THE OFFICE OF THE
Data Protection
Authority

GUIDANCE:
Data Subject Access Requests (for Controllers)

2024 issue

Data Subject Access Requests: A Guide for Controllers

Introduction

Individuals (or 'data subjects' as the Law defines them) are at the heart of data protection legislation. *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 rights is the right of access (also sometimes referred to as a 'subject access request' (SAR), or 'data subject access request' ('DSAR').

This guidance note is to help organisations and other parties processing DSARs to meet the Law's requirements.

In addition to this guidance note, you might also like to watch this Webinar: How to respond to 'subject access requests'.

Table of Contents

Overview

The Law entitles individuals to ask *what personal data a controller holds about them and why* by submitting a **'right of access'** or '**data subject access request**' ('DSAR').

In plain English, a DSAR is when an individual asks you:

- 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 this information?

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

Under a DSAR, an individual is **only** entitled 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). It is important to establish whether the information requested falls within the definition of personal data.

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

You must respond to DSAR requests **within one month**, although this can be extended if the request is complex.

In most cases you cannot request a fee for supplying this information to an individual.

The Law provides for certain, limited and specific exemptions to this right, as it does for most rights.

Data Subject Access Request: Process Overview

To give you a broad overview, there are four aspects to dealing with a DSAR:

1. Acknowledging the request
2. Gathering the information about the person
3. Assessing and reviewing the information gathered
4. Giving the information to the person

The process form and accompanying guidance notes below guides you through each of these four aspects.

Data Subject Access Request: Process Form

To walk step by step through the process for responding to a data subject access request please refer to the **Data Subject Access Request: Process Form** – the form must be read alongside the guidance notes below.

This form asks you a series of yes/no questions to guide you through the process of responding to someone making a request to access information you hold about them (the legal term for this is a 'Data Subject Access Request' or DSAR for short).

How to use this Process Form:

Where there are bracketed numbers in the questions and answers [e.g. **(see note 8)**] this is pointing you to where you can find more information in the indicated numbered section in the guidance notes that start on page 8 of this document.

Depending on whether you answer yes/no to each question, you will be directed to:

- continue to the next question, or
- take certain action, then continue to the next question, or
- take certain action, and then you will be informed that you are at an endpoint and do not need to proceed further.

QUESTION 1: Is this a Data Subject Access Request (DSAR)? (see note 1)	
Yes	Log the request in internal DSAR register, and acknowledge receipt (see note 2) **CONTINUE to next question.**
No	Handle as business as usual. **ENDPOINT: You do not need to continue further in this form.**
QUESTION 2: Is the request valid? (see note 3)	
Yes	**CONTINUE to next question.**
No	Notify the requestor that the request is not valid explaining why so the requestor can try again if they want to. **ENDPOINT: You do not need to continue further in this form.**
QUESTION 3: Is the request manifestly unfounded, frivolous, vexatious, unnecessarily repetitive, or otherwise excessive? (see note 4)	
Yes	Notify the requestor that the request will not be processed and why. See note 4 for detail on what you must include in your response. ***Alternatively*** you can choose to provide the information for a reasonable fee (with the exception of manifestly unfounded requests - which you can simply turn down as long as you explain why). Document the reasoning for your decision. **ENDPOINT: You do not need to continue further in this form.**
No	**CONTINUE to next question.**
QUESTION 4: Can you charge a fee? (see note 5)	
Yes	Check that one of the exceptional circumstances that allows for a fee to be charged have been met. **CONTINUE to next question.**
No	**CONTINUE to next question.**
QUESTION 5: Is the request for information about a child? (see note 6)	
Yes	Ensure additional guidance considered (see note 6). **Then CONTINUE to next question.**
No	**CONTINUE to next question.**
QUESTION 6: Are you sure of the applicant's identity? (see note 7)	
Yes	**CONTINUE to next question.**
No	Verify identity (see note 7). **Then CONTINUE to next question.**
QUESTION 7: Do you need more information to know what the requestor wants/needs? (see note 8)	
Yes	Contact individual for more information. **Then CONTINUE to next question.**
No	**CONTINUE to next question.**

