information there would be a risk that the individual might alert other members of the criminal gang who are still at large. They are also concerned that disclosure could present potential risks to the life and safety of victims.

Taking this into account, and having considered the impact on the individual's fundamental rights and legitimate interests, they decide to restrict access to the information which links the individual to the activities of the criminal gang, based on the need to protect public security.

However, as the incident of affray does not relate to these activities, the police do not need to restrict the individual's access to the CCTV footage. They disclose this information after redacting any personal data about third party individuals.

Protect national security

You can limit or restrict the right of access where this is a necessary and proportionate measure to protect national security.

"National security" is not specifically defined. However, it is generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government.

For more information see our guidance on the national security provisions.

Protect the rights and freedoms of others

You can restrict an individual's right to access their personal information if you consider it to be a necessary and proportionate measure to protect the rights and freedoms of others. For example, this will usually be relevant if the information contains personal data about another individual.

Please see, the next chapter, 'What should we do if the Part 3 request involves information about other individuals?'

Do we need to consult joint controllers about restricting the right of access before disclosing the information?

It depends. See, 'Do we need to consult joint controllers about restricting the right of access before disclosing the information?'

Can we apply more than one relevant provision to restrict the individual's right of access?

The legislation does not prevent you from applying more than one of the relevant provisions in order to restrict an individual's right of access. However, whilst there may be some overlap across the relevant provisions, you should apply the one which is most relevant and suited to your specific circumstances. In responding to a request, it may sometimes be appropriate to apply different relevant provisions to different pieces of information in order to respond to the SAR.

However, since you can only restrict an individual's right of access where you consider it to be a necessary and proportionate response to an identifiable risk, in most cases it will be disproportionate to apply more than one relevant provision to the same information. If you need to restrict access for more than one reason, you should ensure that you keep records of your reasons.

In general, you should aim to provide the individual with access to their data where possible. You should not apply any of the relevant provisions in a blanket way, and you should not apply more than one of the relevant provisions in an attempt to strengthen your position in restricting the right of access. Instead you should assess the individual items of personal data you hold to decide whether the information may be disclosed. If you only need to restrict access to some of the data, where possible you should disclose the rest. See 'What is a 'necessary and proportionate measure'?'

Can we restrict the right of access for a specified period of time?

Depending on the circumstances, you may only need to restrict the individual's right to access their information for a specific length of time, eg until an investigation is complete or criminal proceedings have ended. However, in some circumstances, you may need to restrict the right of access for an indefinite period of time.

You are not required to keep a SAR open after you have lawfully restricted the right of access under the relevant provisions, and responded to the individual. However, if you only need to restrict the individual's right of access for a specific length of time, it is good practice, where possible, to inform the individual when they may be able to resubmit their request.

Do we need to record our reasons for restricting an individual's right of access?

Yes. You must record your reasons for restricting – either wholly or partly – an individual's right of access to the following information:

- confirmation of the processing (ie where you have issued an NCND response);
- any of their personal data;
- any of their supplementary information; and
- certain privacy information – see 'When do we need to take action to enable an individual to make a SAR?'

You should also record why you have deemed this measure to be a reasonable and proportionate response to an identified risk, in accordance with the relevant provisions. You must be able to make this record available to the ICO, on request (although you should only keep personal data in accordance with the terms of your retention and disposal schedule).

Do we need to tell individuals why their rights have been restricted?

In most cases, if you have restricted an individual's right to access their information, you must inform them as soon as possible of:

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

You do not need to explain that you have restricted their right of access or why, if this would undermine the purposes of restricting the right in the first place. However, where possible you should be transparent about your reasons for restricting their right of access to their personal information.

You must record your reasons for restricting the right and make this available to the ICO, if asked to (although you should only keep personal data in accordance with the terms of your retention and disposal schedule).

Can we rely on the UK GDPR exemptions to withhold personal data under Part 3?

No. Schedules 2, 3, and 4 of the DPA 2018 set out the UK GDPR exemptions. You may only rely on these exemptions if you are processing information under the UK GDPR. If you are processing information for law enforcement purposes, you cannot rely on any of these exemptions to refuse to provide information further to a Part 3 SAR.

You may only use the relevant provisions in section 45(4) to restrict access to information processed for any of the law enforcement purposes. For more details about restricting access under these provisions, see above, 'Can we restrict access to the information we provide under Part 3?' Also see 'What happens if independent controllers are processing the same data under different regimes?'

Bear in mind that other rules apply to legal professional privilege – see the next section, 'Can we withhold information on the basis of 'legal professional privilege'?'.

For further details about the UK GDPR exemptions, see our right of access guidance, 'What other exemptions are there?'

Can we withhold information on the basis of legal professional privilege?

There is no specific restriction under Part 3 of the DPA 2018, which specifies that you may withhold information on the basis it is protected by legal professional privilege. However, this does not mean that privilege does not apply.

