DATA PROTECTION NETWORK

The State of Data Subject Access Requests

Research Report

Volumes, Complexity and Trends

November 2026

By Data Protection Network



How requests are experienced by DPOs and others who oversee and/or directly handle them

In partnership with

ProvePrivacy

© 2026 Copyright of Data Protection Network Associates. All rights reserved.
Registered address: 12 Old Great North Road, Stibbington, Peterborough PE8 6LR. Number 12568068.

Any information provided or opinions expressed in this document should not be construed as legal advice.

Foreword

For many years we've talked with others working in data protection about the "weaponisation" of the right of access, with Data Subject Access Requests (DSARs/SARs) used for purposes they were never originally intended. For example, as a tool to gather information for use in employment or other disputes.

Over the past year though, we've had a growing sense something bigger is happening: many first-hand accounts of an uplift in the volume of access requests organisations are receiving.

ICO statistics show DSARs make up a significant proportion of the complaints the regulator receives. Yet there's surprisingly little evidence about the experiences of the organisations handling them. We wanted to understand the trends, so we set out to conduct our own research to establish evidence of the nature and volume of requests received and how they affect people on the sharp end of fulfilling them.

This research does not assess how effectively organisations are fulfilling requests, nor the experience of those submitting them.

We very much hope this research paper can support a broader conversation around whether the right of access remains effective in practice, for both people making requests and the organisations receiving them. A challenge we urge regulators, policymakers and practitioners to help address together.

Philippa Donn & Simon Blanchard
Co-Owners, Data Protection Network

Contents

Foreword 2

Executive summary 4

Introduction and context 6

Survey methodology 7

Respondent and organisation profile 8
- Respondent roles 8
- Respondent role in DSARs 9
- Organisation sector and size 9

Findings 11
- A: Volume, nature and complexity 11
  - Volume change in past 12 months 11
  - Who submits requests? 13
  - Source of increase in requests 15
  - AI-generated requests 17
  - Complexity of requests 17
  - Factors making requests tricky to process 19
  - Rising complexity and challenges 20
- B: Impact of DSARs on the organisations receiving them 21
  - Impact of AI-generated requests 21
  - Impact on teams and organisation 23
- C: Resourcing, handling and performance 25
  - Resourcing 25
  - Role of DPO 27
  - Meeting the deadline 29
  - Dissatisfaction and complaints 30
  - Use of DSAR tools 32
  - Use of external DSAR services 33
- D: Views on legislative change 34
- E: Additional respondent comments 38

Appendices 39
- Appendix 1: Methodology for open text analysis 39
- Appendix 2. Research limitations 40
- Appendix 3. Survey questions 41

About DPN 46

About ProvePrivacy 47

Executive summary

The aim of this research was to establish both quantitative and qualitative evidence of the volume and nature of Data Subject Access Requests (DSARs/SARs) received by organisations, how these may have changed over the past twelve months, and how requests are experienced by those handling them.

Our research shows Data Protection Officers, along with data protection and compliance teams, are increasingly stretched and frustrated by a significant growth in the volume and complexity of DSARs. These trends appear to be largely driven by individuals using AI to draft their requests, and requests being made as part of employment disputes and proceedings.

A dominant theme across survey respondents is strong support for the right of access, combined with a sense the balance has tipped too far. A significant majority would like to see changes to the law. Respondents also called for clearer regulatory guidance and greater public awareness of what the right of access entitles individuals to receive.

Key findings

- **83% of respondents reported an increase in the volume** of requests in the past 12 months, with more than half describing this as a 'significant increase'. **The public sector** has been hit hardest, with more than nine in ten public sector respondents (91%) reporting an increase.
- **90% of respondents receive requests from current or former employees.** These are described as often being submitted alongside grievances, disciplinaries or tribunals.
- **85% said the complexity of requests has increased over the past year** with 62% describing this increase as 'significant'.
- **92% receive requests 'likely to be AI-generated',** with 55% saying this represents a significant proportion of the requests they receive. These are typically described by respondents as longer, broader and harder to decipher.
- **AI-generated requests and the volume of data to be searched** are the most commonly cited reasons for an increase in complexity.
- **76% would like to see a change in the law** to reduce the burden on organisations.