QUESTION 8: Are you confident that only routine changes will be made to the information while processing the request? (see note 9)	
Yes	Carry out a comprehensive search for the information requested including contacting any processors you engage **(see note 10). Then CONTINUE to next question.**
No	Enact safeguards to ensure that only routine changes are made **(see note 9).** Then carry out a comprehensive search for the information requested including engaging with any processors you engage **(see note 10). Then CONTINUE to next question.**
QUESTION 9: Is the request complex? (see note 11)	
Yes	If you can justify an extension to the one month response period **(see note 11)** you must notify the requestor explaining additional time needed and reason for extension. **Then CONTINUE to next question.**
No	**(see note 11)** remember you have one month to respond to a valid request. **Then CONTINUE to next question.**
QUESTION 10: Do you have the information the person is requesting?	
Yes	First you need to check whether there is any other people's personal data included with the requested data **(see note 12). Then CONTINUE to next question.**
No	respond explaining you do not hold requested data. **ENDPOINT: You do not need to continue further in this form.**
QUESTION 11: Where there is other people's data included, is it possible to redact their information without detracting from the context of the information? (see note 12)	
Yes	Apply redaction as necessary. **CONTINUE to next question.**
No	You should perform a 'balancing test' to weigh up whether the requestor's right of access is more important than the other person's rights. **CONTINUE to next question.**
QUESTION 12: After having performed your balancing test, is there some information you can send the requestor? (see note 12)	
Yes	**CONTINUE to next question.**
No	respond to the person explaining you are unable to disclose due to there being other people's data involved. **ENDPOINT: You do not need to continue further in this form.**
QUESTION 13: Do you wish to apply any exemptions? (see note 13)	
Yes	Review **note 13**, apply exemptions as appropriate, and keep an internal record of your reasons for using them. **Then CONTINUE to next question.**
No	**CONTINUE to next question.**

QUESTION 14: After applying any exemptions that may be appropriate, is there any information left to disclose?	
Yes	Remember to include in your response any exemptions you have used and why they apply. Then **CONTINUE to next question.**
No	Respond explaining that you are not providing information on the basis of exemptions under the Law, you **should usually outline which exemptions you think apply**, but see note 13 for the limited circumstances when you would not. **ENDPOINT: You do not need to continue further in this form.**
QUESTION 15: Have you collated all the information required by Schedule 3 of the Law? (see note 14)	
Yes	**CONTINUE to next question**.
No	Collate the data required by Schedule 3. **Then CONTINUE to next question.**
QUESTION 16: Is the content you are intending to send to the requestor understandable? (see note 15)	
Yes	Provide one copy of the requested data along with the information required by Schedule 3, **ENDPOINT: You do not need to continue further in this form.**
No	Prepare additional guidance to help the person to understand what you are sending them. Then provide the guidance along with one copy of the requested data, and the information required by Schedule 3. **ENDPOINT: You do not need to continue further in this form.**

Data Subject Access Request Process Form: Guidance Notes

To guide you through the DSAR process form above please refer to the following explanatory information, the numbering relates to the numbers listed in the form.

Note 1: Is the request a DSAR?

It is important to be able to recognise a request made as part of your usual business operations and a request made under the Law. If in doubt, you should clarify the basis of the request with the individual prior to proceeding. In either case, ensure you acknowledge receipt of the request.

Example:

One of your employees asks for a copy of their employment contract to be sent to them asap. This is likely to be a 'business as usual' request and should be dealt with following your usual process.

Example:

On leaving the firm, an employee asks for one copy of **'all the personal data that you hold about me'** to be sent to them within one month. This is likely to be a DSAR and should be processed in accordance with the Law.

Note 2: Log the request in internal DSAR register

We recommend that you keep a record of all DSARs so you can easily demonstrate compliance with the Law. These records may include:

- The name of the requestor
- The information requested
- The date the request was received
- A record of all decisions made in respect to the DSAR
- A record of all communications made with the requestor

Note 3: Is the request valid?

It is important that you ensure that any DSAR request you receive is valid. You should note the following points when considering a DSAR's validity:

- Are you confident that the person making the request is who they say they are? Or do you need to verify their identity (see note 7 below)?

- Is the person making the request a child? If so, you will need to apply additional considerations (see note 6 below) before proceeding.

- A DSAR can be made verbally or in writing (including through social media). It is therefore important to ensure that you train all your employees to **identify and escalate** DSARs to your data protection lead as soon as possible.