Legal professional privilege is an established common law principle, which provides that clients have a fundamental right to seek and obtain confidential legal advice, without the risk of such details being disclosed to others. Part 3

does not expressly reject the application of this long-established right. As such, controllers may withhold information on the basis of the common law principle of legal professional privilege, even though there is no specific restriction under Part 3.

Example

The prosecution service decides that it has sufficient evidence to prosecute an individual for numerous offences, including aggravated burglary, assault occasioning grievous bodily harm, and possession of a weapon. However, due to numerous complexities in the case, the prosecution service decides to obtain legal advice before proceeding.

The individual makes a SAR for any information the prosecution service holds about them, including any advice or reports obtained. The prosecution service decides that the legal advice is protected by legal professional privilege, as it is a confidential communication between client and lawyer, made for the purposes of obtaining legal advice.

The prosecution service does not need to consider whether any of the information contained in the legal advice is disclosable as privilege applies to the legal advice in its entirety. The prosecution service withholds the legal advice completely.

Relevant provisions in the legislation

See DPA 2018 section 45

What should we consider when acting as joint controllers?

In detail

What do we need to consider if we are acting as joint controllers?

Where two or more competent authorities jointly determine the purposes and means of the processing of personal data, they will be acting as joint controllers.

If you are acting as a joint controller, you **must** ensure that:

- you have an arrangement in place with your fellow joint controllers, which clearly and transparently sets out each of your responsibilities under Part 3, including how you deal with SARs; **and**

- you specify a contact point for individuals, which is one of the joint controllers.

Example

Separate policing organisations have statutory remit to enter into a collaboration agreement for the investigation of serious crime. The agreement sets out the respective functions of officers and staff at each organisation.

As each organisation will be processing personal data as joint controllers, they must have joint arrangements in place, which allocates each organisation's data protection responsibilities under the DPA 2018.

Whilst joint controllers may apportion their responsibilities under the DPA 2018 under their joint arrangements, their obligations under other legislation should not form part of these arrangements.

What are the responsibilities of the "contact point"?

Joint controllers must, in their joint arrangements, name one of the joint controllers as the contact point for individuals. You cannot appoint a third party as the contact point.

It is good practice for each of the joint controllers to name the contact point on their websites or in other communications, and direct individuals to make their SAR to the named contact point where possible. However, a SAR is received as soon as it is received by any of the joint controllers.

If any of the joint controllers receives a SAR, they should forward it to the contact point as soon as possible, and the joint arrangements should make provision for this. In general, it is good practice to make each joint controller aware of every SAR.

The joint arrangements should set out very clearly the duties of each joint controller in relation to SARs. Whilst the contact point will often take responsibility for all aspects of complying with the SAR, including performing reasonable searches, redacting, and providing (or refusing) the information, these duties may be allocated amongst the joint controllers. The contact point may coordinate responses to a SAR, by liaising with the other joint controllers, as appropriate, subject to the terms of the joint arrangements.

Your joint arrangements may specify whether individuals should be able to exercise their rights against each controller, or against the contact point only. Each controller must comply with their specific responsibilities under the terms of the joint arrangements, and also with their statutory data protection obligations.

Whilst the role of the contact point cannot be delegated to a third party organisation, this does not prevent joint controllers from outsourcing certain aspects of their SAR work to a processor. It is important that you clearly set out the respective obligations of each of the parties in your controller/ processor agreement. For further details, see our guidance on 'Contracts'.

Do we need to consult joint controllers about restricting an individual's right of access before disclosing the information?

Whilst you are required to make arrangements for SARs in a joint controllership arrangement, the specifics (eg data sharing, notification about SARs) are for the joint controllers to determine. Depending on the circumstances, you may wish to seek the views of other joint controllers about whether to restrict the right of access. Your joint arrangements should make provision for notifying other joint controllers before responding to a SAR.

Example

Two government agencies (Agency A and Agency B) use shared information access systems to process personal data for law enforcement purposes. They are acting as joint controllers, and have specified in their joint controllership arrangements that Agency A is the contact point for SARs, and is also responsible for responding to requests for information. Agency A receives a SAR from an individual.

The joint arrangements provide that the contact point should obtain the views of each joint controller in order to decide whether it is necessary to restrict the right of access.

Agency A informs Agency B about the SAR and seeks its views before disclosing any information. Agency B believes disclosing some of the information may put another individual at risk. It provides evidence to Agency A which demonstrates why restricting the right of access is a "necessary and proportionate" measure, to protect the rights and freedoms of another person.

As each joint controller will only be liable in accordance with the terms of the joint arrangements, Agency A is therefore responsible for complying with the SAR. It should carefully consider the evidence Agency B has provided, and decide whether restricting access is a necessary and proportionate measure, having regard to the rights of the individual.

On the basis of the joint arrangements, Agency A may be subject to enforcement measures by the ICO if restricting access was not in fact necessary and proportionate in the circumstances. However, any individual, controller, or processor may be required to facilitate the ICO's investigations.

