From DSARs to data protection complaints:

Implementing lessons from 2025

04

Rebecca Morgan
Legal Director
rebeccamorgan@dacbeachcroft.com

Amanda MacKenzie
Associate
ammackenzie@dacbeachcroft.com

Heasha Wijesuriya
Solicitor (Australian Qualified)
hwijesuriya@dacbeachcroft.com

Kate Galloway
Partner
kgalloway@dacbeachcroft.com

Data Subject Access Requests (**DSARs**) remained in the spotlight in 2025. Indeed, developments picked up pace; we saw a number of notable legal and regulatory interventions and trends in technology and public sentiment impact upon the volume and complexity of such requests. What are the lessons we can take into 2026? And how will those lessons serve to support controllers manage data protection complaints in a year when the new statutory complaints handling requirements will come into effect? We examine these issues.

The evolving DSAR legal and regulatory landscape

2025 started with the High Court ruling in *Ashley v HMRC*, notable because recent DSAR related case law is sparse.

This case arose from His Majesty's Revenue and Customs (**HMRC**) challenge to Mr Ashley's property valuations following a 2012 sale, which led to a £13.6m tax bill. Although the tax bill was later withdrawn, Mr Ashley exercised his right under Article 15 UK General Data Protection Regulation (**UK GDPR**) to access all personal data held by HMRC relating to its tax enquiry. HMRC adopted a narrow approach to the DSAR, limiting searches to one department and withholding most data under the "tax" and "legal privilege" exemptions set out in Schedule 2, Data Protection Act 2018 (**DPA 2018**), initially providing very limited information. After prolonged correspondence, Mr Ashley issued court proceedings. In January 2025, the Court ruled largely in Mr Ashley's favour, finding HMRC had failed to meet its UK GDPR obligations.

This case provides valuable guidance on how to manage DSARs. The key takeaways can be summarised as follows:

- **Adequately define the scope of the search:** Controllers should apply a holistic, organisation-wide approach to searches which should not be limited by internal policies or departmental boundaries.
- **Carry out reasonable and proportionate searches:** The Court found that HMRC had incorrectly asserted that the searches were disproportionate based on hours taken (150 hours). Time alone does not make a search disproportionate; consider size, resources and nature of the request.
- **Carefully consider the meaning of personal data:** The Court applied a broad interpretation of the definition of personal data, finding that the valuations of Mr Ashley's properties were to be regarded as his personal data because they were, by reason of *"their content, purpose or effect",* linked to Mr Ashley. Controllers should assess each piece of information individually to determine if it relates to the data subject, maintain consistency across departments and keep an audit trail of decisions.
- **Use of exemptions:** The "tax" exemption allows a controller to withhold personal data if disclosure is likely to prejudice the assessment or collection of tax. It was held that "likely" means a *"very significant and weighty chance of prejudice",* supported by evidence. The application of exemptions requires strong evidence and must be applied granularly, not on a blanket basis.
- **Provision of data:** Responses must be concise, transparent, and intelligible. Controllers should avoid excessive redaction that renders data meaningless; provide context where necessary to ensure intelligibility.

From DSARs to data protection complaints:
Implementing lessons from 2025

In June 2025, the Data (Use and Access) Act 2025 (**DUAA**)received royal assent, making minor changes to the existing DSAR regime. Specifically, it inserted a new Article 15(1A) UK GDPR which provides that a data subject is only entitled to personal data based on a *"reasonable and proportionate"* search. Unusually this provision has retrospective effect and is treated as having come into force on 1 January 2024. The DUAA also inserted a new Article 12A UK GDPR which sets out the meaning of *"applicable time period"*, bringing the "stop the clock" mechanism formally into the wording of the UK GDPR. Whilst these changes merely codify existing guidance from the Information Commissioner's Office (**ICO**), putting them on a statutory footing may encourage controllers to be more robust in their approach to unwieldly DSARs.

The ICO also kept DSARs firmly on its radar with some notable enforcement action in 2025, including those against Bristol City Council (**BCC**) and South West Police (**SWP**). The facts of these cases were similar; both public sector bodies failed to respond to hundreds of DSARs within the statutory time frames over several years. This resulted in numerous complaints to the ICO and some data subjects expressing distress and detriment as a result of the delays. For both BCC and SWP, the DSARs often involved large volumes of data including sensitive information and, in the case of BCC, children's data.

