Data Protection and PECR Training
Supporting notes and further reading
Module 8 : The rights of the individual part 1

Introduction

These notes are designed to set out the key points covered during module 8 of our data protection online training programme. These notes are not designed to replace the online module, but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes and the relevant legislation open whilst watching the online module:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

This document contains:

- Supporting notes
- Further reading

Supporting notes

Module 8 looks at the right of access. It covers:

- The right of access
- Making a SAR
- Responding to a request
- Proof of identity
- The timescales for responding
- Extending the timescales
- A complex request
- Asking for clarification
- Requests which involve third party data
- Making a SAR on another person's behalf
- Making a request on behalf of a child
- Refusing a SAR
- A manifestly unfounded request
- A manifestly excessive request
- Asking for a fee
- A reasonable fee

The right of access

An individual has the right to obtain confirmation that their personal data is being processed and, if so, to access that data.

This right is commonly known as a subject access right and we often refer to people making a SAR or DSAR.

Article 15 lists the information an individual is entitled to, and this includes:

- the purposes of the processing;
- the categories of personal data; and
- the existence of the data subject's rights, for example, the right to object to processing.

There is a full list in the guidance and in Article 15.

Making a SAR

The UK GDPR does not set out formal requirements for a valid request.

Our guidance explains that an individual can make a SAR verbally or in writing, including by social media.

A request does not have to include the phrase 'subject access request'. It just needs to be clear that the individual is asking for their own personal data.

A controller cannot insist the requester fills out a specific form but may have an electronic form for requesters to use. It might also have a form for recording verbal requests.

We recommend that as a matter of good practice, a controller records details of all the requests it receives, particularly those made verbally.

An individual does not have to tell the controller their reason for making the request.

If a controller has doubts over the identity of the requester, it can ask for further information to confirm this.

Responding to a request

If requested, the controller is obliged to provide a copy of the personal data undergoing processing.

If the data subject asks for any further copies of their data, then the controller can charge a reasonable fee based on administrative costs (see below: Charging a fee).

When requested by the data subject, the information may be provided orally, but only if the controller is satisfied of the data subject's identity.

This might work well when there is only a small amount of information that the data subject is entitled to, or if there's another reason the individual has requested a verbal response.

Where the request is made by electronic means, the information should be provided in the same way, unless otherwise requested by the data subject.

Finally, Recital 63 states that where possible the controller should provide remote access to a secure system.

Proof of identity

A controller should ensure that it is satisfied of the data subject's identity before providing any information.

This may not be necessary if the requester's identity is obvious to the controller, especially if they have an ongoing relationship. The controller must take a reasonable and proportionate approach.

If a check is required:

- the controller should use 'all reasonable measures' to verify the individual's identity;
- it should ask for proof of identity within one month and as soon as possible;
- the period for responding to the request begins the day the controller receives the proof of identity;
- it then has one month to respond.

The timescales for responding

The controller must respond to the request without undue delay and within one month of its receipt.

The UK GDPR does not define a month, but we interpret this as meaning a calendar month. If a controller receives a request on 1 July, then the time limit will start that day and the deadline will be 1 August.

If the request is made at the end of a month, the date for response is the last day of the following month. The response to a request received on 31 August is due on 30 September.

If the deadline date falls on a weekend, or is a public holiday, the organisation would have until the end of the next working day to comply.

This means that the exact number of days for compliance with a request will vary, depending on the month in which the request was made.

If a consistent number of days is required, our guidance suggests a controller may decide to adopt a 28-day period to ensure compliance is always within a calendar month.

Extending the timescales

A controller can extend the time limit by a further two months – calculated as three months from the start of the initial period. If an organisation receives a request on 8 August and extends the period by two months, it has until 8 November to comply with the request.

The controller should tell the data subject it requires an extension as promptly as possible, and not wait until the month has elapsed before telling them it's claiming another two months.

The controller can only claim a two month extension where necessary, taking into account:

- the number of requests from that individual (this can include other types of request, which might be other access requests or a request for erasure or restriction of processing); or

- the complexity of the request from that individual, and of any others they have submitted.

Article 12(3) to 12(6) in the UK GDPR applies to all the data subject's rights and outlines the timescales for a response.

A complex request

The UK GDPR doesn't define a complex request. We provide our definition in our guidance.

Whether a request is complex depends upon the specific circumstances of each case. What may be complex for one controller may not be for another – the size and resources of an organisation are likely to be relevant factors.

A request is not complex solely because the individual requests a large amount of information. This may add to its complexity, but it is not enough on its own.

A request is not complex just because a controller has to rely on a processor to provide the information it needs in order to respond.

Our guidance lists a number of factors which might add to the complexity of a request and these include:

- technical difficulties in retrieving the information – for example if data is electronically archived;

- applying an exemption that involves large volumes of particularly sensitive information;

- needing to obtain specialist legal advice.

Example: a controller receives a SAR from a data subject on 10 September

- it holds a large amount of sensitive information which might be exempt
- this will take some time to review so the controller considers the request is complex
- on 20 September the controller informs the data subject that it needs more time to respond and it extends the deadline by a further two months
- the controller responds by the new deadline of 10 December

Asking for clarification

If the controller processes a large amount of information about an individual, it may ask them for clarification before responding.

