Right of access

At a glance

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

Checklists

Preparing for subject access requests

☐ We know how to recognise a subject access request and we understand when the right of access applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests

☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.

☐ We understand what we need to consider if a request includes information about others.

In brief

- **What is the right of access?**
- **What is an individual entitled to?**
- **How do we recognise a request?**
- **Should we provide a specially designed form for individuals to make a subject access request?**
- **How should we provide the data to individuals?**
- **Do we have to explain the contents of the information we send to the individual?**
- **Can we charge a fee?**
- **How long do we have to comply?**
- **Can we extend the time for a response?**
- **Can we ask an individual for ID?**
- **What about requests for large amounts of personal data?**
- **What about requests made on behalf of others?**
- **What about requests for information about children?**
- **What about data held by credit reference agencies?**

- **What should we do if the data includes information about other people?**
- **If we use a processor, does this mean they would have to deal with any subject access requests we receive?**
- **Can we refuse to comply with a request?**
- **What should we do if we refuse to comply with a request?**
- **Can I require an individual to make a subject access request?**

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

What is an individual entitled to?

Individuals have the right to obtain the following from you:

•confirmation that you are processing their personal data;

•a copy of their personal data; and

•other supplementary information – this largely corresponds to the information that you should provide in a privacy notice (see 'Supplementary information' below).

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data.

Other information

In addition to a copy of their personal data, you also have to provide individuals with the following information:

•the purposes of your processing;

•the categories of personal data concerned;

•the recipients or categories of recipient you disclose the personal data to;

•your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;

•the existence of their right to request rectification, erasure or restriction or to object to such processing;

•the right to lodge a complaint with the ICO or another supervisory authority;

•information about the source of the data, where it was not obtained directly from the individual;

•the existence of automated decision-making (including profiling); and

•the safeguards you provide if you transfer personal data to a third country or international organisation.

You may be providing much of this information already in your privacy notice.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to you verbally or in writing. It can also be made to any part of your

organisation (including by social media) and does not have to be to a specific person or contact point.
A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.
This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.
Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Should we provide a specially designed form for individuals to make a subject access request?

Standard forms can make it easier both for you to recognise a subject access request and for the individual to include all the details you might need to locate the information they want.
Recital 59 of the GDPR recommends that organisations ‘provide means for requests to be made electronically, especially where personal data are processed by electronic means’. You should therefore consider designing a subject access form that individuals can complete and submit to you electronically.
However, even if you have a form, you should note that a subject access request is valid if it is submitted by any means, so you will still need to comply with any requests you receive in a letter, a standard email or verbally.
Therefore, although you may invite individuals to use a form, you must make it clear that it is not compulsory and do not try to use this as a way of extending the one month time limit for responding.

How should we provide the data to individuals?

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.
The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.
However, providing remote access should not adversely affect the rights and freedoms of others – including trade secrets or intellectual property.

We have received a request but need to amend the data before sending out the response. Should we send out the “old” version?

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

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

Do we have to explain the contents of the information we send to the individual?

The GDPR requires that the information you provide to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child.
At its most basic, this means that the additional information you provide in response to a request (see the 'Other information' section above) should be capable of being understood by the average person (or child). However, you are not required to ensure that that the information is provided in a form that can be understood by the particular individual making the request.
For further information about requests made by a child please see the 'What about requests for information about children?' section below.

Example
An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to your key or index to explain this information, it would be impossible for anyone outside your organisation to understand. In this case, you are required to explain the meaning of the coded information. However, although it is good practice to do so, you are not required to decipher the poorly written notes, as the GDPR does not require you to make information legible.

Example
You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. You are not required to do this even if the person who receives it cannot understand all of it because it can be understood by the average person. However, it is good practice for you to help individuals understand the information you hold about them.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a subject access request.
However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.
You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.

How long do we have to comply?

You must act on the subject access request without undue delay and at the latest within one month of receipt.
You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.
If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.
If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.
This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example
An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.
If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.
For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.
However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:
•it is manifestly unfounded or excessive;
•an exemption applies; or
•you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.
You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

What about requests for large amounts of personal data?

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.
You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when you receive the additional information. However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request ie by making reasonable searches for the information covered by the request.

What about requests made on behalf of others?

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Exapmle

A building society has an elderly customer who visits a particular branch to make weekly withdrawals from one of her accounts. Over the past few years, she has always been accompanied by her daughter who is also a customer of the branch. The daughter makes a subject access request on behalf of her mother and explains that her mother does not feel up to making the request herself as she does not understand the ins and outs of data protection. As the information held by the building society is mostly financial, it is rightly cautious about giving customer information to a third party. If the daughter had a general power of attorney, the society would be happy to comply. They ask the daughter whether she has such a power, but she does not.

Bearing in mind that the branch staff know the daughter and have some knowledge of the relationship she has with her mother, they might consider complying with the request by making a voluntary disclosure. However, the building society is not obliged to do so, and it would not be unreasonable to require more formal authority.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters:

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

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

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

What about data held by credit reference agencies?

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

What should we do if the data includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

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

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you

disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.
For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

If we use a processor, does this mean they would have to deal with any subject access requests we receive?

Responsibility for complying with a subject access request lies with you as the controller. You need to ensure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the processor.
You are not able to extend the one month time limit on the basis that you have to rely on a processor to provide the information that you need to respond. As mentioned above, you can only extend the time limit by two months if the request is complex or you have received a number of requests from the individual.

Can we refuse to comply with a request?

You can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you need to justify your decision.
You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Act 2018

There are other exemptions from the right of access in the DPA 2018. These exemptions will apply in certain circumstances, broadly associated with why you are processing the data. We will provide guidance on the application of these exemptions in due course.

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

You must inform the individual without undue delay and within one month of receipt of the request.
You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

Can I require an individual to make a subject access request?

In the DPA 2018 it is a criminal offence, in certain circumstances and in relation to certain information, to require an individual to make a subject access request. We will provide further guidance on this offence in due course.