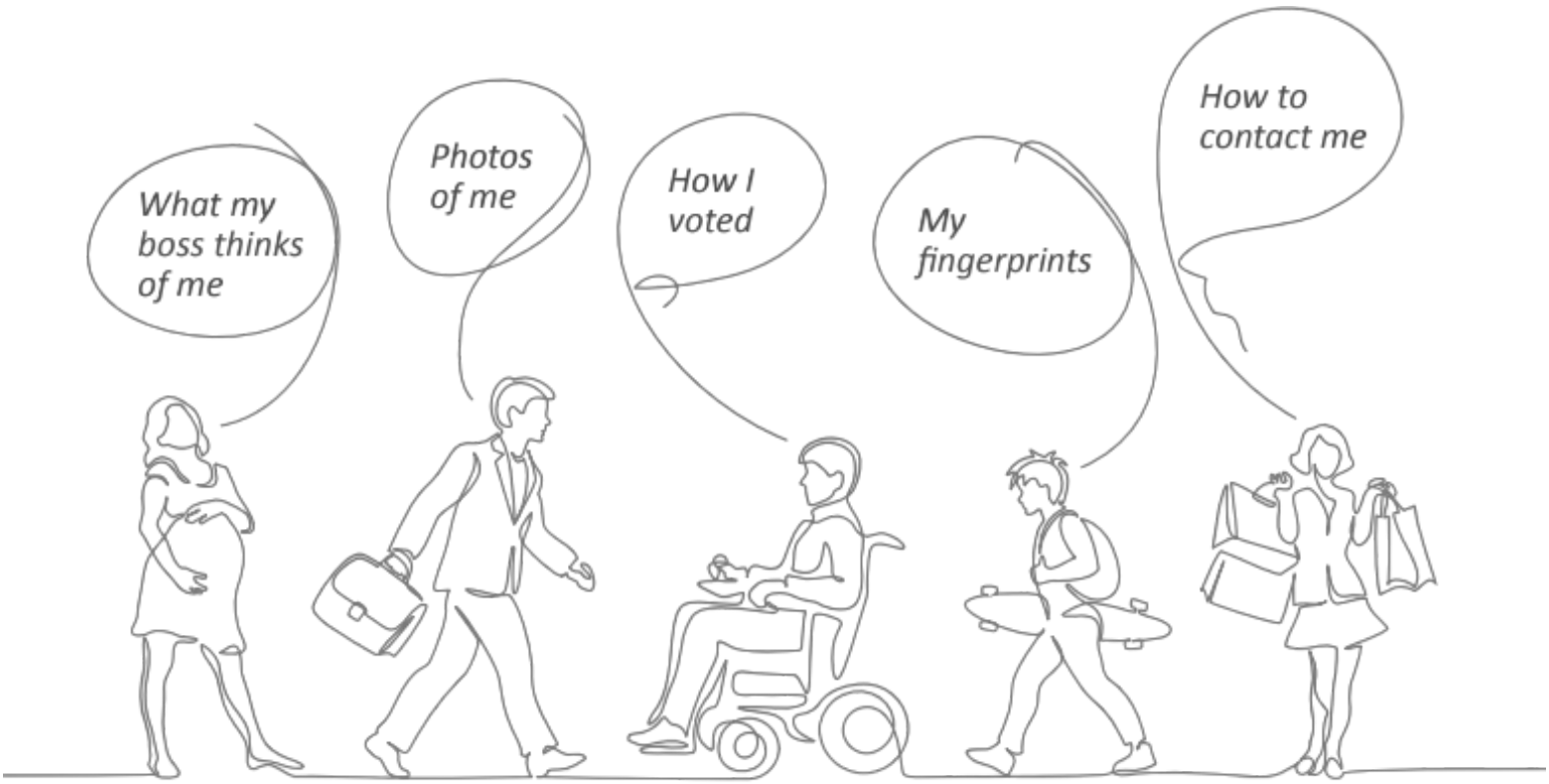
THE OFFICE OF THE
Data Protection
Authority

GUIDANCE: Subject Access Requests (for Data Subjects)



2023 issue

Guidance: Subject Access Requests
(guide for data subjects)

Introduction and Summary
You, and all other living human beings, are at the heart of data protection legislation.

You are referred to in the Law as a '**data subject'** (i.e. you are the subject of any given piece of personal data or information). *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('The Law') contains legal rights and responsibilities and specifically aims to strengthen individuals' rights.

One of the most commonly used right is the 'right of access' (also sometimes referred to as a 'subject access request' ('SAR') or 'data subject access request' ('DSAR').