- The requestor does not need to quote 'Section 15 of the Law', use the term 'data subject request', 'rights request', 'GDPR' or 'the Law' for the request to be valid. If a DSAR 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 making a request 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** your staff can recognise a DSAR and treat it appropriately.

- Requests can be made by the individual or by a third party on another individual's behalf. Where a third party is used, it is important to confirm with the individual that the third party has authority to act on their behalf. 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 DSAR 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 having had the opportunity to review it.

- If you can demonstrate that the DSAR is **manifestly unfounded, frivolous, vexatious, unnecessarily repetitive, or otherwise excessive**, you may refuse to give the information or take the action requested in that part of the request. You bear the burden of proof to show that this is the case and should ensure decisions are appropriately documented.

- You may produce a DSAR request form, 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 DSAR and make it easier for the individual to include all the details you might need to locate the information they want, but an individual does not have to use one if they would rather make their request another way.

Note 4: Is any part of the request manifestly unfounded, frivolous, vexatious, unnecessarily repetitive, or otherwise excessive?

If you receive a request that you believe is **manifestly unfounded**, you must be able to demonstrate that and you may refuse to give the information in that part of the request.

The Law does not limit the number of requests an individual can make to you. However, it does allow some discretion when dealing with requests that are **unnecessarily repetitive** as follows:

- You may refuse to give the information in that part of the request
- You may, in exceptional circumstances, give the information but charge a reasonable fee for the administrative costs incurred

When considering if a request is **unnecessarily repetitive**, you should, consider the following:

- the *nature* of the personal 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 personal 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 within a short period of time.

If there has been a previous request or requests, and the information has been added to or amended since then, when you do respond to the new request, you must ensure that you provide a **full response to the request**: not merely providing information that is new or has been amended since the last request.

Example

A library receives a DSAR 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 harm if no personal data is sent in response to the request, the library made a decision not to comply with this request as they can evidence that it is 'repetitive'.
Note: it would be good practice for the library to respond explaining why they have not provided the information again.

In practice we would accept that you may attempt to negotiate with the requester in order to restrict the scope of their 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 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.

Where you believe the request is **frivolous, vexatious, or otherwise excessive** it is your responsibility to bear the burden of proof to demonstrate that it is. In these instances, you may:

- refuse to give the information or take any action requested in that part of the request
- in exceptional circumstances, give the relevant information or take the relevant action but charge a reasonable fee for the administrative costs of so doing

If you are not giving everything the requestor is asking for you need to **tell them why** (except in very limited circumstances where you cannot tell them why because this would prejudice the reason you

are withholding it for – for example: you would not tell them that they are under investigation by a law enforcement body as this would be tipping them off). As part of your response to them you must tell them that they can complain to the ODPA or take civil action through the Court.

Note 5: Can we charge a fee for dealing with a DSAR?

No – you are not permitted to charge a fee for processing a DSAR except in exceptional circumstances. These exceptional circumstances include where you can demonstrate the request is:

- frivolous
- vexatious
- unnecessarily repetitive
- otherwise excessive

Remember, the burden of proof rests with you to justify why the DSARs meet these rare exceptions.

The only other circumstance where you may charge a reasonable fee is if an individual asks for 'further copies' of personal data (beyond the one copy they are entitled to).

You should let the person know about the fee and how much it is before you do the work.

Note 6: Is the request for information about a child?

In the Law, there is no definition or clarification about children in respect to DSARs. In the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a DSAR 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 can understand (in broad terms) what it means to make a DSAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should consider, 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/guardians should have access to information about them.

There is a specific exemption that relates to requests made by persons with parental responsibilities for a child, or court-appointed administrators. Please refer to our Exemptions Guidance for more information.

Note 7: What verification of identity is required?

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 DSAR 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.

Example

An online retailer receives a DSAR 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 responding to the request.

The level of checks you should make should 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 DSAR 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.

Note 8: Can we ask for more information before responding to a DSAR?

Before responding to a DSAR, if the request is vague or has a very broad scope (such as a request for "one copy of all personal data you process") we would recommend that you consider engaging with the requestor to clarify whether there is something specific they need as this may enable you to narrow the scope. However, the requestor is under no obligation to provide this clarification so you should ensure that, where the scope is not clarified, a full response is provided within the designated period.

