The right of access

At a glance

- Individuals have the right to access their own personal data.
- This is commonly referred to as subject access.
- To do so, individuals must make a subject access request ("SAR") in writing.
- You have thirty days to respond to a request.
- If you need further information from the requestor, the period of time for your response can be extended by the Regulations.
- There is no fee to deal with a request except in exceptional circumstances.

Checklist

Preparing for subject access requests:

- We know how to recognize a subject access request and we understand when the right of access applies.
- We have a policy to record the requests we receive.
- 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 thirty days 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?

The right of access, commonly referred to as subject access or as a Subject Access Request (SAR), 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?

The DPL provides that 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 includes the information you should provide in a privacy notice, but also additional information.

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

- the purposes of your processing;
- the categories of personal data concerned;

- the recipients or classes of recipient you disclose, or may disclose, the personal data to;
- any countries or territories outside the Cayman Islands to which you do, or intend to, transfer the personal data;
- the general measures you take to ensure the security of the personal data (i.e. to comply with the seventh data protection principle);
- any information available as to the source of the personal data;
- the reasons for any automated decision made in relation to the individual, including the individual's performance at work, creditworthiness, reliability or conduct; and
- the right to make a complaint to the Ombudsman.

You may have provided some of this information already in your privacy notice.

A subject access request does not need to be for all the types of information listed above. However, you should clarify to the requestor that they are entitled to the types of information listed above.

For instance, a requestor may only be interested in receiving one type of information you hold, instead of all personal data held.

Personal data of the individual and mixed personal data

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

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

Sometimes, you will come across so-called "mixed personal data", i.e. where personal data of one data subject is very closed linked to the personal data of another data subject. If the third party data subject has not consented to the disclosure of the mixed personal data, you will need to assess whether the mixed personal data will need to be redacted or whether it can be released as mixed personal data.

Example

An individual makes a request for their personal data consisting of the recording of a phone call between the data subject and an employee of the data controller. The recording contains personal data relating to

both the data subject and the employee.

Unless the employee has consented to the disclosure of the mixed personal data of the recording, the data controller will need to assess whether the overall circumstances call for the data controller to redact the phone call in order to not disclose personal data of the employee or whether the circumstances may permit a disclosure of the mixed personal data to the data subject.

You need to assess whether it is reasonable in all circumstances to disclose the mixed personal data. In particular, this will require the data controller to balance the respective interests of the affected data subjects, including:

- whether a duty of confidentiality towards the other data subject is owed;
- what type of the personal data would be disclosed;
- whether any steps were taken by the data controller to seek consent of the other data subject;
- whether the other data subject is capable of granting consent; and
- whether the other data subject has expressly refused consent.

The issue of mixed personal data is addressed in section 8(7)-(10) DPL.

How do you recognize a request?

The DPL specifies that a subject access request must be made in writing.

A request does not have to include the phrase 'subject access request' or section 8 of the DPL, 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 subject access request.

Additionally, it is good practice to have a policy for recording details of the requests you receive. 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.

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

Standard forms can make it easier both for you to recognize a subject access request and for the

individual to include all the details you might need to locate the information they want.

However, even if you have a form, you should note that a subject access request is valid if it is submitted in writing by any means, e.g. in hardcopy letter, by email, etc., so you will still need to comply with any requests you receive in any written format.

Therefore, although you may invite individuals to use a form, you must make it clear that it is optional. You should not try to use this as a way of extending the thirty-day time limit for responding.

How should you provide the data to individuals?

The DPL specifies that data should be provided in the format requested by the individual, unless:

- the supply of such a copy is not possible or would involve disproportionate effort, or
- the data subject agrees otherwise.

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

Where possible, it is best practice to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will not be appropriate for all organizations, 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.

What if the data is already open to access?

If the data is open to access by the public by law or as part of a public register, you should refer the requestor there.

If the data is available for purchase by the public in accordance with administrative procedures established for that purpose, the data must be obtained in accordance with those procedures.

You have received a request but need to amend the data before sending out the response. Should you send out the "old" version?

Strictly speaking, 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 DPL it is an offence to fail to supply, alter, suppress or destroy information that is required to be produced to the Ombudsman.

Do you have to explain the contents of the information you provide to the individual?

The DPL requires that the information you provide to an individual is in an intelligible form, which means using clear and plain language. This may be particularly important where the information is addressed to a child, or if you are a business dealing with consumers who may not be familiar with any technical terms used within documents containing personal data.

If the personal data themselves are not understandable without an explanation (e.g. because the data is coded), they must be provided accompanied by an adequate explanation.

At its most basic, this means that the information you provide in response to a request should be capable of being understood by an average person (or child). However, you are not required to ensure 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 organization 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 poorly written notes if you only have these notes and no clearer version, as the DPL 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 you charge a fee?

The personal data you have to provide following a request must be provided free of charge.

However, the Regulations provide that where the request is manifestly unfounded or excessive you may charge a reasonable fee for the costs of providing the requested data and information, or refuse to act on the request.

This will only be in very few cases, since the DPL defines a request that is “manifestly unfounded or excessive” as a request that:

- is repetitive;
- is fraudulent in nature; or
- would divert the resources of the data controller unreasonably,

As the data controller you have the burden of proving that a request is “manifestly unfounded” or “excessive”. In the event of disagreement, the Ombudsman shall decide on the facts.

How long do you have to comply with a subject access request?

You must comply with a subject access request within thirty days from the date when you receive the request.