For further details about the ICO's enforcement powers (including where there is a joint controllership arrangement in place), see the chapter, 'Can the right of access be enforced under Part 3?'.

What happens if we are only processing some of the information for joint purposes?

There may be circumstances where a number of controllers are acting jointly in relation to one particular aspect of their processing. However, they may act independently of each other in carrying out other processing activities.

Example

A number of competent authorities (Agency A, Agency B, Agency C, and Agency D) are able to access a shared database, which contains information about the criminal convictions of individuals. Agency C owns and manages the system on behalf of the other agencies. The information is being processed under Part 3.

Each of the agencies is an independent controller in its own right. However, they are joint controllers in relation to the information being stored on the shared database. Agencies A, B, C, and D have joint arrangements which set out each of their data protection responsibilities under the DPA 2018, including their arrangements for dealing with SARs.

The arrangements specify that Agency C is the contact point, and responsible for responding to SARs.

Agency D receives a SAR from an individual requesting "all the information you hold about me". Agency D is an independent controller for most of the information it processes about the individual. However, the information held on the shared database is also within scope of the request. As Agency D is not the contact point for the information held on the shared database, it forwards the SAR to the named contact point – Agency C.

Further to the joint arrangements, Agency C must respond to the element of the SAR which concerns the information held within the shared database.

Can we consult other competent authorities in deciding whether to restrict the right of access?

It depends. During the lifecycle of a criminal case, an individual's personal data is likely to processed by a number of competent authorities. For example, police obtain information for the purpose of investigating crime. The prosecution service reviews the information in order to decide whether or not to pursue a prosecution. They work collaboratively, yet independently of each other, and make decisions separately. They are not joint controllers, but are likely to share personal data in the course of a criminal case.

There is nothing in the DPA 2018 which requires you to only consider your own specific circumstances in deciding whether to restrict access. It will not usually be necessary or appropriate to consult other competent authorities before you respond to a SAR. However, if you believe there may be a risk of serious harm in disclosing the information, you may wish to do so.

In these circumstances, you should base your decision on evidence provided to you by the other controller, and be able to justify why you have considered that restricting the right of access is a necessary and proportionate measure, having regard to the rights and freedoms of the individual. Remember that you are responsible for complying with the SAR, and must not arbitrarily restrict the right of access or speculate about risks without proper justification. See 'What is a "necessary and proportionate measure"?' You must also ensure that you respond to the request within one month.

If independent controllers share data with each other, it is important that you have a data sharing arrangement in place. See our guidance on 'Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR – We are a competent authority. How do we share data under Part 3 of the DPA 2018?'

If you require further guidance about controllers, joint controllers or processors, please read our UK GDPR guidance on controllers and processors.

What happens if independent controllers are processing the same data under different regimes?

There are likely to be circumstances in which you and another controller are processing the same personal data for different purposes eg law enforcement and general purposes.

For example, if a hospital shares information with police about the nature of the injuries sustained by a victim – the hospital is processing the data under the UK GDPR, whilst the police are processing it under Part 3.

If you are processing personal data under Part 3, you can only restrict an individual's right of access based on the relevant provisions under section 45(4) of the DPA 2018. However, you may consult other controllers before you respond to a SAR, if you have identified a potential risk of serious harm. If you consult another organisation, you must still respond to the request within one month of receipt of the SAR.

See 'Can we rely on the UK GDPR exemptions to withhold personal data under Part 3?'

Relevant provisions in the legislation

See DPA 2018 section 58

Further reading – ICO guidance

'Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the UK GDPR – We are a competent authority. How do we share data under Part 3 of the DPA 2018?'

UK GDPR guidance on controllers and processors and 'Contracts'.

What should we do if the Part 3 request involves information about other individuals?

In detail

What is the basic rule?

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

Example

A prisoner assaults a fellow inmate, and makes a request for all of their personal data. The prison authority's records contain personal information about the victim, witnesses, and a number of other individuals, including family members of the prisoner.

The prison authority will need to reconcile the prisoner's right of access with the rights of the third party individuals in respect of their own personal data.

You can restrict an individual's right to access their personal information if you consider it to be a necessary and proportionate measure to protect the rights and freedoms of others – in particular, where the individual's personal data also contains information relating to a third party individual. See 'What

is a "necessary and proportionate" measure?'. You should also refer to our three-step process set out below – 'What approach should we take?'

What approach should we take?

To help you decide whether to disclose information relating to a third party individual, follow the three-step process described below. You may also find it helpful to read our guidance on 'Access to information held in complaint files'. Whilst it mainly focuses on freedom of information requests, and requests for environmental information, it also covers SARs.

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

Before you consider restricting the right of access, you should first 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 considering 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.

Depending on the circumstances, it may be appropriate to redact the personal data of other individuals, so that they are no longer identifiable.

