Subject Access Requests
Guide for Data Controllers

The Data Protection Law provides individuals with a number of rights. The one most commonly used is that of subject access.

This guidance note will help those processing subject access requests to meet the requirements of the Law including areas often misunderstood.

This guidance relates to both the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001.

Where the Laws differ and to show differences between the two jurisdictions the page will be split as shown below.

Jersey	Guernsey
Commissioner = Information Commissioner a = article within the Law	Commissioner = Data Protection Commissioner s = section of the Law

Where numbering of passages from the Laws are the same it will be shown as a/s.

April 2017

Table of Contents

Introduction 4

What is a valid subject access request? 5

Can we require an individual to use a specially designed form when making a subject access request? 5

Can we ask for identification from the applicant? 6

What about a subject access request made on behalf of someone else? ..7

What about requests for information about children? 8

Can we ask for more information before responding to a subject access request? 9

Can we charge a fee for dealing with a subject access request? 10

Data is due a routine update before it will be disclosed. Can we do this? 10

What should we do if the data includes information about other people? 11

Disclosure of the data now will interfere with our activities. Can it be withheld? 11

Do we have to explain the contents of the information we send to the individual? 12

What if sending out copies of information will be expensive or time consuming? 13

What about repeated or unreasonable requests? 14

If we use a data processor. Does this mean they would have to deal with any subject access request we receive? 16

What about personal data held by credit reference agencies? 16

Appendix 1 – Subject Access Process Flowchart 18

Appendix 2 – Bailiwick of Guernsey Only – Subject Access to Health Records 19

Contact the Commissioner 21

Introduction

This right, commonly referred to as subject access, is created by a/s 7 of the Law. It is most often used by individuals who want to see what information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given the information contained in personal data; and the details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person and with appropriate authority). Neither are they entitled to information simply because they may be interested in it. It is important to establish whether the information requested falls within the definition of personal data.

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

Jersey	Guernsey
You must respond promptly and in any event within **40** calendar days of receiving the request.	You must respond promptly and in any event within **60** calendar days of receiving the request.

A flowchart can be found in Appendix 1 that shows the subject access process in full and aligns to this guidance.

What is a valid subject access request?

For a subject access request to be valid, it should be made in writing. You should also note the following points when considering validity:

- A request sent by email or fax is as valid as one sent in hard copy (as long as you are satisfied as to the person's identity).

- You do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.

- If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may wish to make a reasonable adjustment for them. This could include treating a verbal request for information as though it were a valid subject access request.

- If a request does not mention the Law specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.

- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that all staff in your organisation can recognise a subject access request and treat it appropriately.

Can we require an individual to use a specially designed form when making a subject access request?

Many organisations produce subject access request forms, and you may invite individuals to use such a form as long as you make it clear that this is not compulsory and you do not try to use this as a way of extending the time limit for responding. Standard forms can make it easier for you

to recognise a subject access request and make it easier for the individual to include all the details you might need to locate the information they want.

However, any request in writing must be considered as a valid request, whatever the format.

Can we ask for identification from the applicant?

You can ask for enough information to establish whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

The key point is that you must be reasonable about what you ask for. You should not request lots more information if the identity of the person making the request is obvious to you. This is particularly the case, for example, when you have an ongoing relationship with the individual.

> Example
>
> You have received a written subject access request from a current employee. You know this employee personally and have even had a phone conversation with them about the request. Although your organisation's policy is to verify identity by asking for a copy of photographic id, it would be unreasonable to do so in this case since you know the person making the request.

However, you should not assume that, on every occasion, the person making a request is who they say they are. In some cases, it will be reasonable to ask the person making the request to verify their identity before responding to the request.

> Example
>
> An online retailer receives a subject access request by email from a customer. The customer has not used the site for some

time and although the email address matches the company's records, the postal address given by the customer does not. In this situation, it would be reasonable to gather further verifying information, which could be as simple as asking the customer to confirm other account details such as a customer reference number, before responding to the request.

The level of checks you should make may well be risk based and depend on the possible harm or distress which inappropriate disclosure of the information could cause to the individual concerned.

Example

A GP practice receives a subject access request from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requestor is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for further verifying information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious. They could ask the requestor to provide more information, such as a date of birth, a passport or a birth certificate.

What about a subject access request made on behalf of someone else?

The Law does not prevent an individual making a subject access request via a third party. This may be a legal adviser 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, and it is the third party's responsibility to provide sufficient evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

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.

What about requests for information about children?

