Subject Access Request (SAR) Guide

A Subject Access Request (SAR) is one of a series of legal rights, provided under General Data Protection Regulation that enables data subjects (individuals) to get confirmation as to whether or not personal data concerning him or her is being processed and, where it is, access to a copy of the personal data. The data controller (for example, the parish) has an obligation to make this personal data available on request (with a small number of exemptions). The request comes in the form of a Subject Access Request.

The Parish must respond, **in full**, to a Subject Access Request (SAR) within **one calendar month** of receiving it.

Preparing for a Request

Start preparing for a SAR by:

- Informing those in charge of data protection for the Parish what a SAR is
- Developing a procedure outlining how the Parish will respond to a SAR when one arrives
- Developing a SAR request form[1] for applicants to complete. This form should ask the applicant to set out the parameters for their request. Often, the applicant is only looking for specific information collected within a certain time period.
- Undertaking a data audit of all personal information processed by Parish and on behalf of the Parish. The Parish should know what data is held, where it is held, why it is held, who it is shared with, how long it is kept and when the information is archived or deleted.
- Archiving or delete personal information that is no longer required
- Ensuring all remaining personal data is kept safe and secure

Responding to a Request

1. Acknowledge and Verify

A SAR request can be made in writing, verbally, via social media or other interactive platforms. They are all valid requests and must be responded to following the same process.

When a SAR arrives:

- Contact the data protection representative for the Parish and plan the response
- Calculate a target response date [2]
- Send an acknowledgement to the individual and ask them to:
  - Complete and return the SAR request form (they are **not** obliged to do this)
  - Provide verification of their identity (The Parish **must be** satisfied of the identity of the individual. Certified copy of a passport or drivers licence or via phone where questions are asked based on information the Parish holds about them).
- Keep details of the applicant as confidential as possible

> The clock is ticking: once the SAR is received, the Parish has one calendar month to respond in full to the request. Even if ID is slow being verified, or the applicant doesn't return the form, the Parish still needs to identify, assess, gather and be ready to respond by the due date.
> **NEVER** share any personal information, regardless of timeframe, if ID is not verified.

[1] There is a template available on the Parish Resource section of the Church of Ireland website
[2] The controller is legally required to respond to a SAR in full within one calendar month. E.g. 25th April – response due by 25th May. This timeframe can be extended by two months in exceptional circumstances.

2. Identify the personal data held on applicant

The Parish needs to identify all the personal data concerning the applicant. Personal data may be contained in hard documents, emails, text messages, WhatsApp, social media, online information, archives and CCTV (if required). All has to be collated as part of the SAR (unless the parameters of the request have been narrowed by the applicant).

a) Check computer files, paper files, all social media, phone messages (both employees and volunteers), CCTV footage and any other places where personal information may be held
b) Contact anyone who might process personal data on behalf of the Parish e.g. Clergy, Treasurer, Administrator, safeguarding panel, select vestry, all employees, contractors and volunteers and ensure they identify any personal data that they may hold on the applicant
c) Liaise with all 3rd party providers to collect any personal data they process on behalf of the Parish e.g. Website Provider; Printer of Newsletter; Auditor
d) Check archived data
e) Collate all the personal data identified

Warning – Do not be tempted to delete records belonging to the applicant at this time, even if the Parish should not have them. This is a data breach and there are serious penalties for doing this.

It can be useful to keep in touch with the applicant to help refine the search and ensure their request is adequately met. Check with the individual about how they would like to receive their personal information when it is ready and/or the calendar month has passed. This may be in hard copy, by email, phone or in person. Confirm their ID if you have any doubt.

3. Assess the personal information held and make suitable for disclosure

All personal information about the individual should be collated and assessed by the Parish's data protection representative. Keep this information safe and secure at all times.

An individual is only entitled to **their own** personal data[3] and not to personal information relating to other people (unless the information is also about them or they are acting on behalf of someone). Personal data cannot be shared about someone else without their permission. Therefore, some parts of a document, which are liable for disclosure, may have to be blanked out. This can be done by:

Hard copy documents

- Print out the document or, if it is a paper record, make a photocopy
- Using a black marker pen, blank out the exempt information
- Make a photocopy of the blanked out version. This is the copy that will go to the applicant

Electronic documents

- Using the highlighter tool, highlight the exempt information in black
- Save the blanked out version as a separate copy
- Print out the document or scan the document to enable it to be sent electronically.

NB - Ensure the record is actually about the person concerned and not about someone else with the same name. Be careful and check continuously.

[3] Note: where personal data includes an expression of opinion about an individual by another person, the individual has the right to a copy of that expression of opinion unless it was given (and there is evidence of this) in confidence.

4. Gather additional information

As part of the response, the Parish also needs to inform the applicant:

- the purposes of processing (what)
- the legal basis for processing[4]
- the categories of personal data concerned (type)
- the recipients, or categories of recipient, the information has been disclosed to (shared with)
- the retention period for storing the personal data (how long it will be kept)
- the existence of their right to request rectification, erasure or restriction or to object to such processing
- the right to lodge a complaint with a supervisory authority[5]
- information about the source of the data, where it was not obtained directly from the individual;
- the safeguards provided if information is transferred to a third country or international organisation

5. Develop your response

Develop the final response for the applicant. This should include copies of all personal data as per request, and answers to the questions in section 4. The response should also include an explanation as to why any information requested cannot be disclosed (if this is the case).

- Do a final check to confirm everything is in order
- Ensure no personal information belonging to someone else is being shared
- Write a cover letter to go with the response. This should be signed by the data protection representative and/or the Clergy.
- Keep a duplicate copy of all information for the Parish (this is subject to retention guidelines)
- Send the information to the individual in the way they requested, e.g. via email. If by post, send by secure mail (e.g. register post)

6. Keep a Record

All SARs should be logged and recorded by the Parish. Keep:

- Copies of the correspondence between the Parish, the applicant, and any other parties.
- Record that ID was verified
- A record of any telephone conversations between the Parish and applicant
- A record of how the decisions were made and by whom
- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

NB - Personal information should not be kept for longer than is absolutely required. Adhere to the Retention Guidelines available on the Parish Resources section of the website. The less personal data processed the less personal data subject to a SAR. The RB library welcomes any historical collections and parish records no longer required in local custody.

Further Resources:

Templates are available from the Parish Resources Section of the Church of Ireland website.
Support is available from the Representative Church Body's Data Protection Officer, Rebekah Fozzard: rebekah.fozzard@rcbdub.org / 01-4125660

[4] Consent, Legitimate Interest; Public Interest; Vital Interest; Contractual Necessity and Compliance with a Legal Obligation. One lawful basis must always apply.
[5] This is the Information Commissioner's Office, Northern Ireland OR the Data Protection Commissioner's Office, Ireland.