In Plain English a DSAR is when you ask what information an organisation holds about you and why, so you are effectively asking:

- what do you **know** about me?
- what do you **think** about me?
- what do you **think you know** about me?
- what are you **doing** with it all?

In this guide you will find: more information specifically about DSARs, how to make one, what you should receive back, and what to do if you're not happy with what you receive.

Table of Contents

How can I find out if information is held about me?

If you want to know whether information or personal data is held about you and if so what, you will need to write to the person or organisation (also known within the Law as the controller or processor) you believe holds the information.

This is known as a 'right of access' request (also sometimes referred to as a 'subject access request' or 'data subject access request' ('DSAR')).

You can ask for a copy of all the information held about you to which the Law applies. This information may take any form (e.g. computerised, paper and archive records, CCTV footage, phone recordings, and images etc).

You can request this information in writing (letter or email), by phone or even over social media, however, we recommend that you send an email or a letter addressed to either the data protection officer ('DPO') or the data protection contact outlined in the organisation's data processing notice. If you are not sure who to write to within an organisation, address it to the Managing Director or equivalent.

It is a good idea to include your full name and address in the heading, together with any other information to assist in identifying you, for example the length of time you may have worked for the organisation, or a reference number quoted in correspondence with the organisation.

It will help the organisation if you can be as **specific as possible** about the information you require.

Some decisions are made by an automatic process (for example, by a computer system). If you want to be told of the logic involved in certain types of automated decisions which the organisation may take (for example, your performance at work or credit worthiness), you should mention this specifically.

It is best to send your DSAR by email or recorded delivery and to keep a copy of the letter and any further correspondence.

See **Appendix 1** below for an outline example of a letter which you can use, but you can use your own words if you choose.

How much does it cost to obtain the information?

Organisations are not permitted to charge a fee for responding to your DSAR **unless exceptional circumstances apply**. These exceptional circumstances include where they can demonstrate your request is:

- frivolous
- vexatious
- unnecessary
- repetitive

The **burden of proof rests with the organisation** to justify why they believe your DSAR meets these rare exceptions. That means the organisation needs to prove that the request is one of any of the above to charge you for its response; you do not need to prove to them that it is not any of those things.

Responding to your request

Organisations must respond to your DSAR within one month of the later of:

- the day they receive your request
- the day they receive any information reasonably necessary to confirm your identity
- the day any fee or charge payable under this Law is paid

Where a controller can demonstrate that your request is complex, this time limit may be extended by a further two months, however, the controller must notify you of their intention to extend the period as soon as possible (and definitely within the original one month) and explain the reasons for any extension.

The organisation can ask you for additional information (such as ID) to establish whether you are who you say you are, and that the personal data requested relates to you. 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 they must be **reasonable** about what ID they ask you for. They should not request lots more information if your identity is obvious to them. This is particularly the case, for example, when you have an ongoing relationship with the organisation (i.e., you are a former employee).

EXAMPLE:
You make a DSAR to your current employer. They know you personally and have even had a phone conversation with you about the request. Although the organisation's policy is to verify your identity by asking for a copy of photographic ID, it is likely to be unreasonable to do so in this case since they know it is you making the request.

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

EXAMPLE:
You make a DSAR request to an online retailer you have used to purchase goods on several occasions. You have not used the site for some time and although your email address matches the company's records, the postal address you have given does not. In this situation, it would be reasonable for the organisation to request further verifying information, such as your customer reference number, before they respond to your request.

The verification checks carried out by an organisation on your identity are likely to be greater where there is more possibility of harm or distress for an individual in the event of inappropriate disclosure of the information.

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

If I require an explanation as to how any automated decisions have been made about me, what must I do?

Organisations are required to outline whether any decisions about you are made based on automated processing of your personal data. Where this occurs, they must provide you with meaningful information about the logic involved, as well as the significance and the envisaged consequences of this processing.

Even though organisations are legally required to provide information to you about automated processing, we recommend you **specifically request** information about automated processing as part of your request.

What will be sent to me?

You are entitled to be told if any personal data is being processed about you and if it is, to be provided with a copy of all the personal data processed. Alongside this copy of your personal data the organisation is also required to give you information set out in Schedule 3 of the Law.

In summary, Schedule 3 requires information to be provided to you about:

- whether any of the personal data is 'special category data'
- the source of the personal data
- the legal basis of processing
- who has received the personal data
- if the personal data has been shared or is intended to be shared outside of an authorised jurisdiction
- how long the personal data will be retained for
- if any of the personal data is subject to automated processing.

The information must be given to you with any unintelligible terms explained.

- Where you request the information in writing, the organisation should send you a response as a computer printout, photocopy, in a letter or on a form unless the supply of such a copy is not possible, or you agree otherwise.
- Where you request the information electronically, the organisation should send you a response in a commonly used electronic format (unless otherwise requested or agreed by you).

