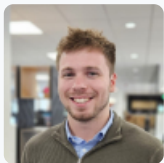


Article

Aug 2026

The rise of AI-assisted Subject Access Requests

Subject Access Requests (SARs) are some of the most taxing processes in an organisation. And now, with the introduction of AI, it is becoming increasingly easier for people to submit them.



Alex McIntosh

Information Security Consultant

Email alex.mcintosh@waterstons.com

SARs have long been a feature of the data protection landscape. Under UK GDPR, any individual has the right to request what personal data is held, and confirmation whether, and how, it is being processed. They are commonly used as a tactical tool in employment disputes, often disrupting operations due to the significant amount of time and effort needed for response.

SARs are no longer simply a compliance task. They are becoming a data discovery and security operations challenge. AI is about to make that challenge much bigger, and organisations need to be ready.

How is AI changing SARs?

Generative AI is fundamentally lowering the barrier to submitting SARs. What once required a large amount of legal knowledge, careful drafting and an understanding of relevant legislation and regulations, can now be produced within minutes using a Large Language Model. AI is now able to support a requestor in:

- Drafting legally structured SARs complete with statutory references, deadline reminders, and escalation language
- Identifying what to request. A simple prompt such as "List every system an employer might hold my personal data in" can generate a comprehensive annex covering Microsoft 365, Teams, WhatsApp, CCTV, HR systems, and more
- Iterating and escalating by generating follow-up requests, chasers, and formal complaints about SAR handling with minimal effort.

For IT and security managers, this puts pressure on data mapping, indexing and search capability across the estate to ensure the data is organised and easy to find.

But it's not just the requestor who is benefitting from AI in this context. AI can also support an organisation's defence, helping with search, classification and redaction, provided the underlying data is well managed.

Why handling SARs properly is vital

For IT leaders, SARs represent a significant operational risk. From unmanaged data sprawl and shadow IT, to unclear data ownership and the resource strain on an IT team to run searches under pressure, they can be challenging without effective data management and early coordination with HR to pre-empt possible requests.

Failing to handle SARs properly also carries serious consequences from an organisational and reputational perspective.

- Fines of up to £17.5 million or 4% of global annual turnover, whichever is higher.
- Legal action for not complying with a SAR.
- Reputational damage through ICO publication of complaints against companies, leading to loss of trust amongst clients and employees.

Organisations can refuse requests that are 'manifestly unfounded' (for example, submitted purely to disrupt the organisation) or 'manifestly excessive' (too broad, repetitive or disproportionate). This may be especially relevant where AI is used to generate or submit requests at scale for improper or potentially nefarious purposes.

What should you do now

Teams that handle SARs should be treating them as a governable, repeatable process – not simply an administrative task. From an IT and security perspective, this is what we recommend.

- Ensure the full data architecture and system inventory, where personal data actually lives, including shadow IT, backups and legacy systems, are well managed and up to date
- Invest in technology to ease the greatest burden. Review and redaction are often the most time-consuming processes, so consider using eDiscovery-style tools, such as Microsoft Purview, to provide automated redaction that is supported by human quality assurance, as well as implementing redaction automation and QA workflows to speed up reporting
- Consider access control and least-privilege when pulling data to restrict who sees what during the process
- Ensure there's a log and audit trail of search and decisions for defence and auditability
- Where AI tools are used to help process SARs, ensure clear governance is in place, including a policy to prevent personal data being fed into public LLMs.

Ultimately, strengthening data governance is vital to managing SARs efficiently. Apply retention schedules consistently, limit the use of unsanctioned communication channels (especially WhatsApp and consumer messaging platforms) for work activity, and ensure managers understand that internal commentary may be disclosable as personal data.

Looking ahead

The convergence of workplace data sprawl and AI-driven accessibility means that Subject Access Requests will only grow in volume, sophistication, and strategic intent. Organisations must move beyond treating SARs as a reactive obligation and instead embed them within a proactive, well-governed data protection process.

How can Waterstons help?

Firstly, let's take a step back and understand what you do and don't have in place already. Do you need redaction automation, eDiscovery tooling, or simply a closer look at your data management processes? Through data mapping and a technical audit of systems, we can see where any gaps might be.

Once these are in place, we can help with compliance oversight through:

- A virtual Data Protection Officer to help meet your privacy and compliance obligations without employing a full-time DPO.
- SAR support by carrying out the bulk of the request – from email filtering to redaction – if you don't have the resources or time to respond.

Want to find out more? Get in touch to see how you can save time and effort on your organisation's SARs at info@waterstones.com.au