In the Law, there is no definition or clarification about children. 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 able to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than a parent or guardian. 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;
- any views the child or young person has on whether their parents should have access to information about them; and

- any views of the professionals from your organisation that have had dealings with the child.

Can we ask for more information before responding to a subject access request?

Before responding to a subject access request you are entitled to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the subject access request until you have received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for you to delay responding to a subject access request unless you reasonably require more information to help you find the data in question.

> Example
>
> A chain of shops is dealing with a general subject access request from a member of staff at one of their branches. The person dealing with the request is satisfied that the staff member has been sent all information held in personnel files and in files held by his line manager. However, the member of staff complains that not all information about him was included in the response. The employer should not ignore this complaint, but it would be reasonable to ask the member of staff for further details. For example, some of the information may be in emails, and the employer could reasonably ask for the dates when the emails were sent, and who sent them, to help find the information requested.
>
> It might also be useful for the employer to ask if the member of staff is seeking information that does not relate to his employment. For example, he may be seeking information that relates to a complaint he made as a customer.

You should not ignore a request simply because you need more information from the person who made it. You should not delay in asking for this, but should ensure the individual knows you need more information and should tell them what details you need. Provided you have done so, the period for responding to the request does not begin to

run until you have received the appropriate fee (see below) and any additional information that is necessary.

Can we charge a fee for dealing with a subject access request?

An organisation receiving a subject access request may charge a fee for dealing with it. If you choose to charge a fee, you need not comply with the request until you have received the fee. The usual maximum fee you can charge is £10. The only differences to this are for charges for credit reference files (see page 16) and in the Bailiwick of Guernsey charges for health records (see appendix 2).

Although you need not comply with a request until you have received a fee, you cannot ignore a request simply because the individual has not sent a fee. If a fee is payable but has not been sent with the request, you should contact the individual promptly and inform them that they need to pay.

Some organisations choose not to charge a fee. However, once you have started dealing with an individual's request without asking for a fee, it would be unfair to then demand a fee as a way of extending the period of time you have to respond to the request.

Data is due a routine update before it will be disclosed. Can we do this?

The Law specifies 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 or to delay responding to ensure the data are amended or deleted.

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

Data you hold about the individual making the request may also involve information that relates both to them and to another individual or individuals. The Law says you do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

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

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 in respect of their own personal data. 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. If disclosure is made you should inform the third party and clarify the basis for the decision.

For the avoidance of doubt, you cannot refuse to provide subject 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.

Disclosure of the data now will interfere with our activities. Can it be withheld?

The Law recognises that in some circumstances disclosing information as part of the subject access process would impede the purposes for which the information is intended. For such circumstances there are a number of exemptions that organisations may apply.

These are outlined in detail in the Exemptions guidance note, found on our website. It is important to remember that the exemptions are not blanket conditions to prevent disclosure; they should be applied on a case-by-case basis after careful consideration. Given that to withhold information is restricting an individual in exercising their rights you are advised to make sure you document why it is felt the exemption applies, in order to defend that decision if needed.

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

The Law requires that the information you provide to the individual is in "intelligible form". At its most basic, this means that the information you provide should be capable of being easily understood. However, the Law does not require you to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

> 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 the organisation's key or index to explain this information, it would be impossible for anyone outside the organisation to understand. In this case, the Law requires you to explain the meaning of the coded information. However, although it would be good practice to do so, the Law does not require you to decipher the poorly written notes, since the meaning of "intelligible form" does not extend to "make legible".

> Example
>
> You receive a subject access request from someone whose English comprehension skills are poor. You send a response and they ask you to translate the information you sent them. The Law does not require you to do this since the information is in intelligible form, even if the person who receives it cannot

understand all of it. However, it would be good practice for you to help them understand the information you hold about them.

What if sending out copies of information will be expensive or time consuming?

In some cases, dealing with a subject access request will be an onerous task. This might be because of the nature of the request, because of the amount of personal data involved, or because of the way in which certain information is held.

Under a/s 8(2) of the Law you are not obliged to supply a copy of the information in permanent form if it would involve disproportionate effort to do so. You must decide whether supplying a copy of the information would involve disproportionate effort. Even if you do not have to supply a copy of the information in permanent form, the individual still has the other basic rights described above.

The Law does not define "disproportionate effort" but it is clear that there is some (albeit limited) scope for assessing whether complying with a request would result in so much work or expense as to outweigh the individual's right of access to their personal data. However, it should be noted that this qualification to the right of subject access only applies in respect of "supplying" a copy of the relevant information in permanent form. So you cannot refuse to deal with a subject access request just because you think that locating the information in the first place would involve disproportionate effort.