Example

A prisoner requests access to their personal data. Their file contains the name and other personal details about prison administrative staff.

By redacting the personal data of the prison staff, the individuals concerned are no longer identifiable.

However, you should bear in mind that individuals may be identifiable from the context or circumstances even if you redact their name or other personal details. For example, if you disclose a witness statement to a suspect, the suspect might be able to identify the witness from the general content and context of the statement. See our guidance, 'What is personal data?'

Example

An individual is arrested for assault occasioning actual bodily harm. A witness who lives nearby has made a statement describing the attack and the nature of their injuries. The individual who was arrested makes a SAR for their personal data. If the witness statement is released, it is reasonably likely that the individual will be able to identify the witness from the date, time, description of the incident, context and circumstances.

Step two – Do we need to consider restricting the individual's right of access?

If you process personal data that relates to more than one individual, and there is a risk that the third party individual may be identifiable from the information, you should consider whether, in the circumstances, it may be appropriate to restrict the individual's right of access.

You may restrict an individual's right of access to their personal information only if you consider that it is a necessary and proportionate measure to protect the rights and freedoms of others.

In determining whether to restrict access, you must also consider the fundamental rights and legitimate interests of the individual.

If information contains the personal data of an individual and that of third party individuals, you have to carefully consider whether it is reasonable to disclose this information. You need to consider whether disclosure may adversely affect the rights and freedoms of the third party individuals. You must also consider the fundamental rights and legitimate interests of the individual, ensuring that any restriction is necessary and proportionate. See 'What rights and interests may be impacted by restricting an individual's right of access?', and also, 'What is a necessary and proportionate measure?'

So, although you may sometimes be able to disclose information relating to a third party individual, you need to decide whether it is appropriate to do so in each case. This decision involves balancing one individual's right of access against the other individual's rights relating to their own personal data.

Step three – how do we decide if the balance weighs in favour of disclosure, or against?

It is important that you carefully consider the rights and freedoms of both the requester, and the third party individual. Having considered the rights of both parties, you then need to consider whether restricting the right of access is a necessary and proportionate measure in the circumstances.

You should consider all relevant circumstances in deciding whether it would be reasonable to disclose the information. For example, you may consider:

- the type of information that you would disclose;
- how you have categorised both the individual making the request and the third party individual for whom some of the data relates;
- the impact of restricting access on the fundamental rights, freedoms and legitimate interests of the individual who made the SAR;
- the impact of disclosure on the fundamental rights and freedoms of the third party individual for whom some of the data relates;
- any duty of confidentiality owed to the third party individual; and
- whether it may be appropriate, in the circumstances, to obtain consent from the third party individual.

This is an non-exhaustive list, and ultimately it is for you to make this decision taking these factors into account, along with the context of the information. As a competent authority, you should make a reasoned decision about what approach is appropriate in the circumstances.

Due to the sensitivities of law enforcement processing, it may not always be appropriate to ask third party individuals whether or not they consent to the disclosure of their data to the requester. However, it is for you, as controller, to decide what measures are appropriate on a case-by-case basis, taking into account the specific circumstances of the request.

Example

The police receive a number of reports concerning various incidents of domestic violence occurring within a household. These reports have been made by the complainant. The suspect in question has a number of previous convictions, and the police hold a large amount of personal data about them.

The suspect makes a SAR for all the personal data the police hold about them. Some of the information will be restricted because there are ongoing investigations, and disclosure may result in prejudice to the investigation.

However, the police have completed their investigations into the domestic violence allegations made by the complainant. The prosecution service has decided there is insufficient evidence to pursue a prosecution at this stage. However, the police are keeping the information on record in case the complainant makes further allegations or the situation escalates. The police understand that the suspect may not be aware of the allegations their partner has made about them.

The police balance the suspect's right to access the reports of domestic violence made about them, against the need to protect the rights and freedoms of the complainant. They have concerns that disclosing the information may risk the life and safety of the complainant. On balance, restricting the suspect's right of access to this information is a necessary and proportionate measure in these circumstances. However, the police decide they are able to disclose some of the information they hold about the individual which does not relate to the domestic violence allegations made against them as this does not present a risk to the complainant or prejudice the ongoing investigations.

It is important that you consider the risk to other individuals broadly. If you redact personal details, you should carefully consider whether the third party individual may be identifiable by jigsaw identification.

Example

An individual is charged with possession of cannabis with intent to supply, after a fifteen year old child who lives in the area noticed the individual behaving suspiciously one evening whilst out walking their dog. They reported the incident to police and later provided a statement.

The individual makes a SAR to the police for their personal data. If the police redact the child's name and personal details, they are not obviously identifiable from the statement, or the transcript telephone recording in which they reported the incident. However, if the police disclose the statement or telephone transcript, the individual may be able to identify the child through jigsaw identification, eg the fact the child walks their dog in a specific location at the same time each day, and there is also a risk that the suspect's acquaintances may have noticed the child in the area on the evening in question.

