Complying with a Subject Access Request

information commissioner
Barrantagh Fysseree

The contents of this guidance note are set out below.

Contents

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

Legal Responsibility of Controllers

Controllers are required to "facilitate the exercise of data subjects rights", including the right of access to personal data.

The right of access is exercised by making a request, usually known as a 'Subject Access Request' ("SAR"). This right allows an individual (data subject) to find out what "personal data" about them is being processed by a controller.

The right of a data subject to access their personal data is unaffected by any other existing or potential matter or action between the controller and data subject, for example, staff disciplinary matters or employment disputes.

No enactment or rule of law that would otherwise prohibit or restrict the disclosure of information, or authorise the withholding of information, removes or restricts the right of access to personal data.

The only restrictions on the right of access are those set out, and to the extent specified, in Schedule 9 to the GDPR and LED Implementing Regulations 2018. A controller must be able to demonstrate how the relevant restriction was engaged and why it was necessary to restrict the right of access to the specific personal data in any particular situation.

Consequences of failing to comply with a subject access request

Failure to comply with a SAR could mean that the data subject could:

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

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

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

What law gives this right and governs how to respond?

Article 15 of the Applied GDPR provides the right of access to personal data and, together with Article 12, sets out the requirements and obligations on controllers when complying with a SAR.

Controllers should record the actions they take when dealing with SARs as this may be required by the Commissioner should a complaint be made.

Where a data protection officer (DPO) has been designated under Article 37 of the Applied GDPR, the contact details for that DPO must be made available via transparency information. Data subjects may, under Article 38(4) of the Applied GDPR, contact the DPO with regard to the exercise of their rights.

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

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

Technicalities of subject access requests

Who can make a SAR?

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

A data subject is an *"identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

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

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

- A legal representative acting on behalf of the data subject

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

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

What will a SAR look like?

There is no standard format.

SARs can be made **verbally or in writing**, including via electronic means. Although controllers may produce SAR forms, individuals cannot be obliged to complete a form, nor can controllers make responding to a SAR conditional on completion of that form.

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

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

Can a fee be charged?

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

Is some form of identification necessary?
No - it is not necessary, particularly when the data subject is known to the controller.

In general, the controller may only request the provision of additional information necessary to confirm the identity of the data subject where the controller has reasonable doubts concerning the identity of the data subject making the SAR.

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

The additional information obtained to confirm identity will itself be personal data and must be processed in line with the principles. In particular, it should be adequate, relevant and the minimum necessary for the purpose of identifying the data subject and the personal data they are seeking.

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

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

It is important to ensure that the personal data supplied in response to the SAR is provided to the correct data subject and it may be appropriate to ask the person collecting the information to provide suitable identification at the point of collection (recording what was provided, but not retaining a copy).

This may be particularly important if the personal data supplied in response to the SAR is special category data, for example, medical or social care records, or police records.

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

What can be sought under a SAR?

Information constituting the "personal data" of the data subject can be sought under a SAR, but it is not a right to copies of documents, emails, etc. that contain the personal data.

Personal data is defined as "any information relating to an identified or identifiable natural person". More information about what constitutes "personal data" can be found on the website.

For example, the fact that the data subject's name is included as the signatory to a letter or sender/recipient of an email, does not automatically make the content of the letter/email the personal data of the data subject. Whilst the content may include some 'personal data' if it is about the data subject, any content about anyone else, or any other matter, will not be the 'personal data' of the data subject.

What if the request is not clear?

A data subject is not obliged to tell you why they are making the SAR, or to specify what they are seeking. Equally, they may be seeking particular personal data and specify what they want, for example by reference to an event, time or date.

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

This will make sure **the controller** is looking for the right personal data and **the data subject** will receive what they really want.

You cannot ask the requester to narrow the scope of their request, but you can ask them to provide additional details that will help you locate the requested information, such as the context in which their information may have been processed and the likely dates when processing occurred. The data subject may refine their request as a result; however, they are entitled to ask for 'all' the personal data held about them.

Controllers cannot expect a data subject to know how filing systems work, where the information is stored, or who may have sent emails or correspondence that may contain their personal data. Such information should not therefore be sought.

A controller is not excused from complying with a SAR if a data subject refuses to provide additional information, does not respond to a request for such information, or is unable to provide it, and must make reasonable searches for the information covered by the SAR.

Is there any information that cannot be released?

Yes - in some cases there are restrictions on the right of access; the only restrictions are set out in Schedule 9 of the Implementing Regulations.

However, the restrictions only apply in particular circumstances, to certain personal data, and sometimes only by specified controllers.

These are not 'bans' on providing a data subject with their personal data, nor from providing as much personal data as possible that does not fall within the scope of the particular restriction.

There are no 'blanket' exemptions and it is unlikely that any one restriction will apply to all personal data. Each separate instance of personal data must be considered separately, taking into account the context and purpose for processing.

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

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

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

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

What is the time frame for taking action on a SAR?

You must provide the personal data requested **promptly** and in any event **within a calendar month**.

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

There is no stop/start provision in calculation of the period for compliance.

If no personal data is being processed you must still communicate this to the data subject within a calendar month, in accordance with Article 12(4) - failure to do so will be an infringement.

Can the time be extended?

The time can only be extended in the restricted circumstances set out in Article 12(3) of the Applied GDPR permits an extension of up to two further calendar months if necessary when a SAR is particularly complex or due to the number of requests from the data subject.

The volume of data does not make a request 'complex', but may indicate that the controller is infringing the principles of data minimisation and storage limitation. You should ensure appropriate records management procedures are in place to handle large requests and locate information efficiently.

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

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

What must be included in the response to the data subject?