Note 9: Enact safeguards to ensure that only routine changes are made

The Law specifies that a DSAR relates to the personal data held at the time the request was received. However, in many cases, routine use of the personal 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 personal data if you would not otherwise have done so or to delay responding to ensure the personal data are amended or deleted.

Example

You are a high street bank and receive a DSAR dated 15 June. Between 15 June and 30 June, when you respond, the balance on the current account of the requestor changes due to routine fees and transaction. It would be appropriate to send the balance at 30 June in this instance.

Example

You review your records as part of your DSAR response process and note some unfavorable emails from the requestor's line manager about the requestor's behaviour. You are not permitted to delete this personal data to avoid sending to the requestor.

Note 10: Carry out a comprehensive search for the information requested

You must carry out a comprehensive review to ensure that all personal data that you process about the requestor is located. This includes reviewing:

- All paper records
- All electronic records (including emails, cloud systems, and deleted items)
- All filing systems
- All archive records
- All workplace messaging systems and devices

You must also ensure that any data held by any processors you use is searched and included in your response.

Example

An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party processor is analysing the information.

The employer receives a DSAR from a member of staff. To respond, the employer needs information held by the processor. The employer is the controller for this information and should instruct the processor to retrieve any personal data that relates to the member of staff.

In some cases, dealing with a DSAR 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 certain information is held. The better your data governance standards are, the more straightforward such requests are likely to be.

The Law does not allow any extension to the time limit in cases where you have to rely on a processor to provide the information that you need to respond. If you use a processor, then the Law requires you to have contractual arrangements in place to ensure data protection obligations are met, including that DSARs are dealt with properly, irrespective of whether they are sent to you or to the data processor.

Note 11: How long do I have to respond to a DSAR?

You must respond to DSAR requests **within one month** of the latest of:

- the day you receive the request
- the day on which you receive any information reasonably necessary to confirm the identity of the requestor
- the day on which any fee or charge payable under the Law is paid

Where you receive a complex request, this time limit may be extended by a further two months. But you must tell the person making the request that you are using this extension as soon as possible and you must also be able to justify why you need the extra time (note: the complexity of your own systems is not a valid reason).

You should ensure that all decision-making is appropriately documented.

Note 12: What should we do if the data includes information about other people?

Data you hold about the individual making the request may involve information that relates to another individual or individuals.

Although you may sometimes be able to disclose information relating to another individual, you need to decide whether it is reasonable to do so in each case. This decision will involve comparing the data subject's right of access with the other individual's rights in respect of their own personal data.

If the other individual consents to you disclosing the information about them, then you are free to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

The Law includes some provisions for circumstances where you do not feel able to comply with a DSAR without disclosing information relating to another identified or identifiable individual. These provisions include the ability for you to refuse to respond to a request where it is reasonable to protect the significant interests of the other individual.

To determine if it is reasonable to refuse the request, you should consider the following (known as a 'balancing test'):

- if the other individual has **consented or expressly refused consent** to the disclosure
- the ability for the other individual to be able to give **informed consent**
- the type of personal data involved (remembering that the Law dictates that you should take extra care with special category data)
- the significant interests at stake in the disclosure / non-disclosure of the information for the requestor, and the other individual
- the reasonable expectations of **each individual** in relation to the disclosure of that information
- the persons to which, and the circumstances in which, the disclosure is to be made
- if storage of that information is or may be involved following disclosure, the period for which that information is or may be stored
- the existence of appropriate safeguards for the protection of that information, once disclosed
- the possible consequences for **each individual** of disclosure of that information.

If you decide to disclose the information you should inform the other individual and clarify the basis for the decision.

If you are not giving everything the requestor is asking for you need to **tell them why** (except in very limited circumstances where you cannot tell them why because this would prejudice the reason you are withholding it for – for example: you would not tell them that they are under investigation by a law enforcement body as this would be tipping them off). As part of your response to them you must tell them that they can complain to the ODPA or take civil action through the Court.

Note 13: Do you wish to apply any exemptions?

The Law provides for certain, limited and specific exemptions to this right, as it does for most rights. Ensure you read and understand this guidance on exemptions before proceeding, and keep an internal record of any that apply to the DSAR in question and why you are using them.

If you are not giving everything the requestor is asking for you need to **tell them why** (except in very limited circumstances where you cannot tell them why because this would prejudice the reason you are withholding it for – for example: you would not tell them that they are under investigation by a law enforcement body as this would be tipping them off). As part of your response to them you must tell them that they can complain to the ODPA or take civil action through the Court.