We stress that you should rely on this provision only in the most exceptional of cases. The right of subject access is central to data protection law and we rarely hear of instances where an organisation could legitimately use disproportionate effort as a reason for not allowing an individual to access their personal data. Even if you can show that supplying a copy of information in permanent form would involve disproportionate effort, you should still try to comply with the request in some other way.

Example

An organisation has decided that to supply copies of an individual's records in permanent form would involve disproportionate effort. Rather than refuse the individual access, they speak to her and agree that it would be preferable if she visited their premises and viewed the original documents. They also agree that if there are particular documents that she would like to take away with her, they can arrange to provide copies.

What about repeated or unreasonable requests?

The Law does not limit the number of subject access requests an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Law says that you are not obliged to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

The Law gives you some help in deciding whether requests are made at reasonable intervals. It says that you should consider the following:

- the nature of the data – this could include considering whether it is particularly sensitive;

- the purposes of the processing – this could include whether the processing is likely to cause detriment to the individual; and

- how often the data is altered – if information is unlikely to have changed between requests, you may decide that you are not obliged to respond to the same request twice.

If there has been a previous request or requests, and the information has been added to or amended since then, you might consider whether you need only provide the new or updated information to the requester. However a/s 8(6) of the Law states that "information to be supplied pursuant to a request….must be supplied by reference to the data in question at the time when the request is received…". This means that,

when answering a subject access request, you are required by the Law to provide a full response to the request: not merely providing information that is new or has been amended since the last request.

In practice we would accept that you may attempt to negotiate with the requester in order to restrict the scope of their subject access request to the new or updated information; however, if the requester insists upon a full response then you would need to supply all the information.

Example

A library receives a subject access request from an individual who made a similar request one month earlier. The information relates to when the individual joined the library and the items borrowed. None of the information has changed since the previous request. With this in mind, along with the fact that the individual is unlikely to suffer if no personal data is sent in response to the request, the library need not comply with this request. However, it would be good practice to respond explaining why they have not provided the information again.

Example

A therapist who offers non-medical counselling receives a subject access request from a client. She had responded to a similar request from the same client three weeks earlier. When considering whether the requests have been made at unreasonable intervals, the therapist should take into account the fact that the client has attended five sessions between requests, so there is a lot of new information in the file. She should respond to this request (and she could ask the client to agree that she only needs to send any "new" information). If the client does not agree, the therapist should provide a copy of all the information on the file.

But it would also be good practice to discuss with the client a different way of allowing the client access to the notes about the sessions.

We use a data processor. Does this mean they would have to deal with any subject access request we receive?

Responsibility for complying with a subject access request lies with you as the data controller. The Law does not allow any extension to the time limit in cases where you have to rely on a data processor to provide the information that you need to respond.

> Example
>
> An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party data processor is analysing the information.
>
> The employer receives a subject access request from a member of staff. To respond, the employer needs information held by the data processor. The employer is the data controller for this information and should instruct the data processor to retrieve any personal data that relates to the member of staff.