The police carefully consider whether they should restrict the individual's right of access in these circumstances. They should take into account any relevant factors, including that the statement is likely to be disclosed in the course of criminal proceedings anyway – but under the jurisdiction of the court. Once they have considered all relevant factors, the police need to balance the rights of the individual making the SAR, with the rights of the child who provided the statement.

For further details on dealing with requests containing data relating to third party individuals, see our right of access guidance – 'What should we do if the request involves information about other individuals?' For information about requests made by or on behalf of children, see 'What about requests for information about children or young people?'

You should also refer to the sections, 'Does the categorisation of individuals impact what information we can provide them with?'

In certain circumstances, you may also decide to issue a "neither confirm nor deny" response – see 'When can we neither confirm nor deny we hold the information?'

What about confidentiality?

Confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third party individual without their consent. A duty of confidence arises where an individual discloses genuinely confidential information (ie information that is not generally available to the public) to you, with the expectation that it remains confidential. This expectation might result from any statutory or common law obligations to keep certain information confidential, for example, statutory prohibitions, court orders (such as witness protection measures) or anonymity orders.

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

Does the categorisation of individuals impact what information we can provide them with?

Under Part 3, competent authorities are required to make a distinction between personal data they process about different categories of individual. This includes:

- those suspected of having committed, or being about to commit, an offence;
- those convicted of a criminal offence;
- victims and complainants; and
- witnesses or those with information about offences.

You may also hold information about contacts or associates of suspects and convicted offenders.

How you categorise an individual may have a bearing on what information you are able to provide them with when responding to a SAR. The categorisation of individuals may be particularly relevant if you need to restrict an individual's access to any of their information, in particular where there is a need to protect the rights and freedoms of others. It may be a factor in weighing up risk, and balancing the fundamental rights and freedoms and legitimate interests of individuals.

For example, risk of prejudice to an investigation may vary depending on how the individual has been categorised. For example, disclosing information to the complainant may be less risky than disclosing information to a suspect. Or if two people make a SAR for information about the same issue (eg an investigation), your response to each of them may vary, depending on what information is already known by each of them. The categorisation of each person should help you identify the possible issues before you respond.

Example

The police hold information on their records about a crime. The convicted individual and victim both make a SAR for their personal information. Some of the information being processed is about both individuals. The police need to separately consider whether they can disclose this information to each individual.

In responding to the SAR made by the convicted individual, the police consider whether, having regard to the fundamental rights and freedoms of the convicted individual, it is necessary and proportionate to withhold the information to protect the rights and freedoms of others – in this case, the victim. While there are a number of reasons why they think the convicted individual has a right to the information, the police ultimately decide against disclosing it, as the convicted individual, due to their history of violence, may use this information to harm the victim.

In responding to the SAR made by the victim, the police consider whether, having regard to the fundamental rights and freedoms of the victim, it is necessary and proportionate to withhold the information to protect the rights and freedoms of the convicted individual. In weighing up the rights of both parties, the police decide the impact to the convicted individual in these specific circumstances is minimal and disclose the information to the victim.

In different circumstances, the police might decide that the information should be disclosed to the convicted individual but not the victim – eg where the convicted individual needs the information to obtain legal advice.

How you respond to individuals is up to you. It is important to document the reasons for your decision, and be able to justify your position to the ICO if required. See 'Can we restrict the right of access under Part 3?'

How you categorise individuals may also help you to target your searches appropriately – see 'Can we clarify the request in Part 3?'

How should we deal with requests from individuals who fall within multiple categories?

There may be instances where an individual falls under more than one of the categories described in the above section, 'Does the categorisation of individuals impact what information we can provide them with?' You may process an individual's personal data in different contexts, or hold their information within different files across your systems.

Example

The police process an individual's personal data for the purpose of investigating crime. The individual is a suspect in a burglary, but is also a prosecution witness in a murder case. They are the complainant in an assault case, and the key witness in a dangerous driving case.

If an individual falls within more than one category of data subject, it is important that you are able to clearly identify and distinguish between these different categories, in relation to each piece of information you hold about the individual. If the individual makes a SAR to you, it is important that you are able to identify what information their request relates to, and whether any of the section 45(4) restrictions are relevant to the specific information requested.

You may consider risk broadly. In many circumstances, disclosing personal data which relates to one case, may risk prejudicing another case. For example, it may be reasonable to restrict an individual's right of access if disclosure would prejudice a separate or linked investigation. However, you must be able to justify why you have restricted an individual's right of access in these circumstances, and you should ensure that any restriction is necessary and proportionate. See, 'What is a "necessary and proportionate measure"?'.

If you receive a SAR from an individual who falls within multiple categories, it may be helpful to ask the individual to explain what information they are looking for or to provide general details about what their request relates to (See 'Can we clarify the request in Part 3?').

If an individual does not provide further clarification, you should still perform a reasonable search and respond to the SAR within the usual time limit (See 'How long do we have to comply?').