Note 14: Have you collated all the information required by Schedule 3 of the Law

In addition to providing one copy of all the personal data processed, you are also required to provide the information listed in Schedule 3 of the Law.

When responding to a Data Subject Access Request, this information must be specific to the information that has been processed as per appendix 2, unless there is an applicable exemption or exception such as the exception to the right of access involving disclosure of another individual's personal data (see section 16 guidance).

In accordance with the section 16 guidance, where information has been shared with a senior member of staff or decision maker, it is expected that the name of the senior member of staff or decision maker is provided unless doing so poses a significant risk.

In summary, an individual is entitled to be:

- told **whether** any personal data is being processed
- provided with **one copy of the data** being processed
- provided with the information listed in Appendix 2

Note 15: 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.

If you are not giving everything the requestor is asking for you need to **tell them why** (except in very limited circumstances where you cannot tell them why because this would prejudice the reason you are withholding it for – for example: you would not tell them that they are under investigation by a law enforcement body as this would be tipping them off). As part of your response to them you must tell them that they can complain to the ODPA or take civil action through the Court.

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".

Need further help?

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

Example

You receive a DSAR 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, as best you can.

Appendix 1 - Glossary

Authorised jurisdiction	• The Bailiwick of Guernsey • A Member State of the European Union • Any country, any sector within a country, or any international organisation that the (European) Commission has determined ensures an adequate level of protection within the meaning of Article 45(2) of the GDPR and for which the determination is still in force. • A designated jurisdiction (by Ordinance)
Child /children	An individual under 18 years of age. Visit our children and young people area for more information.
Controller	A person (individual or legal) that, alone or jointly with others, determines the purposes and means of the processing of any personal data.
Data subject	A 'data subject' is the **person** who is identified (or identifiable) by personal data. So you, me, your family and friends are referred to as 'data subjects' when our personal data is being used by a organisation/entity.
Data subject rights	Means a legal right a person* has under our Law. Please see Your Rights for more detail.
Identifiable individual / Individual	An individual is identifiable from any information where the individual can be directly or indirectly identified from the information, including – by reference to a name or an identifier by reference to one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity, where, despite pseudonymisation, that information is capable of being attributed to that individual by the use of additional information, or by any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing.
One month	The Law requires controllers to comply with a request to exercise data subject rights within the designated period which is specified as one month. *The Interpretation and Standards Provisions (Bailiwick of Guernsey) Law, 2016* provides that one month shall mean **calendar month**.
Personal data	'Personal data' has a very broad legal definition, it is: '*any information relating to an identified or identifiable [living] individual*'. The scope of what is considered 'personal data' expands even further when you consider that it includes both **factual** information about people as well as **opinions** expressed about people. It also includes anonymised data that could identify people if it was combined with other information. NOTE: personal data does **not** include: any data about a **deceased person**; any information, facts or opinions **that do not relate to, or**

	identify people (e.g. employment statistics, or anything else that has been irreversibly anonymised)
Processing	The legal definition of 'processing' is very broad: '*Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means*.' In plain English, 'processing' can be summed up as: **anything you do with personal data**. Some examples of processing *include*: Collection; Recording; Organisation; Structuring; Storage; Alteration; Retrieval; Consultation; Use; Disclosure; Dissemination; Restriction; Erasure; Destruction.
Processor	An individual or other person that processes personal data on behalf of a controller. This definition also includes 'secondary processors' (another processor engaged by the 'primary processor').
Significant interests	A person's 'significant interests' are defined in the local Law as any aspect of their life that could be put at risk due to their personal -data being breached. This could include their physical safety, reputation, a risk of identity theft, fraud, financial loss, psychological distress or humiliation.
Special Category Data	Personal data revealing an individual's racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, data concerning an individual's sex life or orientation, criminal data.

Appendix 2 - Schedule 3 of the Law

*Note: For points 4, 7, 8 and 9 listed below, you should **tailor the information to be relevant** for the requestor of the DSAR. This means, where appropriate and proportionate, listing the **specific sources of the personal data**, the **specific recipients of the requestor's information**, and the **countries their information has been transferred to**, as well as the more general information usually listed in your data processing notice.*

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.