For example, it might ask the requester to specify the information required or processing activities their request relates to. If necessary, it should provide the requester with advice and assistance to help them narrow their request.

The time limit for responding to the request is paused until the controller receives the clarification. This is referred to as 'stopping the clock' and the controller should explain this to the data subject when requesting the clarification.

For example, if a request is received on 1 July, the deadline for a response is 1 August. If clarification is requested and it takes three days to arrive, the deadline will be extended by three days to 4 August. So the clock has been paused for three days and starts running again once clarification is received.

A controller should only ask for clarification if:

- it is genuinely required in order to respond to a SAR; and
- the controller processes a large amount of information about the individual.

It is up to the controller to decide if it wants to ask for clarification, and it may choose to perform a reasonable search instead.

If the controller does decide to ask, it must be satisfied that it holds a large amount of information, and that it is not clear what the individual is requesting. In these circumstances, it is reasonable to request clarification so the controller knows what it is looking for and where to look.

But an individual cannot be forced to clarify their request and is entitled to ask for 'all the information held' about them.

If clarification is refused, a controller must comply with the request by making reasonable searches for the information.

If the controller asks for clarification, and the data subject doesn't respond, after a reasonable period it can consider the matter closed.

This is discussed further in the guidance.

Example: a controller receives a SAR from a data subject on 1 October. The deadline is 1 November.

- the requester asks for 'all the information' held about them
- the controller processes a large amount of information about the individual and it is not clear exactly what the request relates to
- on 10 October the controller asks the data subject to clarify the request and for any information which will help it focus its search
- this clarification is received on 20 October
- the clock has stopped for 10 days and starts running again when clarification is received. 10 days is added to the original deadline
- the controller must respond to the request by 11 November

Requests which involve third party data

Individuals only have the right of access to their own personal data, although sometimes this can be linked with someone else's data (a third party).

The UK GDPR says that the right of access should not adversely affect the rights and freedoms of others.

The DPA (Schedule 2, Part 3, paragraph 16) covers requests which involve other people's personal data. Paragraph 16(1) states that the controller is not obliged to disclose information to the data subject, if doing so would involve disclosing information relating to another individual who can be identified.

But this isn't absolute because paragraph 16(2) allows the controller to comply with a request which includes someone else's data if:

- the other individual has consented to the disclosure; or
- it would be reasonable in all the circumstances to comply with the request without that individual's consent.

In this situation, it is a matter of balancing the data subject's right of access against the other individual's data protection rights.

The DPA says that the controller should take the following into account:

- the type of information to be disclosed;
- any duty of confidentiality it owes to the other individual (for example, did that individual disclose the information to them in the expectation it would remain confidential, such as information given to a doctor by a patient);
- any steps the controller has taken to obtain their consent;
- whether the individual(s) are capable of giving consent (for example, they might be a very young child or can't be contacted);

  and

- any express refusal by the other individual.

These considerations often apply when an individual requests their personal data in a Tribunal investigation where witnesses have given evidence about them. The controller must consider its duty of confidentiality to those witnesses.

The controller must also consider what is reasonable in all the circumstances so this isn't an exhaustive list. Please see our guidance for further information.

Example: a patient in hospital makes a complaint about a nurse and then requests a copy of the report investigating the complaint

- the details of the complaint will be the patient's personal data and so will be provided
- any steps taken against the nurse will be the nurse's personal data and will not be disclosed to the patient
- the care of the patient by the nurse will be the personal data of them both
- without the nurse's consent to disclose this data, the controller should consider whether, in all the circumstances, it is appropriate to release information that concerns both the patient and the nurse to the patient
- its considerations should include any duty of confidentiality it has to the nurse

The DPA also outlines a test of reasonableness to disclosure - without consent of the other individual - of health data, social work data and education data. Please see the guidance for more details.

Making a SAR on another person's behalf

There is nothing in the UK GDPR to prevent someone making a SAR on another individual's behalf.

It is that person's responsibility to provide the controller with evidence that they are entitled to act on behalf of the data subject.

This might be written authority from the data subject or a more general power of attorney.

There are no specific statutory provisions to enable someone to exercise subject access rights on behalf of another person who does not have the mental capacity to manage their own affairs.

But it is reasonable to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority.

In most cases, provided the controller is satisfied that the individual making the request has the appropriate authority to do so, it should respond directly to that person.

Making a request on behalf of a child

A child's personal data is their own personal data. This means that parents or guardians do not have a specific right to their children's personal information.

They can make a request on behalf of their child, provided the controller is satisfied the parent or guardian concerned is entitled to act for that child. The guidance outlines what the controller should consider in these circumstances, for example, any duty of confidence it owes to the child.

A child may exercise their UK GDPR rights on their own behalf as long as they are competent to do so.

If they make a SAR themselves, the controller would need to be satisfied they understand the nature of the request. They must make a judgement on a case-by-case basis, taking into account the particular child, the nature of the data and the circumstances of the request.