You should calculate the time limit as thirty days from the day after you receive the request (whether the day after is a working day or not).

If you have asked for a fee or further clarification from the individual (e.g. proof of identity), this may suspend the period for responding. The period resumes when the fee and/or further information has been supplied.

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 i.e. by making reasonable searches for the information covered by the request.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to

respond.

Example

An organization receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organization until 3 October to comply with the request, (i.e. thirty days after the request was received.

Can you extend the time for a response?

Regulation 4 (1) provides that you can extend the time to respond to a request for up to thirty additional days, if:

- a large amount of data is requested or is required to be searched and meeting the timelines would unreasonably interfere with your operations;
- more time is required to consult with a third party or other data controller before you are able to decide whether or not to give the requestor access to the requested data; or
- the data subject has given consent to the extension.

If you extend, the period for responding to a request, you must inform the requestor, and provide reasons for the extension.

It is the Ombudsman'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.

Regulation 4 (2) provides that, with the permission of the Ombudsman, you can extend the period for responding to a request by more than thirty days, if:

- one or more of the circumstances described above apply; and
- the Ombudsman considers that it is appropriate to do so.

If you believe you need to extend the period for responding to a requestor for more than thirty days, you should contact the Office of the Ombudsman with all the details, and request an extension in writing.

Can you 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 if 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.

While you may need to confirm the identity of the person making the request, this does not mean you are always justified to keep a copy the information provided, due to the third and fifth data protection principles.

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.

Where the request is manifestly unfounded or excessive because the request "would divert the resources of the data controller unreasonably", 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

See above for more on charging a fee in certain circumstances.

What about requests made on behalf of others?

The DPL 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.

Example

A bank 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 bank is mostly financial, it is rightly cautious about giving customer information to a third party. If the daughter has been appointed by the court to manager her mother's affairs, the bank 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, if permitted under banking law. However, the bank 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 may not be able to manage their own affairs because they do not have the mental capacity to do so, or for another reason. Such individuals should be represented by a court-appointed guardian who can request access to their data on behalf of the data subject.

The exemption relating to education in the DP Regulations provides that where the data is an educational record that consists of information that a child has been subject to abuse, or may be at risk of it, the right to access by a parent or someone appointed by the court to manage the individual's affairs does not apply if it would not be in the interests of the child.

The exemption relating to social work in the DP Regulations also restricts the application of the right to access exercised on behalf of a data subject by a parent or someone appointed by the court, if the information was initially provided to the data controller in the expectation that the data would not be disclosed to the person making the request (unless the data subject has indicated they do not have this expectation any longer).

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. 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 authorizes 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.

The Regulations define a child as a person under the age of eighteen years old.

See also the exemption on social work and education.

What should you 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 DPL 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.

Data about a third party individual may include information on the source of the personal data. However, 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.

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

- 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.

This does not mean that you are excused from communicating as much of the personal data sought in the request as can be communicated without disclosing the identity of the other (third party) individual. This can be done by redacting or omitting the names or other identifying particulars from the data.

If we use a processor, does this mean they would have to deal with any subject access requests you 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 directly, or to the processor who acts on your behalf. For more on contracts with processors here.

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, the Regulations allow you to extend the time limit only for another thirty days if:

- a large amount of data is requested or required to be searched and meeting the deadline would

unreasonably interfere with your other operations;
- more time is required to consult with a third party or other data controller to decide on access; or
- the data subject has agreed with the extension.

In exceptional circumstances, if even more time is needed the timelines can be extended further, but only with the permission of the Ombudsman.

Can you refuse to comply with a subject access request?

The Regulations provide that you can refuse to comply with a subject access request if it is manifestly unfounded or excessive because the request:

- is repetitive;
- is fraudulent in nature, or
- would divert the resources of the data controller unreasonably.

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. In the case of disagreement, the Ombudsman shall decide on the facts.

As well, if the data is already available by law as part of a public register or otherwise, or for sale under administrative procedures, you must provide access under those administrative procedures and not under the DPL.

What are the exemptions to the right to access?

The DPL recognizes the following exemptions from the right to access:

- Section 19: if the personal data is processed for crime prevention, detection or investigation, the apprehension or prosecution of any person suspected of having committed an offence, or the assessment or collection of any fees or duty;
- Section 21: if the personal data is processed for monitoring, inspection or a regulatory function, to the extent that applying it would be likely to prejudice the discharge of the function;
- Section 24: if the data consists of information you are obliged by law to make available to the public;
- Section 27: if the personal data is processed for purposes of conferring any honour or dignity by the

Crown or the Premier;
- Section 28: if the data is processed for purposes of corporate finance and the application of the provision could affect the price of a financial instrument, or for the purpose of safeguarding an important economic or financial interest of the Cayman Islands;
- Section 29: if the personal data consists of intentions in regard to any negotiations with the individual which would be prejudiced by the processing;
- Section 30: if the personal data is being processed for legal or trust purposes;
- Regulation 7: if the release of personal data could reasonably cause mental or physical harm to any person; or
- Regulation 9: to the extent that the notification would be likely to prejudice the carrying out of social work because of serious harm to the physical or mental health or condition of any person.

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

You must inform the individual that you refuse to comply with the request without undue delay.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the Ombudsman; 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.

Relevant provisions

Data Protection Law, 2017

Sections 8-9: Right to access

Data Protection Regulations, 2018

Regulation 3: Fees for requests

Regulation 4: Extension of time for response

Regulation 6: Additional circumstances when the data controller does not have to comply with a request under section 10 (right to stop processing)