Depending on the circumstances, you may deem a request to be manifestly unfounded or excessive instead – for further details, see our guidance on manifestly unfounded or excessive requests.

For further details about how to make searches, see our right of access guidance – 'How to find and retrieve the relevant information?'

Relevant provisions in the legislation

See DPA 2018 sections 38(3) 44(4)(e), and 45(4)(e)

Further reading – ICO guidance

'What is personal data?'
Guide to Law Enforcement - Categorisation of individuals
'Access to information held in complaint files'

What do we need to consider if personal data is processed by a court for law enforcement purposes?

In detail

Does an individual have a right to access personal data created by a court?

An individual does not have a right to access their personal data by making a SAR if it is contained in:

- a judicial decision; or
- in another document created by or on behalf of a court or other judicial authority in connection with,
    - a criminal investigation, or
    - criminal proceedings, including proceedings for the sentencing of an offender.

The DPA 2018 describes such information as "relevant personal data".

This does not mean that competent authorities will not be required to disclose personal data. Usually, there will be other ways for individuals to access their information.

Bear in mind that the ICO does not regulate the processing of personal data by an individual, court or tribunal acting in a judicial capacity. In England and Wales, such processing is overseen by the Judicial Data Protection Panel.

What does "by or on behalf of a court or other judicial authority" mean?

The terms "judge", "judicial authority", and "court" are often used interchangeably. As this exception only applies in the context of criminal proceedings, the term "by or on behalf of a court or other judicial authority" should be interpreted narrowly.

The term "court or other judicial authority" includes any individual or organisation acting in a judicial capacity. In general, this exception to the right of access only applies if the controller is a judge, magistrate, or other judicial authority **and** they are processing the information for a criminal case, including sentencing proceedings. As a general rule, this exception will apply to judges or judicial authorities presiding over criminal cases or appeals, either alone or as part of a panel. However, it may also apply to independent judicial commissioners, if they are performing a judicial function in respect of a criminal matter. It may also include sheriffs and summary sheriffs presiding over criminal cases in Scotland.

In England, Wales, and Northern Ireland, this includes judges or judicial authorities presiding over:

- Magistrates' Courts;
- Crown Courts;
- the Court of Appeal
- the County Court (in Northern Ireland only);
- the High Court; and
- the UK Supreme Court.

In Scotland, this includes:

- the High Court of Justiciary;
- Sheriff Courts hearing a criminal matter;
- Justice of the Peace Courts; and

- Sheriff Appeal Courts.

It does not apply to competent authorities with powers to issue out of court disposals, for example police or local authorities issuing fines, cautions or conditional discharges.

This exception does not just apply to documents created by a judge, for example, notes made by the judge in the course of a criminal trial. It can also cover any documents commissioned by the judge or within the exclusive jurisdiction of the court. This includes documents created by non-judicial organisations **on behalf of** the court.

Example

The judge asks the Probation Service to prepare a pre-sentence report on its behalf. The judge will then use the report to determine an appropriate sentence for the convicted offender.

In these circumstances, the Probation Service is acting on behalf of the judge. The report has been commissioned by the judge, and has therefore been prepared "by or on behalf of the court".

The provision limits the circumstances when the exception may be used. It generally only applies to judicial functions, ie matters within the exclusive jurisdiction, and under the express instruction of the court.

The term "on behalf of" does not mean the same as processor in this context. Where a non-judicial organisation eg the Probation Service acts on behalf of the court or other judicial authority, it is carrying out a delegated activity to enable the judge to carry out their judicial function, eg where it prepares a report on behalf of the judge. However, the non-judicial organisation is likely to be acting as a controller in its own right, in relation to the information it processes about the individual. If it has prepared a document on behalf of the court, that document belongs to the court, and only the court may authorise its disclosure.

While the court service will often act as a processor for the judge, this exception does not apply to the administrative functions of the court, or to documents created by court staff, as these are not judicial functions.

What is a judicial decision?

In this context the term "judicial decision" means the judgment of a court in written form. However, it is not restricted to the judgment itself, and may cover any ruling or decision made by the court in the course of, or at the end of, proceedings, including:

- decisions about sentencing, or
- applications made by either prosecution or defence.

For more on this see, 'What types of documents will be created by or on behalf of a court for criminal proceedings?'

It may also include any notes, or early drafts prepared by the judge or magistrate for any of these purposes. Whilst an individual cannot make a SAR for their personal data contained in the judicial decision, where relevant, the judgment itself may be published at the conclusion of proceedings eg following an appeal.

What information will be created by or on behalf of a court for a criminal investigation?

The criminal court or other judicial authority is generally an independent decision-maker. As such, it does not therefore conduct criminal investigations.

However, other competent authorities may in some circumstances, require specific approval from the court to conduct certain types of investigations. For example, judicial approval will often be needed where police, or a local authority, want to conduct intrusive covert surveillance to investigate a crime.