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

- The purposes for processing
- The categories of personal data processed
- Recipients of classes of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries
- The envisaged period for which the personal data will be stored where possible, or , if not possible, the criteria used to determine that period
- The source of the data (if available) if they were not obtained directly from the data subject
- Details of any automated processing or profiling and the logic involved
- Details of the appropriate safeguards (Applied GDPR, article 46) relating to transfers of personal data to any third country
- The existence of the rights to rectification, erasure and restriction of, and/or objection to, processing
- The right to lodge a complaint with the Commissioner

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

There is no exemption from providing those details to the data subject.

How should the personal data be provided?

Article 15(3) obliges controllers to **provide the data subject with a copy of the personal data undergoing processing**.

If a SAR is made electronically, a copy of the personal data should be provided to the data subject *"in a commonly used electronic form"*, wherever possible, unless the data subject requests otherwise. In

other cases, it is suggested that you communicate with the data subject about the means by which the information is to be provided.

A data subject is entitled to **"a copy"** of their personal data - a controller is not obliged to provide a copy of the personal data in more than one format and may charge a *"reasonable fee based on administrative costs"* for any further copies of the personal data.

However, the practice of making personal data **available** to the data subject via a third party online storage provider does not, in the Commissioner's opinion, amount to the **provision** of a **copy of the personal data in a commonly used electronic form** by the controller. In such cases, the data subject will be required to take action to either download or print their personal data in order to acquire the "copy of the personal data" that the **controller** is obliged to "provide" in accordance with Article 15(3).

The third party storage provider will be likely, in any event, to be acting as a processor, requiring the controller to enter into an appropriate contract in accordance with Article 28.

FAQs

The data subject has been given the information they have asked for before - do we have to comply with the SAR

Yes - unless the personal data was supplied in response to a previous SAR.

If the information was given to the data subject in any other circumstances or for any other reason, there is no exclusion from the obligation to comply with the SAR.

The data subject has previously made a SAR – do we have to do it again?

Not necessarily.

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

The controller:

- must inform the data subject without delay and within one month if it is **not going to act** on the request;
- *"bear[s] the burden of demonstrating the manifestly unfounded or excessive nature of the request"* .

Failure to do the above will infringe Article 12 of the Applied GDPR and may lead to remedial action being taken by the data subject, including making of a complaint to the Commissioner or court action against the controller.

However, if a previous SAR was refused, or partially refused, due to the application of exemptions, those exemptions may no longer apply and the controller should comply with the new SAR.

There is information about other people mixed in with the data subject's personal data

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

- Controllers should record their decisions about disclosure.

Separate guidance is available on dealing with third party information.

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

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

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

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

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

However, there are significant differences between the right of access and the legal disclosure process and the information you are required to provide.

The file contains medical records, what should I do?

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

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

The request is for CCTV footage

Details about where the data subject was, and an approximate time, will be needed to help locate the footage required.

If the data subject is not known to the controller, then the data subject should be asked to provide an up-to-date photograph of themselves against which images can be compared.

In most cases, unless the CCTV system and software is sufficiently sophisticated to use facial recognition techniques, images cannot be located without human intervention in reviewing the footage. If the data subject cannot provide a reasonable timeframe, location and comparative image, the controller may consider whether the request is "excessive" and, if so, may choose whether to refuse to act on the request or charge a reasonable fee based on administrative costs for doing so. The controller must, however, advise the data subject of that decision and bears the burden of demonstrating the "excessive" nature of the request. (Article 12(5))

The right of access only applies to images of the data subject making the request - the controller may be required to redact or obscure images of other persons.

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

No – Whilst the Commissioner makes general guidance available on the website, the controller must make that decision. The controller must be able to demonstrate which restriction/exemption applies, which personal data it applies to and why it was necessary to apply that restriction or exemption.

The main obligation is to provide a copy of the personal data - if there is any doubt whether the right should be restricted, then the controller can seek legal advice as necessary.

General guidance on actions to comply with a SAR

Search

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

Collate information and review

1. **Identify the personal data**

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

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

See the separate guidance on dealing with third party information.

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

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

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

Prepare a copy of the personal data for the data subject

The right of access is not a right to copies of documents that contain personal data.

A controller may, of course, provide the individual with a copy of the document, with other information or third party information removed, or redacted.

A controller may also, for example, copy and paste the personal data contained within documents, emails etc, into a new document, or if a request has been made for a recording of a telephone call, transcribe the call.

Both methods will satisfy the requirement to *"provide a copy of the personal data"* provided sufficient contextual information or narrative is also supplied to enable the data subject to understand where the personal data emanates from.

Provide a copy of the personal data to the data subject

Before providing the personal data –

Check:

- Is it all "personal data"?
- Does it all relate specifically to the data subject?
- Is there any information identifying third parties that should be withheld/redacted?
- If you have applied redactions to any information, are they irreversible?
- Are the files marked to show this personal data has been supplied under a SAR?
- Is there a copy of the details in case they get lost in transit, or are queried?
- If a copy is kept, where, and for how long, is it stored?
- Is there a record of compliance with the SAR in the event a complaint is lodged with the Commissioner or court action against the controller is instigated?

Provide a copy of the personal data to the data subject together with the other information specified in Article 15(1) (See ***"What must be included in the response?")***

In some cases, it is appropriate to ask a data subject to collect their personal data, for example in the case of medical records or other sensitive records. It may also be appropriate to request sight of some form of identification at the point of collection. This protects both the controller and data subject against possible unauthorised disclosure to the wrong person, or the possibility of sensitive information being lost in transit. Asking a data subject to collect the copy of their personal data does not infringe the controller's obligation to "provide a copy".

Appendix – example of SAR process