Whilst it would be usual for the organisation to provide the requested information in permanent form, you may request information in alternative forms (e.g., verbal).

Can an organisation refuse to give me what I ask for?

An organisation can refuse to give you what you want if it believes that the request, or a part of your request, is:

- manifestly unfounded
- frivolous
- vexatious
- unnecessary
- repetitive

The **burden of proof rests with the organisation** to justify why they believe your DSAR meets these rare exceptions. That means the organisation needs to prove that the request is one of any of the above to refuse you the information; you do not need to prove to them that it is not any of those things.

In most cases you should be told why the information has been withheld. You should also be told you have the right to complain to the ODPA and the right to bring a civil action.

Is an organisation allowed to withhold any information?

There are circumstances where an organisation may find that complying with your DSAR means that information will be disclosed relating to another individual / individuals.

Unless that other individual / individuals consents to the disclosure of the information, or it is **reasonable** in all the circumstances to comply with the request without the consent of the other individual, the organisation is entitled to withhold the information from you.

There are other limited circumstances in which a controller may lawfully withhold information from you, these circumstances are set out in the Law, and are detailed in our exemption guidance. In most cases you should be told why the information has been withheld. You should also be told you have the right to complain to the ODPA and the right to bring a civil action.

What can I do if the Controller does not comply with my subject access request?

If the organisation fails to respond to your request within the time limit, or fails to respond to your satisfaction, and you have sent all the information required to enable them to deal with your request, you should send the organisation a reminder, keeping a copy of your letter.

If they still do not respond, we may be able to assist by chasing them for a response, where appropriate, and highlighting their legal responsibilities. Please read our 'Make a Complaint' page for further details.

If you are not satisfied with the response and you are able to:

- Provide us with **evidence of your concerns**, and

- Provide us with **evidence that you have sought to resolve this with the entity directly**

you can lodge a formal complaint with us.

The act of lodging a complaint enables us to consider conducting an investigation under Section 68 of the Law, using the powers provided to us by the Law where needed.

Need further help?

If you need further clarity on this area, please Contact Us.

Appendix 1 – Example DSAR Letter

Please tailor this template to your needs by amending/removing the red text as appropriate.

Your name
Your address

Date

Company name

Company address

Dear addressee / sir/ madam

Please provide me with information which I am entitled to under Section 15 of *The Data Protection (Bailiwick of Guernsey) Law, 2017* [in relation to [give details of any specific information you require]] within the designated period of 1 month from the date of this request.

[Please would you also advise me of the logic involved in any automated decisions taken by you about me pursuant to Section 24 of *The Data Protection (Bailiwick of Guernsey) Law,2017*.]

[I have included XXXX by way of Identification confirmation]

If you need further information from me, please let me know as soon as possible. If you do not normally handle these requests for your organisation, please pass this letter to your Data Protection Officer or another appropriate officer.

Yours faithfully

Signature

Appendix 2 - Schedule 3 of the Law

INFORMATION TO BE GIVEN TO DATA SUBJECTS

1. The identity and contact details of the controller and, where applicable, any controller's representative.

2. The contact details of the data protection officer, where applicable.

3. Whether any of the personal data is special category data.

4. If any of the personal data has not been collected from the data subject by either of the controller or a processor acting on the controller's behalf – (a) the source of the personal data, and (b) if applicable, whether the personal data was obtained from a publicly available source.

5. The purposes and the legal basis of the processing.

6. Where the lawfulness of processing is based on the processing being necessary for the legitimate interests of the controller or a third party, the legitimate interests concerned.

7. The recipients or categories of recipients of the personal data, if any.

8. If the controller intends to transfer the personal data to a recipient in an authorised jurisdiction, other than [the Bailiwick or] a Member State of the European Union, a statement of which of the following applies to that authorised jurisdiction – (a) an adequacy decision is in force in respect of the authorised jurisdiction, or (b) the authorised jurisdiction is a designated jurisdiction.

9. If the controller intends to transfer the personal data to a recipient in an unauthorised jurisdiction, reference to the appropriate or suitable safeguards applying to the transfer and the means to obtain a copy of them or where they have been published or otherwise made available.

10. The period for which the personal data is expected to be stored, or if that is not possible, the criteria used to determine that period.

11. The data subject rights under sections 14 to 24.

12. Where the lawfulness of processing is based on the consent (explicit or otherwise) of the data subject, the existence of the right to withdraw consent at any time (without affecting the lawfulness of processing based on consent before its withdrawal).

13. The right to complain to the Authority under section 67[…].

14. Whether any decision would be made based on automated processing of the personal data, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.