Respondents described a considerable and growing impact on those handling access requests. DSARs are described as relentless, with complex cases often taking days or weeks to complete. This diverts time away from, and in some cases prevents, other data protection work from being completed. The pressure is felt acutely in small teams or where only one person handles requests, where a single complex request can bring all other work to an abrupt halt.

DSARs are also having a very personal impact. Across organisations of all sizes, those handling requests reported stress, burnout and low morale, driven by the workload, the pressure of deadlines, and repeated challenges from requesters.

Organisations are incurring additional costs through new roles, overtime, outsourcing, legal advice and technology. Many are struggling with growing backlogs and experiencing difficulty meeting statutory deadlines.

About the survey

The survey received 412 responses from people who handle or oversee DSARs. For a specialist professional group, this is a strong level of response, giving a broad and detailed picture of how requests are managed in practice across organisations of different sectors and sizes.

Respondents were highly engaged, with between 67% and 88% providing optional comments to the main free-text questions. These responses give valuable insight into the practical realities of fulfilling requests.

As with any voluntary survey, respondents chose to take part. The findings are therefore best read as a clear indication of practitioners' experiences rather than a precise measure across every organisation. However, the same themes came through consistently, which gives us real confidence the findings reflect widely shared experiences in the profession.

Responding to the findings

> *"This timely report sets out an important snapshot of the realities data protection practitioners face in handling DSARs. The commitment DPOs have to the essence of this right is clear, but it is right that we start a wider discussion in the DP community about how we can best tackle these challenges in the short, medium and long term."*
>
> **Steve Wood, Director at PrivacyX Consulting and former UK Deputy Information Commissioner**

> *"This Report is very timely as it highlights the increase in DSARs, the increasing use of AI to generate complex and often over-engineered requests, and the impact that these DSARs have on organisations that receive them. Whilst many DSARs are fair and reasonable, there is an increasing weaponisation of these requests."*
>
> **Robert Bond, Senior Counsel at Privacy Partnership Law and outsourced DPO**

This research shows there's a real risk a disproportionate amount of time is being taken up fulfilling requests. We're hopeful there can be agreement on measures to ease the burden on organisations, while still protecting this very important individual right.

Introduction and context

> *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data…*
>
> *Article 15, UK GDPR*

The right of access has existed in UK law since the Data Protection Act 1984, but it attracted wider awareness when the GDPR became applicable in 2018. This new regime also strengthened the right. It removed organisations' ability to charge a fee (£10 in the UK) and shortened the response time from 40 calendar days to one calendar month.

The right entitles individuals to receive a copy of their personal data held by organisations acting as controllers, along with specific supplementary information. It's commonly referred to as a Data Subject Access Request (DSAR) or Subject Access Request (SAR). In this report, we use the term DSAR.

Handling a request can be relatively straightforward where the personal data held is limited, or where the request is specific and clearly defined. In other cases, it can be complex and may involve extensive searches of large volumes of data across multiple systems and applications. The information retrieved needs to be checked for relevance and assessed against exemptions which may apply, requiring certain information to be redacted or withheld.

The Data (Use and Access) Act 2025 has enabled amendments to UK GDPR which give existing case law and regulatory guidance a statutory footing. These confirm the response period does not start until organisations are satisfied as to the person's identity and that organisations only need to carry out reasonable and proportionate searches. It also allows the 'clock' to be paused if seeking clarification from the requester. An amendment to the Data Protection Act 2018 also means from 19 June 2026, controllers must have a data protection complaints process.

The regulator responsible for overseeing UK data protection law is the Information Commission (ICO), formerly the Information Commissioner's Office. The regulator has published detailed guidance on the right of access, which stretches to more than 100 pages and was updated in December 2025. The guidance covers a wide range of rules and considerations, many of which have to be assessed on a case-by-case basis.

Survey methodology

Design: The survey was designed to collect both quantitative and qualitative data. It contained 29 questions, a mix of closed questions with one choice or multiple choices, and questions with free-text options, so respondents could explain their answers in their own words.

Dates live: The survey was live online from 9 September to 5 October 2026.

Promotion: The survey was promoted to DPN's 6,000+ newsletter subscribers and posted on LinkedIn, where other data protection professionals also shared it. A paid LinkedIn 'boost' promotion was targeted at people working in data protection, information governance and compliance roles. The survey was also shared by word of mouth.

Number of respondents: The survey received 412 fully completed responses.

