ProvePrivacy

GUIDE

SAR Exemptions: Protecting Third Party Identities

Every SAR response should be checked against one rule before it goes out, whatever exemptions elsewhere in this series did or did not apply. Personal data rarely exists in isolation: a case note, an email chain or a complaint file usually says something about someone other than the requester too. This guide covers the general protection for that other person's identity, a rule that sits apart from every exemption covered so far because it applies by default to almost every disclosure you make.

1. The rule that applies to almost every SAR

Schedule 2 to the Data Protection Act 2018 provides that a controller is not obliged to disclose information to the extent doing so would involve disclosing information relating to another individual who can be identified from it. This protection covers more than an obvious name: it extends to anything that would identify a third party as the source of information, such as who raised a complaint or supplied a tip off, and it takes into account not just the document itself but any other information the requester already has, or is likely to get hold of, that could unmask the third party even after redaction.

The rule only removes the obligation to disclose to the extent identification is unavoidable. If a document can be edited so the third party is no longer identifiable, whether by name, role, or a distinctive combination of details, the rest of it should still be disclosed.

WHY REDACTION IS NOT ALWAYS ENOUGH

Removing a name is not the same as removing identifiability. If the requester already knows who raised a particular complaint, or the surrounding detail narrows it down to one person, deleting the name alone will not satisfy this exemption. Assess what the requester already knows or could reasonably obtain, not just what is on the page.

2. The three step process

The ICO's guidance sets out a three step sequence for deciding whether third party information can be disclosed. Work through it in order for every document that touches someone other than the requester.

STEP ONE

Can you comply without identifying the third party

Consider whether the request can be met without revealing information that identifies the other person, taking into account both the document itself and anything else the requester is reasonably likely to know or obtain. Where the third party's information does not form part of what was actually requested, redacting names or details rather than withholding the whole document is usually the right approach.

In practice: test the redacted version against what the requester could reasonably piece together, not just against what is visible on the page.

STEP TWO

Has the other person consented

If the third party consents, the information must be disclosed. You are not obliged to seek consent, and in some cases it will not be appropriate to ask: for example, if you have no way of contacting the third party, asking would reveal something to them the requester does not already know, it would be inappropriate for the third party to learn a SAR has been made, or there is an imbalance of power that means consent could not be freely given, such as asking an employee about their manager.

In practice: document why you did or did not seek consent, since you will need to justify that decision if the disclosure is challenged.

STEP THREE

Is it reasonable to disclose without consent

Where consent has not been given or has been refused, you must still decide whether disclosure is reasonable, weighing the type of information involved, any duty of confidentiality owed to the third party, the steps taken to seek consent, whether the third party was capable of consenting, and any express refusal. This is not a discretion to withhold by default: if disclosure is reasonable, the information must be provided.

In practice: reasonableness is a judgement you must be able to explain, not a default answer in either direction.

3. Confidentiality and the other factors that shape reasonableness

Whether a duty of confidentiality is owed to the third party is usually the single biggest factor in this decision. A duty of confidence arises where genuinely confidential information, information not otherwise generally available, was shared with an expectation that it would stay confidential. Certain relationships carry that expectation as a matter of course, including a doctor and patient, an employer and employee, a solicitor and client, a bank and customer, a counsellor and client, and a trade union representative and member. Where a duty of confidence exists, it is usually reasonable to withhold the third party's information unless they consent.

Confidentiality is not automatic, though. Marking a letter confidential does not by itself create a duty of confidence, and information that is already widely available elsewhere is unlikely to carry the necessary quality of confidence, whatever label it was given.

Other factors worth weighing

Beyond confidentiality, three further considerations tend to matter in practice. Disclosure is more likely to be reasonable where the requester already knows the third party's information, has previously received it, or where it is publicly available; a colleague acting in the course of their duties, known to the requester through previous dealings, is generally easier to identify than an anonymous member of the public. The significance of the information to the requester also counts: the more central it is to understanding their own case, the more that can weigh against withholding it even where the third party refuses consent. Finally, consider the context of the request itself, including the conduct of the parties involved and the likely impact of disclosure on everyone concerned.

> **WHY MARKING SOMETHING CONFIDENTIAL IS NOT A SHIELD**
>
> A document is not protected simply because someone wrote confidential on it. Assess whether the information actually has the necessary quality of confidence and was shared with a genuine expectation of confidentiality, not just whether a label was applied.

SCHEDULE 2, PART 3, PARA 17

A presumption for health, social work and education data

Three narrow categories get a shortcut through the reasonableness test. It is treated as reasonable to disclose a third party's identity without their consent where they are a health professional who compiled, contributed to, or was involved in the data subject's care within a health record; a social worker, children's court officer, or equivalent, acting in an official capacity; or an education worker whose information relates to that role. These tests mirror the definitions used to assess serious harm in the health, social work, education and child abuse guide elsewhere in this series, so cross check the same source material if you are already working through that assessment.

In practice: this presumption only covers identifying these specific professionals in their professional capacity, not any other third party who happens to appear in a health, social work or education record.

SUPPLEMENTARY INFORMATION IS COVERED TOO

The same protection applies to the supplementary information you must provide alongside the substantive content of a SAR response, such as who you have shared the requester's data with. You can withhold the specific identity of an individual recipient while still disclosing the category they belong to, for example naming a legal department generally rather than the individual lawyers within it.

DECEASED DATA SUBJECTS

The UK GDPR, and this exemption with it, does not apply once a data subject has died, so the rights of others exemption cannot be used to protect a deceased person's identity in someone else's SAR response. A common law duty of confidentiality may still apply instead, so do not assume a deceased person's information is automatically free to disclose.

4. The pitfall to avoid

The most common error is redacting the obvious identifier, a name, while leaving in enough surrounding detail for the requester to work out exactly who it was anyway.

THE PITFALL

Deleting the third party's name from a document but leaving in enough surrounding detail, job title, dates or department, that the requester can still work out exactly who it was.

THE REMEDY

Test the edited version against everything the requester already knows or could reasonably obtain, not just against the document on its own, and redact whatever combination of detail would still unmask them.

KEY TAKEAWAY

This exemption applies by default across almost every SAR you handle, independent of every other exemption in this series. Run the three step process on any document that mentions someone other than the requester, even where no other exemption is in play.

Conclusion: prioritise identifiability, documented reasoning and proportionate redaction

Protecting a third party's identity is rarely about withholding a whole document. In most cases the right outcome is precise redaction: removing the specific names, roles or details that would identify someone else, while disclosing everything else the requester is entitled to see. Work through the three step process for every third party reference, document why you did or did not seek consent, and record the reasoning behind every redaction you make.

A few checks worth running before you rely on this exemption:

- **Spot every third party:** read for anyone else identifiable in the document, not just people named in the requester's own complaint or query.
- **Test real identifiability:** assess what the requester already knows or could reasonably obtain, not just what a redacted document shows on its own.
- **Weigh confidentiality first:** a genuine duty of confidence is usually the deciding factor in whether disclosure without consent is reasonable.
- **Record your reasoning:** log why consent was or was not sought, and why disclosure was or was not reasonable, for every third party redaction.

New: DSAR redaction, included in your subscription

Separating a third party's identifying detail from the rest of a record, rather than withholding the whole document, is exactly the kind of precise redaction the ProvePrivacy platform's DSAR Redaction tool is built for. Ask your account manager for a walkthrough.