Any decision made by the court in such cases, or any documents created by the judge in the course of hearing such matters (for example an application for a search warrant) will be deemed to be relevant personal data. As such it does not need to be disclosed as a result of a SAR. However, this information may only be excepted from the right of access for a certain period of time, for example until the warrant has been executed. For further details, see 'Is this exception time-bound?'.

Example

The police are investigating a drug cartel, and suspect the involvement of a number of individuals. However, they do not have enough evidence to arrest anyone.

In order to investigate the crime they want to deploy a specially trained officer to plant eavesdropping devices at the residential homes and private vehicles of the identified suspects.

However, the police require judicial approval under the relevant laws to carry out these operations. They make an application to the appropriate court. Any documents containing personal data the judge creates in the course of hearing these proceedings is relevant personal data and does not have to be disclosed if it is subject to a SAR.

The DPA 2018 does not specify that this exception to the right of access will only apply in the context of certain legislation. However, it is likely to be relevant where competent authorities make applications to a court to obtain judicial approval for carrying out surveillance or monitoring, for example under:

- the Regulation of Investigatory Powers Act 2000 (RIPA);
- the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A 2000);
- the Protection of Freedoms Act 2012; or
- for search warrants under the Police and Criminal Evidence Act 1984, the Police and Criminal Evidence (NI) Order 1989, or the Police, Public Order and Criminal Justice (Scotland) Act 2006.

What information will be created by or on behalf of a court for criminal proceedings?

Any documents created by or on behalf of the court or other judicial authority (either before, during or after the criminal proceedings in question) may be excepted from the right of access requirements. However, some information may only be excepted for a certain period of time. There may also be alternative routes for obtaining access to the information.

Therefore, you are not required to disclose records made by the court or on its behalf in the course of criminal proceedings, in order to comply with a SAR. This may include judges notes or documents prepared in the course of a trial, eg where the defence makes an application for some evidence to be declared inadmissible, on the basis it is not relevant to the criminal case.

Example

Counsel for the defence is acting for an individual charged with possession of cannabis with intent to supply. The prosecution wants to submit evidence that the defendant has previous convictions for burglary and common assault.

The defence counsel makes an application to the court to have such evidence excluded on the basis it is irrelevant and prejudicial to the individual's defence.

Any notes or other documents created by or on behalf of the court, whilst hearing the applications made by both prosecution and defence, or in reaching its final decision, is not disclosable further to a SAR.

The exception can also cover documents commissioned by the judicial authority, and created by a non-judicial organisation on behalf of the judge. This includes circumstances where a court is required by law to obtain a specific document, or the judge has exercised their discretion and orders that such a document is prepared, for example a pre-sentence report prepared by a probation officer.

Example

In making a decision about sentencing an individual who was found guilty by a jury of dangerous driving, the court commissions the probation officer to prepare a pre-sentence report on its behalf. The pre-sentence report will assist the court in determining the most suitable sentence for the defendant.

In advance of the sentencing proceedings, the individual makes a SAR to the court office for their pre-sentence report. However, the court office refuses to provide the information under a SAR as it is excepted from the right of access requirements. It is however, able to provide the individual with a copy under other legislation.

Access to court documents is generally covered by different rules. So even if information may not be disclosed under a SAR, there will usually be another way for the individual to access the information.

For example, the defendant may be able to access their personal data under legislation which governs the disclosure of information in criminal proceedings. In England, Wales, and Northern Ireland, this is the Criminal Procedure and Investigations Act 1996. In Scotland, this is the Criminal Justice and Licensing (Scotland) Act 2010.

Bear in mind that the personal data used to inform the document, will be potentially disclosable under a SAR, even if the report itself is not.

Example

An individual is aware that a probation officer is preparing a pre-sentence report about them, in advance of sentencing proceedings. The individual makes a SAR to the Probation Service, asking it to provide them with access to their personal information.

The Probation Service is processing personal data about the individual which it will use to prepare the pre-sentence report. As the judge has commissioned the report, this means the report itself contains relevant personal data and is therefore excepted from the right of access requirements. However, the information used by the Probation Service to inform the report is potentially disclosable further to the SAR, even though the report itself is not. Although the report may not be provided further to the SAR, the individual will be entitled to see a copy of the report in the course of the proceedings.

What does "relating to" mean?

The term "relating to" should be interpreted broadly. It is generally used to refer to information about, or linked to the proceedings. It does not just include admissible evidence, or information relevant to the outcome of the case. It can apply to most information created by or on behalf of a court in the course of the proceedings, including information which is not really relevant.

Example

During a Crown Court criminal trial, the judge makes a note of the names of prosecution and defence counsel, instructing solicitors, defendant, witnesses, the complainant, and other individuals present.

The judge also notes that the defence counsel is not wearing appropriate court dress for Crown Court proceedings and reprimands them, before making an adjournment.