Anonymous: Responses were anonymous. Respondents were not asked for any personal information or for the name of their organisation.

Terms: Some terms, such as "complexity", were deliberately left undefined. Respondents were left to judge for themselves what counted as an increase in complexity. Respondents used their own judgement on whether requests received were "likely to be AI-generated".

Use of AI to process the findings: AI tools were used to support analysis of the results in two ways:

a) **cross-tabular analysis**, for example, assessing whether organisation size or sector made a difference to the results for selected questions, and;

b) qualitative thematic analysis of **free-text responses**, to identify the most common themes emerging across free text answers.

The outputs from AI were verified by the research team. More detailed methodology for specific datasets can be found in *Appendix 1.*

Quotes: Respondents' quotes are presented as written, with minor spelling corrections. Where illustrative quotes are used in the report, these were manually selected by the research team.

Base responses: All quantitative questions were mandatory, with some questions only shown to a sub-set of respondents dependent on their answer to a preceding question. Most qualitative (free text) questions were optional.

Percentages: These are rounded to whole numbers, so totals may not always add to exactly 100%. Combined figures, such as bracketed totals, are calculated from the underlying counts and may differ by one percentage point from the sum of the rounded figures. Free text answers may have been coded to more than one theme, so percentages can add up to more than 100%. Some questions allowed more than one answer, and thereby percentages can add up to more than 100%.

Reassigning 'other': Where respondents selected 'other' but their free text answer was considered highly likely to fit an existing category, this was reassigned. For example, when asked about their sector, some respondents selected 'other' and wrote charity, this was reassigned to third sector.

Organisation size: Organisations with 1 to 249 employees were merged into one group.

The survey was not piloted prior to launch. No weighting has been applied to the results.

Respondent and organisation profile

Respondent roles

Respondents were asked to select their role from a list of options or complete a free text option for 'other'. 87% said they were a DPO/Privacy Officer, Data Protection Manager/Lead (or similar), or were members of data protection teams.

Role	%
DPO / Privacy Officer	39%
Data protection manager/lead (or similar)	34%
Data protection team member	14%
Legal/compliance team	7%
HR manager or HR team member	<1%
Other	6%
Total	**100%**

Base: all respondents (n=412). Percentages are rounded to the nearest whole number and may not total exactly 100%.

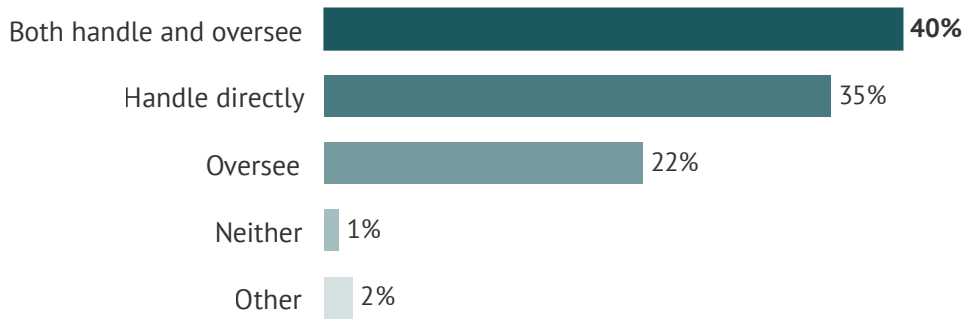
Of the 6% who selected "Other", most held governance, risk or compliance roles or combined DPO duties with another role; a small number described themselves as senior managers, information rights or security specialists, or other roles.

As the majority of respondents were data protection professionals, including DPOs, data protection leads and team members, the findings reflect the views of those with direct, day-to-day experience of fulfilling requests.

Respondent role in DSARs

Almost all respondents (97%) are directly involved in DSARs, whether handling requests themselves, overseeing them, or both. Two fifths (40%) both handle and oversee.

Role respondents play in handling DSARs

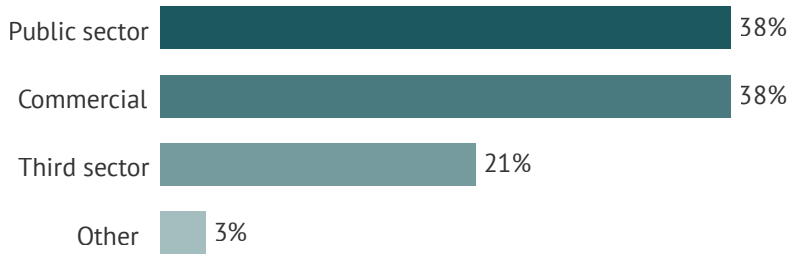


Base: all respondents (n=412). Percentages are rounded and may not total exactly 100%.

