

The SAR Response Kit

How to respond to a subject access request — on time, and without the panic. A plain-English, step-by-step guide for any UK organisation.

UK GDPR · Data Protection Act 2018 · Data (Use and Access) Act 2025 | Not legal advice — see final page.

Someone — an employee, a customer, a service user, a tenant, or a member of the public — has asked for a copy of the personal data your organisation holds on them. That's a **subject access request (SAR)**, and you have **one calendar month** to respond. This kit walks you through it end to end, shows you exactly what to search and redact, and gives you a response letter you can adapt. Work through it in order.

8 The SAR response process, step by step

1 Recognise it as a SAR

A SAR can be made verbally or in writing, to anyone in your organisation, in any words — they don't have to say "subject access request" or quote the law. If someone asks for "everything you hold on me," treat it as a SAR and act.

2 Verify their identity

Before releasing anything, confirm the requester is who they say they are, using reasonable, proportionate proof. If you genuinely need ID, ask promptly — the clock can pause while you wait (see the deadline box).

3 Log it and start the clock

Record the date received, the requester, and what they've asked for. Your deadline is one calendar month from that date (or from when you receive ID / clarification).

4 Clarify the scope (if needed)

If you hold a large amount of data about them, you can ask the requester to specify what they want. A reasonable request for clarification can also pause the clock.

5 Search — reasonably and proportionately

Find the personal data across your systems. You must make a **reasonable and proportionate** search — and be able to show what you did. Use the checklist on the next page.

6 Review exemptions and third-party data

Not everything is disclosable. Screen out other people's personal data and check whether any exemptions apply (references, legal privilege, and others — see page 3).

7 Redact and compile

Remove third-party and exempt information using **true, destructive redaction** — never a black box laid over text that's still readable underneath. Assemble the disclosable material into one pack.

Respond and record

Send the pack securely with a covering letter (template on page 4). Keep a record of what you searched, what you withheld and why — your evidence that you handled the request properly.

The deadline rules — get these right

- **One calendar month** from receipt (or from the date you receive ID or requested clarification).
- **Extension:** you can take up to **two further months** if the request is complex or you've received several — but you must tell the requester **within the first month**, and explain why.
- **"Stop the clock" (DUA Act 2025):** the month can pause while you reasonably wait for the requester to confirm their identity or clarify what they want. It resumes when they reply.
- **Reasonable and proportionate search (DUA Act 2025):** you must carry out — and be able to evidence — a search that is reasonable and proportionate. You are not required to leave no stone unturned, but you must document your approach.
- There is normally **no fee**. You can only charge, or refuse, where a request is manifestly unfounded or excessive — apply this narrowly and record your reasoning.

✓ Reasonable & proportionate search — checklist

Which systems apply depends on your relationship with the person — a customer, a tenant, a service user and an employee live in different places. Work through the ones that fit, tick each as you check it, and where you decide *not* to search a source, note why — that's your proportionality reasoning, and it's exactly what the ICO expects to see.

- | | |
|--|---|
| ☐ Email mailboxes (current + archived) | ☐ Meeting notes & minutes |
| ☐ Shared drives / SharePoint / OneDrive | ☐ Call recordings (if any) |
| ☐ CRM & customer / account records | ☐ CCTV / door-access footage (if relevant) |
| ☐ Case-management or casework systems | ☐ Marketing / mailing lists |
| ☐ Finance, billing & payment records | ☐ HR / personnel file (if they're a worker) |
| ☐ Correspondence, complaints & enquiry logs | ☐ Third parties & contractors acting for you |
| ☐ Any team inbox they've contacted | ☐ Paper files & archive boxes |
| ☐ Internal messaging (Teams / Slack) | ☐ Work data on personal devices (if used) |

Third-party data & redaction

- A SAR entitles the requester to **their own** personal data — not other people's. Where a document names or identifies someone else, redact that detail unless the third party has consented or it's reasonable to disclose without it.
- Use **true redaction** that removes the underlying text. A black rectangle drawn over live, copyable text is one of the most common — and most serious — ways a SAR turns into a data breach.
- Check metadata, tracked changes and comments before you send — personal data hides there too.

§ Common exemptions — apply narrowly

Exemptions let you withhold specific material. They are narrow and you must be able to justify each one. The ones organisations meet most often:

- **Confidential references** — references your organisation has given (or received) in confidence are exempt.
- **Legal professional privilege** — legal advice and litigation-related material.
- **Management forecasting & planning** — where disclosure would prejudice the conduct of your business (e.g. a restructure or a pending decision).
- **Negotiations** — records of negotiations with the requester, where disclosure would prejudice them (e.g. a settlement or a claim).
- **Third-party personal data** — as covered above.

Record which exemption you applied, to what, and why. If in doubt on a sensitive request, take advice before withholding.

Response letter — template

Adapt this covering letter to send with the response pack. Replace the highlighted parts.

Dear **[requester name]**,

Your subject access request

Thank you for your request dated **[date]** for a copy of the personal data we hold about you. We are providing our response within the statutory period.

We enclose the personal data we hold about you that falls within the scope of your request, following a reasonable and proportionate search of our systems. Where information has been withheld or redacted, this is because it relates to another person, or because a legal exemption applies. **[Delete if not applicable.]**

The information is provided securely via **[secure link / password-protected file]**. **[If sending a password separately, say how.]**

If anything is unclear, or you think we've missed something, please contact us at **[contact]** and we'll be glad to help. If you're unhappy with how we've handled your request, you can complain to the Information Commissioner's Office at ico.org.uk.

Yours sincerely,

[name, role] · [organisation]

One-page checklist

- ☐ Logged the request and recorded the date received
- ☐ Confirmed the requester's identity (paused clock if waiting for ID)
- ☐ Diarised the one-month deadline — and flagged if an extension is needed (tell them within the month)
- ☐ Clarified scope with the requester if the volume is large
- ☐ Completed a reasonable & proportionate search (checklist on page 2) and recorded what I searched
- ☐ Reviewed for third-party data and applicable exemptions
- ☐ Applied true redaction and checked metadata / comments / tracked changes
- ☐ Compiled the response pack and covering letter
- ☐ Delivered securely and confirmed receipt
- ☐ Filed a record of the search, decisions and exemptions applied

Doing all this by hand, every time?

SARRequest is building software that does the heavy lifting — it searches your connected systems, suggests the redactions, tracks the deadline, and keeps the audit trail — so a SAR becomes an afternoon's review instead of a fortnight's dread. See how it works at sarequest.co.uk.

This guide is general information to help UK organisations respond to subject access requests under the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. It is **not legal advice** and does not create a professional relationship; for advice on a specific request, consult a qualified d