

Handling Subject Access Requests

What is a subject access request?

The Data Protection (Jersey) Law 2018 provides individuals with rights over their personal data.

More specifically, the Law provides individuals with a right to access to personal data which is processed about them by a data controller, such as the States of Jersey. Individuals are entitled to be informed:

- whether their personal data is being processed by the SOJ (or on the SOJ's behalf)
- the purposes for which they are being or are to be processed by or on behalf of that controller;
- the categories of personal data concerned
- the recipients or classes of recipients to whom they are or may be disclosed
- how long that data is likely to be retained
- where the data was collected from if not from them
- about any automated decision making about their personal data and the rationale behind it
- about safeguards in place where data is transferred to a third country (this usually means outside Europe) or international organisation

Individuals also have rights to:

- lodge a complaint with the Data Protection Authority
- request rectification, erasure, restriction of processing (under certain circumstances)
- object to processing on the basis of direct marketing, legitimate interest or public function
- request for their data to be provided in a structured machine readable format in order to transmit to another data controller (portability)

Crucially, individuals can also ask, free of charge, for a copy of personal data processed about them by SOJ and this must be (with some exceptions) provided within 4 weeks.

This right of access includes both electronic records and paper records.

How has the law changed since 2005?

The right to subject access already existed under the Data Protection (Jersey) Law 2005, however there are some important changes under the new Law.

- A fee can no longer be charged

- The time for responding to a request reduces from 40 days to 4 weeks (with an 8 week extension in exceptional circumstances detailed below)

Catalyst for improved customer service

This change has created a catalyst for rationalising and centralising the SAR process across the SOJ, following the FOI model. By making this information available in a timely and consistent manner, the SOJ will demonstrate transparency, efficiency and responsiveness to our customers.

Improvements will include:

- a 'one stop shop' portal for customers when they engage with Government
- reduction in duplication of effort, as SARs often cover several departments
- increase in accuracy and professionalism, as redaction and exemptions will be applied in a consistent way across all information
- reduction in delays due to lack of awareness and communication
- reduction in potential breaches and complaints
- increase in the quality of data
- unprecedented access to statistics and measurements about SARs made to the SOJ
- the ability to make a SAR online via a central portal (the option of applying directly to departments will still exist but those requests will be directed to the central unit).
- the identification of SAR Points of Contact for every department
- the creation of a full time role of an Information Governance Officer to handle SARs and SAR related issues

How to recognise a SAR

A SAR can be made in writing to an employee of the States. A SAR could take the form of a letter, an email or even a social media post. The request does not need to quote the Law or be made to a specific person- it simply needs to be a request from an individual for their personal information.

It is important therefore that every staff member across the States, can recognize a SAR and take the appropriate action which would be to alert their SAR POC or to direct the individual to the central SAR portal which is available at:

<https://www.gov.je/Government/dataprotection/Pages/SubjectAccessRequest.aspx>

Where the individual will be required to complete a form. The exception to this is requests for SoJ police information. This should be requested directly from the Police. However, the SoJ Police will inform the Central Data Protection Unit when they receive a request and when it was fulfilled so that the central statistics can be completed.

The role of the SAR Points of contact

Each department has appointed a SAR point of contact (SAR POC).

The SAR POC will be responsible for:

- fulfilling all SARs received from the Central Data Protection Unit, in collaboration with relevant officers within their department. This will include sourcing the information, applying relevant exemptions and redactions.
- liaising with their department's Data Protection Officer (if there is one) and with the Corporate SAR Manager in order to ensure that the SAR is responded to in a timely and accurate manner.
- providing best practice guidance to members of staff within their department
- liaising with the Corporate SAR Manager regarding exemptions, redactions, time extensions and any other issues
- completing any relevant training as directed

If a SAR is received directly to the department in question, rather than via the central SAR portal, then the SAR POC **must** contact the central Information Governance Officer via sar@gov.je at the earliest opportunity so that the request can be verified, recorded and tracked corporately.