Both controllers cited lack of resources and experienced staff to deal with backlogs. Whilst the ICO acknowledged these difficulties, stating *"Although the Commissioner understands the difficult impact under-resourcing has on organisations, this is not an issue for the Commissioner to rectify. The Commissioner is of the view that it is for organisations to demonstrate compliance with their data protection obligations and to judge what resources are appropriate for their organisation as they alone will best understand the pressures they face and the nature of their business",* it found that infringements had occurred and issued formal enforcement notices requiring urgent remedial action within specified timescales. This aligns with the ICO's public sector approach to enforcement; had the controllers been private sector companies there may well have been an outcome which included a monetary penalty notice.

These actions illustrate the importance the ICO places on the enforcement of this fundamental right and serve as a broader warning to all organisations that failure to prioritise DSAR compliance can lead to reputational damage, regulatory scrutiny, and significant operational disruption.

An unreported ICO prosecution in September 2025 signalled a possible shift in its approach to DSAR enforcement with what we understand to be its first criminal prosecution under section 173 Data Protection Act 2018 (DPA 2018). While DSAR non-compliance is usually handled as a civil matter, with the ICO able to take enforcement action including the issuing of a monetary penalty notice, section 173(3) DPA 2018 provides an alternative route of action. Under this section, it is a criminal offence to intentionally alter, erase, block, or conceal information to prevent disclosure in response to a DSAR, designed to deter deliberate obstruction of the right of access.

In this case a director of a care home was convicted for deliberately obstructing a DSAR submitted on behalf of a resident. Instead of responding to the request, the director concealed and erased records, prompting an ICO investigation and resulting in a criminal prosecution leading to a conviction and a fine of £1,100 (plus costs of £5,440). This case illustrated that deliberate obstruction can lead to criminal liability of the controller, as well as its employees, officers or individuals. This offence is punishable not only by a fine but, in serious cases, imprisonment.

The implications of the ICO's step change in its decision to bring a criminal prosecution is potentially significant, particularly in light of the new enhanced investigatory and enforcement powers under the DUAA. At the time of writing, these powers were expected to come into force in early 2026 or swiftly thereafter, and enable the ICO to require the production of documents under existing powers to issue "information notices"; require individuals to attend interviews and answer questions via new provisions relating to "interview notices"; and require controllers or processors to commission and pay for a report by an "approved person" as part of an investigation into a specific matter. These broad powers will enable the ICO to conduct more thorough and effective investigations.

Trends in technology and public sentiment

2025 seems to have been the year that DSARs entered the mainstream. Public awareness has steadily increased, such that any contentious employment matter, data breach, or other issue causing dissatisfaction to a data subject will inevitably see the submission of a DSAR. This rise in public consciousness, coupled with the accessibility of technology, has led to a perfect storm for controllers on the receiving end of requests.

The rise of AI-supported DSARs

With the use of AI technology such as ChatGPT now commonplace in our daily lives, it is clear to see its growing utilisation in data protection issues, and especially in relation to DSARs. The ease of use and free access to these tools has brought about a commensurate rise in the number of DSARs organisations are receiving. From a data subject perspective, any technology that makes exercising individual rights easier is to be welcomed. But what of the impact this is having on controllers?

We have observed AI-supported DSARs falling squarely into two camps. On the one hand, some data subjects are clearly using AI to generate what will often be very long and confused correspondence, frequently containing irrelevant or out of context UK GDPR references, without applying much in the way of critical thinking to the request. This makes the task of deciphering the request itself time-consuming for the controller, before they have even begun to respond.

On the other hand, and particularly in the employment field, we are seeing a large increase in DSARs that are becoming increasingly sophisticated. There is clear evidence of the considered use of AI technology to carefully scope DSARs in ways which can make the response more complex for the employer with clear links being made to the issues in prospective or ongoing employment disputes.

Further to the initial DSAR, AI-generated complaints are now commonplace, frequently being sent to controllers within minutes of the parties' prior communications. As well as the obvious impact on resources involved in responding, the effect on the data protection team's morale should also be acknowledged. Having to dedicate additional time to respond to largely unfounded or fallacious queries which have been AI-generated, as opposed to genuinely-held concerns of the data subject, can be frustrating as well as time-consuming, especially where it is obvious that the data subject has not taken the time to properly consider the response they have received.

These issues highlight that data subjects themselves are often misinformed and may not even fully understand their own requests or correspondence. For instance, the accuracy of the AI output will be guided by the quality of the prompts made by data subjects. For controllers, we can expect to see a rise in the submission of complex DSARs; either being complex in the sense that they are difficult to decipher, or because the DSARs are very focused on the key issues in hand, which are in themselves complex in nature.

The rise in use of AI technology is clearly benefiting data subjects by making it easier to exercise their right of access, with controllers across the board feeling the additional burden of both the uptick in volumes of requests, and the increasing sophistication and complexity of the DSARs being submitted.

There is certainly a role for controllers to make use of AI tools themselves to support DSAR responses, but we are some way from AI being a panacea for the headache that is a complex or bulk DSAR.