In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This is not the case in England, Wales or Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

In some cases, the controller may have to ask the child over 12 for written permission for their parent to make a SAR on their behalf.

Remember that in relation to information society services, the DPA allows a child over 13 to provide their own consent to processing.

Example: a father makes a SAR to the schools his two children attend, to request their personal data

- the father does not have parental responsibility
- the younger child is 6 and so the primary school refuses the request
- the older child is 14 - their school considers they have competence to make their own SAR
- the school asks this child if they wish their father to make a SAR on their behalf
- the older child refuses to give their authorisation and so their school also refuses this request.

Parents making requests on behalf of their children is a complex issue and is often contentious.

Even if a parent has parental responsibility, a controller might apply an exemption and refuse to provide the personal data. For example, if it considers it would not be in the best interests of the child to provide their personal data in response to the SAR.

There is also other legislation which gives a parent the right to access their child's educational records. Please see the guidance for more information.

Refusing a SAR

A controller can refuse a SAR if:

- an exemption applies; or
- the request is manifestly unfounded or manifestly excessive.

If a controller refuses a request, it must inform the data subject without delay and at the latest within one month.

We will discuss exemptions in modules 10 and 11.

A manifestly unfounded request

A manifestly unfounded request might be intended to cause disruption or is clearly prompted by malice. It must be considered in the context in which it is made and is unlikely to be manifestly unfounded if the individual genuinely wants to exercise their rights.

A manifestly excessive request

A manifestly excessive request should be clearly unreasonable.

The controller should consider whether the request is proportionate when balanced with the burden or costs involved in dealing with it.

The controller must take into account all the circumstances of the request, including:

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

There are further details in our guidance.

A request is not necessarily excessive just because the individual requests a large amount of information.

A controller should also consider asking the individual for more information to help it locate the information they want. Remember it can ask for clarification.

Another alternative is for the controller to ask for a fee.

Asking for a fee

In general, a copy of the information must be provided to the data subject free of charge.

But the controller can charge a 'reasonable fee' based on administrative costs if the request is:

- manifestly unfounded or excessive; or
- the data subject requests further copies of information already provided (although this doesn't mean that a controller can charge for all subsequent requests).

A reasonable fee

When determining a reasonable fee, a controller can take into account the administrative costs of:

- assessing whether or not it is processing the information;
- locating, retrieving and extracting the information;
- providing a copy of the information; and
- communicating the response to the individual.

A reasonable fee may include the costs of:

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

Staff time is based on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate.

If the controller asks for a fee, it must do so as soon as possible and within a month. It must then respond within one month of receiving that fee.

Example: a data subject requests all the personal data an organisation holds about them

- the organisation is a small company and it holds a lot of data about this individual
- the request largely repeats other requests which it has responded to very recently
- it considers it has provided all the personal data it holds about this individual
- the organisation does not want to charge a fee for retrieving and extracting this data
- it refuses the request as manifestly excessive

Example: a data subject requests all the personal data a council holds about a housing complaint they have made

- the council provides the data it holds but the individual argues it must hold more and they make another SAR asking for all the rent payments they have made over the past 10 years
- it provides this information, but the individual is still not satisfied and argues they will continue to make SARs every week until the council provides the missing complaints data they require
- they argue the data protection officer is involved in a cover-up and is wilfully holding back data. They accuse the DPO of conspiracy and incompetence. They make another SAR for all the emails they have sent to the council's Housing Department over the past 10 years
- the council considers the individual is clearly setting out to harass its DPO. It has provided the data it holds in response to the first two requests, and does not hold the specific complaints data the individual is seeking. The individual has made it obvious that they are not motivated by a genuine desire to gain access to personal data, but are now trying to simply cause disruption
- the council refuses the last request as manifestly unfounded

[Back to top](#)

Further reading

The right of access

In the Guide to the UK GDPR , under the section Individual rights, have a look at the section Right of access

Read the 'At a glance' points and the 'In brief' questions and answers.

At the bottom of the page click on the link to take you to the detailed guidance to the right of access. You should take some time to read these paragraphs but in particular, look at:

- What should we consider when responding to a request?
    - How long do we have to comply?
    - Can we extend the time for a response?
    - When is a request complex?
    - Can we clarify the request?
    - Can we charge a fee?
    - Can we ask for ID?

Find an example where a supermarket asks an employee for clarification following a request for 'all the information' held about them. Look at the clarification requested by the supermarket (see the yellow boxes for examples).

- When can we refuse to comply with a request?
    - Can we refuse to comply with a request?
    - What does manifestly unfounded mean?
    - What does manifestly excessive mean?
    - What general considerations should we take into account when deciding if a request is manifestly unfounded or excessive?

Find an example of a manifestly unfounded request (see the yellow boxes for examples).

- What should we do if the request involves information about other individuals?
    - What is the basic rule?

- What approach should we take?
- Are there any other relevant factors?
- Do we need to respond to the request?

Find an example of an individual who makes a subject access request to a council where the information held includes reports containing the personal data of other people. What considerations must the council take into account? (see the yellow boxes for examples)

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022