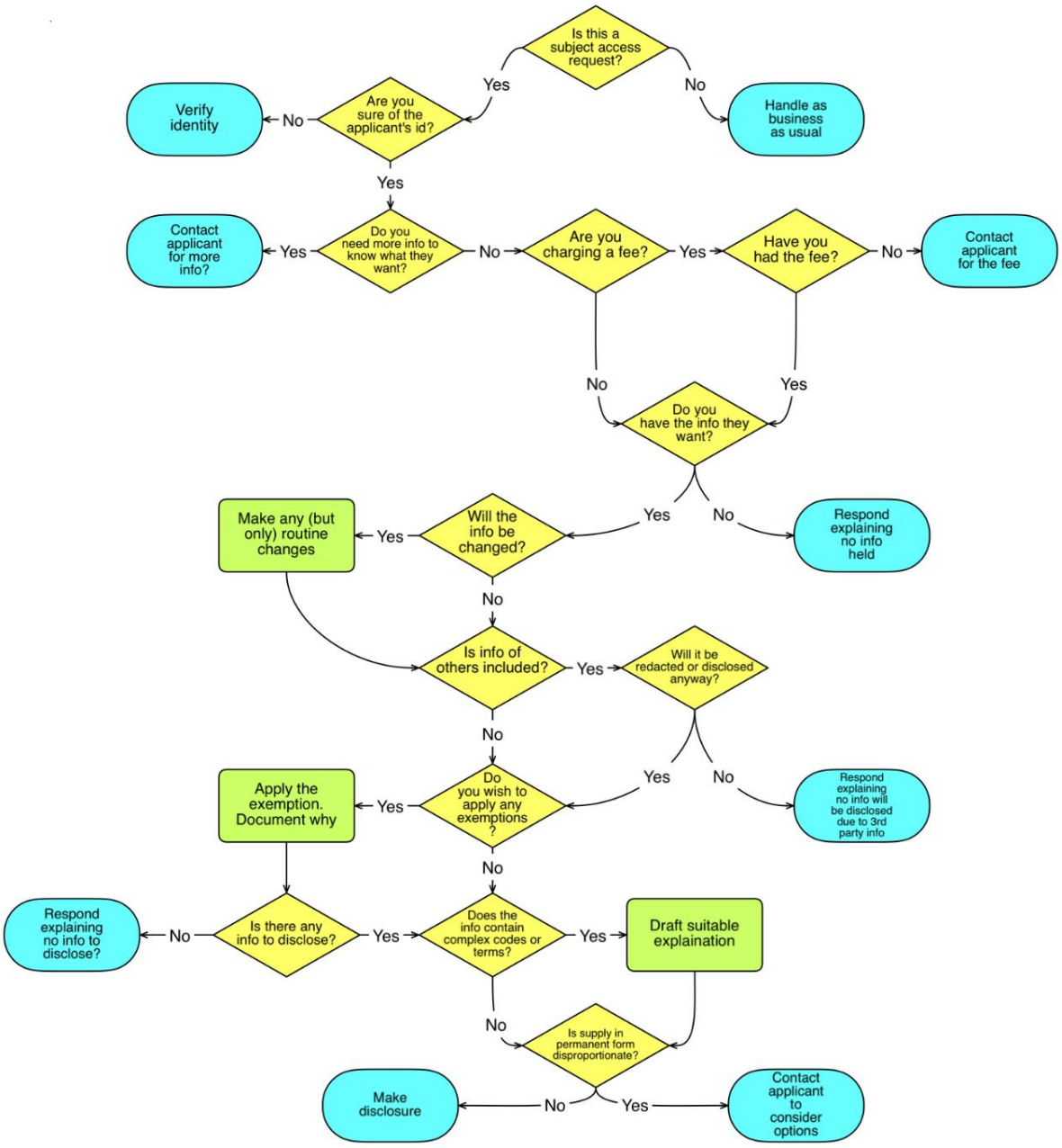
If you use a data processor, then you need to make sure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the data processor.

What about personal data held by credit reference agencies?

There are special provisions regulating access to personal data held by credit reference agencies. Where credit reference agencies hold personal data relevant to an individual's financial standing (information in a credit reference file), they must provide a copy of the information within seven days of a written request and on payment of a £2 fee. Credit reference

agencies will need to verify the identity of the person making the request before they respond.

Appendix 1 – Subject Access Process Flowchart



Appendix 2 – Bailiwick of Guernsey Only – Subject Access to Health Records

The Data Protection (Subject Access Modification) (Health) Order 2002 outlines alternative fees for access to health records. This is applicable only to the Bailiwick of Guernsey.

What is a 'health record'?

A 'health record' is defined in the Law as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.

The definition of a 'health record' could apply to material held on an X-ray or an MRI scan, for example. This means that whenever a subject access request is made, the information contained in such material must be supplied to the applicant within the fee structure described below.

It is clear, therefore, that records being held by the Hospital, the MSG, surgeries and other health care institutions will constitute 'health records' and will therefore fall within the scope of the subject access provisions of the Law.

Who is a 'health professional'?

Section 67(1) of the Law has been amended to define a "health professional" as:

> *"The States of Guernsey Board of Health and any person who practices … as a regulated health professional or uses any regulated title within the meaning of the Registered Health Professionals Ordinance, 2006"*

How much can be charged for granting subject access?

As from 24th June 2010 an amendment to the Law provides that the maximum amount that may be charged for subject access to health records is in accordance with the following scale:

> If the information is provided other than in writing on paper (e.g. electronically on a CD) - £50;
>
> If the information is provided in writing on paper the maximum fee is:
> - £10 for up to 10 pages;
> - £50 for up to 100 pages;
> - Thereafter, £0.50p per page.

It should be noted that there is no express provision for any additional fee to be charged for copying or despatching copies of records.

Contact the Commissioner

Enquiries and Publication Requests

Jersey

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org