Mass DSARs

Throughout 2025, the trend for DSARs stemming from circumstances of a cyber-attack has continued. Given the constant threat of cyber incidents, as evidenced by several high-profile attacks in the UK this year, we do not expect this trend to slow in the coming year.

AI-generated DSARs can only serve to fuel this trend, often being utilised as a vehicle to overwhelm controllers where a large group of data subjects have been impacted by the same data breach. For instance, we have observed a vocal community of data subjects sharing AI-generated DSARs via social media (e.g. Reddit) for onward transmission to the relevant controller following a personal data breach involving over 4,000 data subjects.

The combined use of AI and social media by data subjects exposes controllers to the risk of mass DSARs which have the potential to overwhelm organisations, taking significant resources to respond.

Whilst by no means a new development, we are continuing to observe the submission of mass DSARs via Claims Management Companies (**CMCs**) as a pre-cursor to bringing a regulated complaint or litigation. This frequently raises questions about the authenticity of the DSARs; whilst clients of CMCs may have signed letters of authority, they are not always fully aware that this right will be exercised on their behalf. Indeed, we are aware of cases where CMCs have insisted that DSARs are pursued, failing which the data subject is told they will be required to pay significant costs incurred by the CMC on their behalf. Although such pressure tactics displayed by CMCs may not be considered 'enforced' DSARs within the meaning of the DPA 2018, it is clear that in some cases it is not the data subject that genuinely wants to exercise their rights. Whilst the ICO guidance is silent on this point, controllers might therefore look to other avenues, such as refusing a request on the basis it is manifestly unfounded.

In any event, controllers must generally respond to DSARs despite the use of AI. While there are existing protections against DSARs considered manifestly unfounded or excessive, guidance from the Information Commissioner's Office explicitly refers to an expectation that DSARs are reviewed on a case-by-case basis. Whilst at one point, there were proposals to lower the threshold for refusing to deal with such requests to those which were 'vexatious', this proposal to lower the bar did not find its way into the final text of the DUAA.

Even if the burden on controllers in handling individual AI-generated DSARs does not seem onerous, one can appreciate the issues caused when DSARs are brought to controllers en mass. Obvious difficulties emerge in relation to the capacity of controllers to review mass DSAR requests which are increasingly being weaponised by data subjects given ease of access via AI.

Strategies for dealing with DSARs

Having painted a pretty bleak picture, you may be wondering what practical steps you can take to get a handle on DSARs. A controller's guiding principles for approaching DSARs might look something like this:

- **If in doubt, ask the data subject:** this applies to seeking clarification if a request is unclear (especially if it is difficult to decipher what the data subject is genuinely seeking when they have submitted an AI-generated DSAR), requesting proof of ID if there is any uncertainly, or requiring a letter of authority where a DSAR is submitted on behalf of (rather than directly by) the data subject. Where clarification or ID is required, the controller may adjust the deadline in accordance with the relevant provisions.
- **Create an appropriate search strategy:** this should be considered early on in the process, and documented, particularly as searches are refined to create a set of responsive documents that are relevant to the data subject's request as well as being reasonable and proportionate. The controller should think about the background that has given rise to the DSAR and use that context to identify key data custodians across the organisation and to generate search terms, along with any key phrases that the data subject may have used in the request.
- **Extend the deadline where a request is complex:** it is perfectly legitimate to extend the deadline by up to a total of three months if there are complexities in handling the DSAR. This will perhaps be even more likely with the submission of AI-supported DSARs. Use the ICO's guidance to help identify all relevant factors and document the decision. The data subject should be made aware of the application of the extension, along with the accompanying reasons. In any event, the controller should respond "without undue delay" which may be earlier than within the full three months where appropriate.
- **Refuse to handle manifestly unfounded requests:** where the DSAR appears not to be a true exercise of the data subject's right, consider whether the request can be refused on the basis that it is manifestly unfounded. This should be considered on a case-by-case basis, but if a data subject appears to be under pressure from a CMC to make or continue with a DSAR, then this may be one option to refuse the request.
- **Use AI and other tech to your advantage:** careful use of AI tools can save time and reduce manual involvement. Current use cases predominantly focus on activities such as de-duplication, batching and transcribing. We expect to see further uses of AI as technologies develop and become more sophisticated. Might we see an AI tool that could assess the tone of a data subject's correspondence to predict when a DSAR might be made, to enable a controller to be on the front-foot in terms of recognising DSARs promptly and predicting peaks in resourcing requirements?
- **Use AI with care:** don't assume that references to legislation and caselaw are correct and train your staff to be healthy sceptics regarding any AI-generated content.
- **Accountability:** always keep clear records of your DSAR handling especially in relation to search parameters and the application of any exemptions. You should ensure that this records the use of exemptions on a case-by-case basis, and not as a blanket approach. Records will prove useful if you receive a data subject complaint (on which, see below) or ICO enquiries.
- **Peer review:** for particularly contentious DSARs, consider whether the DSAR response should be peer reviewed by someone within the business (with skills beyond data protection), who is aware of the broader context in which the DSAR has been submitted. In an employee context, carefully consider who will review the response bearing in mind the potential sensitivity of HR related issues and the need to have knowledge of any wider anticipated or ongoing employment dispute.
- **Respond but don't pander:** Try to avoid being drawn into protected and lengthy correspondence after responding to the DSAR. Refer back to the original comprehensive response and remind the data subject of their right to submit a data protection complaint, following which they may complain to the ICO. Ensure you keep a record of all your correspondence in case it is required by the ICO.