Each department (represented by the SAR POC) will be responsible for sourcing and supplying data they control. They will also be responsible for applying any redactions or exemptions although the Corporate SAR Manager and the Corporate Data Protection Officer can advise on more complex cases. Advice from the Law Officers' Department will also be available.

The role of the corporate information governance officer

The Corporate Information Governance Officer will:

- receive and disseminate SAR requests from the public, whether it is via the central portal or via a departmental referral
- verify the identity of the requester at the point of both initial request and release of the information
- keep track of the time remaining to respond and ensure a timely response
- record requests and collate statistics
- provide advice and guidance in relation to redaction, exemptions, information sourcing and other matters in relation to responding to a SAR and other subject access rights or issues
- oversee the release the information to the requester by their preferred method, ensuring that their identity is verified.

Exemptions and redactions

The right for an individual to a copy of their own information is not an absolute right and is subject to various exemptions. Therefore many SAR releases will contain redactions. The most obvious reason for redaction is to remove details about other people. Another reason might be that the information is subject to an ongoing court case.

Each SAR POC will be responsible for applying their own redactions and exemptions. However, in more complex cases, the central Information Governance Officer will assist and where there is contention around exemptions, the CDPO, with advice from the LOD, will make the final decision.

Deadline to respond and time extensions

SOJ has 4 weeks to respond to a SAR. If the request is complex, or there are a large number of requests of a similar nature, the Law states there can be an extension of up to 8 weeks. However this extension can only be granted at the discretion of the Corporate SAR Manager, and the requester must be informed at the earliest opportunity about the delay.

Releasing the SAR

With the exception of Police information, the completed SAR will be released by the Corporate Data Protection Unit, who will be responsible for verifying the identity of the requester or the person authorised to collect the information.

Save for the below, in most cases the central Data Protection Unit will release the information directly to the individual but they will not be party to the contents of the release.

The individual must collect the information:

- in hard copy in person, and present photographic ID and sign for the package. A proxy can collect if they have a signed letter of authority and photographic id.
- by recorded post at an address specified by the requester
- by encrypted email at an address specified by the requester. The password will be supplied by phone call by the Department who controls the information.

If the individual is not on Island then the information must be sent securely by registered post (or courier where it is very sensitive) to a verified address.

If it is considered necessary by an appropriate medical practitioner, arrangements (via the central data protection unit) will be made for the information to be provided to the individual whilst accompanied by a social worker. Similarly, if the records are to be supplied to a minor, it may be considered necessary, after consultation with relevant professionals, for the information to be released in the presence of an education professional or social worker.

The department/s in question should also retain a copy of the information released.

Can you make a SAR for another person's information?

In most cases, it is not possible to make a request for someone else's information. A lawyer or someone else can make a request by proxy, but a valid and signed letter of authority would be required. If the child is 12 or under, someone with parental responsibility can make a request on their behalf, but there are various checks to make.

The Corporate SAR Manager is responsible for assisting with more complex requests and can help SAR POCS to verify the identity and rights of the requester.

SARS and FOI – the difference

It is common for people to become confused between the difference between SARS and FOI requests. The centralised SAR process aims to reduce this confusion thus improving customer service.

FOI covers information held by public authorities, but not requests for personal information about the person making the request. FOI is about providing access to public information, while data protection legislation provides the right to access personal data.

The Corporate Information Governance Officer will liaise with the FOI manager to ensure that customer's requests are routed through the correct process.

SARs and complaints

It is common for complaints to include or be concurrent with a SAR however historically, these processes have not been joined up.

As the complaints process is also now centralized, the Corporate SAR Manager will liaise with the Complaints Manager in order to avoid duplication and delay, thus improving the customer experience and reducing dissatisfaction.

Further information

You can find further information at <https://www.gov.je/Government/dataprotection/Pages/SubjectAccessRequest.aspx> or by contacting dataprotection2018@gov.je