Subject Access Request (SAR) Procedure

SOP · UK · Updated 2026-07-11 · Square brackets are placeholders to replace with your own details.

A subject access request (SAR) procedure is the written process your team follows when someone asks for a copy of the personal data you hold about them — how to recognise the request, who owns it, how to verify identity, where to search, what to redact, and how to respond within one calendar month.

SARs arrive without warning, in any words, through any channel. A line in a complaint email or a comment to a shift manager counts just as much as a formal letter, and the deadline runs whether or not the right person spots it. The recognising-and-routing step matters as much as the searching.

This template gives you the complete procedure: recognition examples for staff, logging and identity checks, a systematic search, third-party redaction, and the response and record-keeping steps.

Purpose and scope

This procedure sets out how [Your company] handles requests from individuals for access to their personal data. It applies to requests from anyone — customers, current and former staff, job applicants, suppliers — received by any member of staff through any channel.

Recognising a SAR

- Any request for a copy of someone's own personal data is a SAR: "send me everything you hold on me", "I want a copy of my file", "what information do you have about my account?"
- It does not need to use the words "subject access request", mention UK GDPR, or be in writing — verbal requests count.
- It can arrive by email, letter, phone, social media, review reply, or in person, addressed to anyone.
- Requests can come through a representative, such as a solicitor or family member — check their authority to act before releasing anything.
- If you are unsure whether something is a SAR, pass it to the SAR owner and let them decide.

Roles and responsibilities

- SAR owner ([name/role], deputy [name/role]): logs, runs, and signs off every request.
- Managers: pass anything that might be a SAR to the SAR owner the same working day.
- IT and system administrators: run searches across the systems they manage when asked.
- All staff: never ignore, delay, or answer a SAR themselves — route it.

Log, acknowledge, and verify

1. Forward the request to the SAR owner the same working day it arrives.
2. Log the date received — the response deadline is one calendar month from that date, not from when it reached the SAR owner.

3. Acknowledge the request and confirm the deadline to the requester.
4. Verify identity only if there is genuine doubt, asking for the minimum needed — do not use identity checks to buy time.
5. If you genuinely cannot respond without clarifying what the requester wants, ask promptly and check ICO guidance on how clarification affects the deadline.

Search

1. List every system that could hold the requester's data: [email, HR system, CRM, booking or till system, CCTV, shared drives, messaging tools, paper files].
2. Search using their name, known variants, email addresses, and account or payroll numbers.
3. Suspend routine deletion for anything in scope while the request is open.
4. Gather results into a single secure working folder at [location], access-limited to those handling the request.

Review and redact

1. Remove or redact other people's personal data unless they consent or it is reasonable to disclose it — take a considered view and record it.
2. Consider any exemptions narrowly, and record which were applied and why.
3. Check the material is intelligible — explain codes and abbreviations where needed.
4. Prepare the supplementary information (purposes, recipients, retention, rights) — usually by enclosing or linking the privacy policy.
5. Have the SAR owner review the final bundle before anything is sent.

Respond

1. Send the response securely — [encrypted file, secure portal, or tracked post] — before the deadline.
2. Include a plain-language covering note listing what is enclosed, any redactions or exemptions applied, and how to complain, including to the ICO.
3. Record the date sent, the method, and exactly what was provided.

Records and review

The SAR log at [system/location] records every request: dates, identity checks, search scope, redaction decisions, and the response. Keep the response bundle for [period] in case of follow-up or complaint.

This procedure is reviewed [frequency, e.g. annually] and after any request that ran late or drew a complaint. Owner: [name/role]. Next review due: [date].

How to use this template

1. Brief every customer-facing and management team on the recognition examples — the procedure fails at the front desk, not the back office.

2. Build the systems list in the search section by actually walking through where data lives, including legacy systems and archived mailboxes.
3. Name the SAR owner and a deputy who can cover leave — a one-calendar-month deadline does not wait for holidays.
4. Run a practice SAR on a volunteer staff member to time how long a real search takes.
5. Ask the SAR owner to read the ICO's right-of-access guidance before the first live request, not during it.

Official guidance

› ICO — UK GDPR guidance and resources