DUAA – Data Subject Complaints

The DUAA introduces a new section 164A DPA 2018 which requires controllers to establish processes to handle data protection complaints. The requirement is expected to come into force in or around June 2026. A data protection complaint may arrive in a number of guises: it may relate to a stand-alone data protection issue, be a follow-up to a DSAR where the data subject is dissatisfied with the response or could even be submitted alongside the DSAR itself.

Controllers will be required to facilitate the making of such complaints, for example by making complaint forms available online or by hard copy, noting that a form is not mandatory but is suggested as one option. An acknowledgement must be issued within 30 days of receipt, and the controller must take appropriate steps to respond to the complaint without undue delay and inform the data subject of the outcome. The data subject should be kept informed if the final response is going to take some time.

Aside from the mandatory 30 day complaint acknowledgement and the obligation to investigate and respond without undue delay, the DUAA is not unduly prescriptive, and it therefore leaves controllers with a healthy degree of flexibility to tailor their complaints process to their own business.

It is also worth being aware of related powers issued to the Secretary of State to issue secondary legislation establishing mandatory complaint volume reporting to the ICO. When in planning phase, controllers would be wise to think about what management information they should collect, both for internal reporting purposes but also with one eye to the future if the mandatory reporting requirements do come to fruition.

ICO guidance

Noting that this is a new requirement, albeit many controllers will already have some form of complaints process in place, the ICO has already produced and consulted on draft guidance. We are expecting the final guidance to be published this year, to give controllers time to take into account the ICO's views when establishing or finessing a data protection complaints process. As well as addressing specific legislative requirements, the draft guidance also offers examples of practical steps.

Creating a data protection complaints process

Key to ensuring that your organisation is ready for this new requirement is to create a complaints procedure, and make your staff aware of the right to complain and who will be responsible for handling any complaints. Crucially, you should consider any overlap with other complaints obligations you may have, especially if your organisation is in a regulated sector, since data protection issues are most often raised as a precursor to or as a result of a bigger issue. Do you want your complaints processes to be conjoined, or separate but aligned? Do other complaints regimes have stricter timescales attached to them?

The key steps in preparing to deal with data protection complaints include:

- Drafting or updating a formal complaints procedure, which data subjects can easily access.
- Assign roles and responsibilities – will your process facilitate an independent review by a colleague who was not involved in any previous correspondence with the data subject?
- Consider how data subject complaints will sit with any other complaints obligations you are subject to.
- Ensure that you keep adequate records to be able to respond to complaints.
- Inform and train staff – this will involve specific training for data protection staff, as well as general awareness-raising across your organisation so that complaints are recognised and dealt with promptly.
- Establish a process to identify any trends and to reflect so that any lessons are learned.

Whilst a new data protection complaints regime may feel like an additional burden, it might also help to draw a line under protracted correspondence with dissatisfied data subjects. Once you have issued a final complaint response, an ICO referral is the next logical step. If you are confident that you have addressed the data subject's concerns, and have documented any decisions taken, then you should take a robust approach to using the complaints process as the end point and let the complaint run its course via the ICO. When crafting your complaints processes and any associated management information you will collect, think carefully about how this data can be used to your advantage; allow the information to give you meaningful insights into your organisation's compliance so you can get ahead of any more systemic issues; if you have good oversight of your complaints you will be able to identify recurring themes, and can intervene before they become big-ticket problems.

It's clear that 2026 will be a busy year for data protection practitioners, not least because we are unlikely to see any decline in the number of data subjects exercising their rights and thereafter submitting complaints about the handling of those requests, or for broader data protection concerns. Whilst there is no effective short-cut to compliance, controllers can begin to make smart use of technology to assist where possible, and should shore-up internal processes, training, and strategies to ease the burden of handling DSARs and data protection complaints.