The defence counsel makes a SAR for a copy of the judge's notes. However, as the notes were made during the course of criminal proceedings, the court can rely on the exception, and refuse to disclose the note further to the SAR.

What does "for the purpose of executing a criminal penalty" mean?

The term "for the purpose of executing a criminal penalty" is not specifically defined, but should be interpreted in the general context and meaning of sections 43(3) and (4) of the DPA 2018. Since the exception typically only applies to judges or magistrates who process information in the course of a criminal trial, it will generally mean any sentence handed down by the court. For example, this can cover documents created by or on behalf of a court in issuing a discharge, fine, community sentence, or custodial sentence. It may also apply to courts with powers to hear appeals about the length of a sentence, for example.

It does not apply to other competent authorities with powers to issue out of court disposals, such as fines or cautions. Any documents created by such authorities for these purposes are potentially disclosable under a SAR.

Does the exception cover documents filed or placed in the custody of the court?

No. This exception does not cover documents filed or placed in the custody of the court.

In a criminal trial, the prosecution and defence will produce and test evidence, by examining and cross-examining witnesses in order to make their case to the court. Any documents or other evidence (eg witness statements, medical or forensic reports, or skeleton arguments) they submit

to the court is for the purpose of advancing their case. While the legal representatives are duty bound not to mislead the court, they are not carrying out any judicial functions.

However, any notes or documents created by the judge during the course of the criminal proceedings will be excepted from the right of access provisions. See 'What types of documents will be created by or on behalf of a court for criminal proceedings?'

Does the exception apply if the court has shared the information with another organisation?

It depends. This exception does not usually apply to information the court or other judicial authority has shared with another organisation, or the parties to the case. The individual may make a SAR to the organisations which received copies of the information, unless the judge disclosed the information in confidence or caveated the disclosure with certain conditions. If so, you must have regard to any court order or specific judicial instructions in relation to the data.

Is this exception time-bound?

There is nothing in the legislation to suggest that the exception only applies until the criminal proceedings have concluded. It really depends on the circumstances and the nature of the information.

For example, information may be excepted from the right of access until it has been disclosed under statutory or common law procedures, during the course of proceedings, or at the conclusion of proceedings, eg the pre-sentence report, and the judicial decision. However, it is likely that certain information will be excepted from the right of access indefinitely, for example judges' notes.

Relevant provisions in the legislation

See DPA 2018 sections 21(2), 29, 43(3) and (4), and 117

Further reading – ICO guidance

UK GDPR right of access – 'Unstructured manual records'
Law Enforcement Guidance – 'Categorisation.'
Guide to the UK GDPR – 'Storage Limitation'.

Can the right of access be enforced under Part 3?

In 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, or their duty to give the individual enough information to allow them to make a SAR.

In these circumstances, the individual can ask the ICO to check that the controller acted lawfully in refusing their SAR or restricting any of their rights.

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

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

The ICO will exercise these enforcement powers in accordance with our Regulatory Action Policy.

Whilst a processor does not have any obligations under section 45 of the DPA 2018, under section 59 the controller and processor must have a contract in place. The contract must state that the processor will assist the controller with their obligations to comply with a SAR by taking appropriate technical and organisational measures, as far as this is possible (taking into account

the nature of the processing). For more information please read our UK GDPR guidance on contracts between controllers and processors.

If you are a joint controller, you will only be liable to the extent you are responsible for the specific action in question, under the terms of the joint arrangements. Joint controllers must ensure they make appropriate joint arrangements for dealing with SARs – see 'Who is responsible for responding to a request?'.

However, bear in mind that the ICO may issue an information notice or assessment notice against any individual.

Can a court order be used to enforce a SAR?

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

If you are a joint controller, bear in mind that a court may only make an order against you, to the extent you are responsible for the specific action in question, in accordance with the terms of the joint arrangements.

Can an individual be awarded compensation?

If an individual suffers damage or distress (which includes financial loss) because a controller has infringed their data protection rights (including by failing to comply with a SAR) they are entitled to claim compensation from them. They are only able to claim compensation from the processor if it has not complied with any of its statutory obligations, or has acted outside or contrary to the controller's instructions.

If you are a joint controller, and your responsibilities for SARs are covered in your joint arrangements, you will only be liable if you are responsible for complying with the provision which has been contravened, in accordance with the terms of the joint arrangements.

Only the courts can enforce an individual's right to compensation. However, they may seek to settle their claim with you directly first before starting court proceedings. You will not be liable to pay compensation if you can prove that you are not responsible in any way for the event giving rise to the damage.

Is it a criminal offence to destroy and conceal information?

Yes. It is a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information a person making a SAR would have been entitled to receive. It is a defence if you can prove that:

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

Relevant provisions in the legislation

See DPA 2018 sections 44, 45, 51, 167, 169, and 173

Further reading – ICO guidance

Regulatory Action Policy
Contracts and liabilities between controllers and processors