Organisation sector and size

Respondents came from a broad cross-section of organisations: the public sector (38%), the commercial sector (38%) and the third sector (21%). Percentages are rounded. In the raw results there were just four more respondents from the public sector than from the commercial sector.

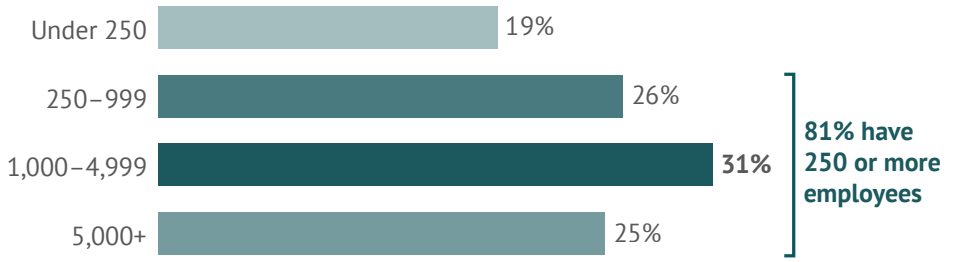
Sector respondents work in



Base: all respondents (n=412). Some "Other" answers were reassigned to a defined sector, for example "charity" was moved to third sector. Percentages are rounded to the nearest whole number.

A range of organisations of different sizes is represented, but the sample is weighted towards larger organisations. Four in five respondents (81%) work in organisations with 250 or more employees. More than half (55%) work in organisations with over 1,000 staff, and a quarter (25%) in larger organisations of 5,000 or more. The single largest group, at 31%, is organisations with 1,000 to 4,999 employees.

Size of organisation (number of employees)



Base: all respondents (n=412). Organisations with 1–9, 10–99 and 100–249 employees are combined as "Under 250". Percentages are rounded to the nearest whole number.

91% of respondents indicated they work for organisations with a Data Protection Officer (DPO).

This organisational profile is likely to reflect where dedicated data protection roles are found. Larger organisations are more likely to employ a DPO or a data protection team and are also more likely to receive higher volumes of DSARs, particularly from employees.

The findings therefore lean towards the experience of medium and large organisations. That said, smaller organisations still make up almost one in five respondents (19%), a meaningful group in their own right.

Findings

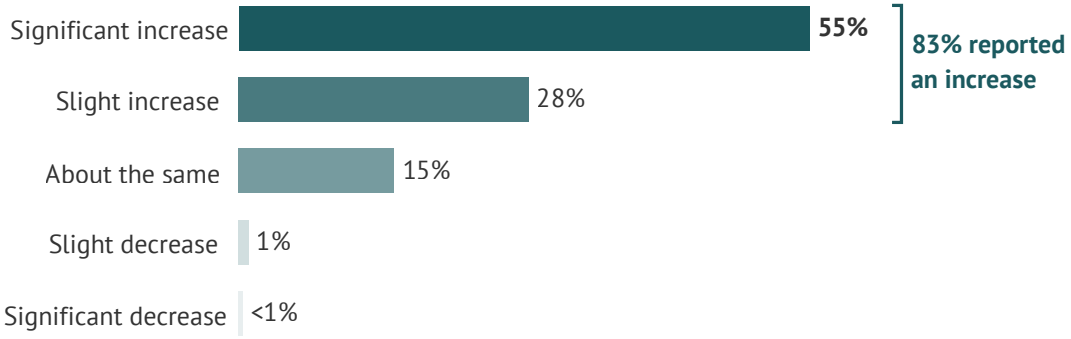
A: Volume, nature and complexity

Volume change in past 12 months

Respondents were asked how many DSARs their organisation had received in the previous 12 months. Over two-fifths (41%) reported receiving more than 100 requests.

When asked how the volume of requests compared with the preceding year, a large majority (83%) reported an increase in volume, and more than half (55%) described the increase as significant.

Change in volume of DSARs compared with the previous year



Base: all respondents (n=412). Percentages are rounded to the nearest whole number.

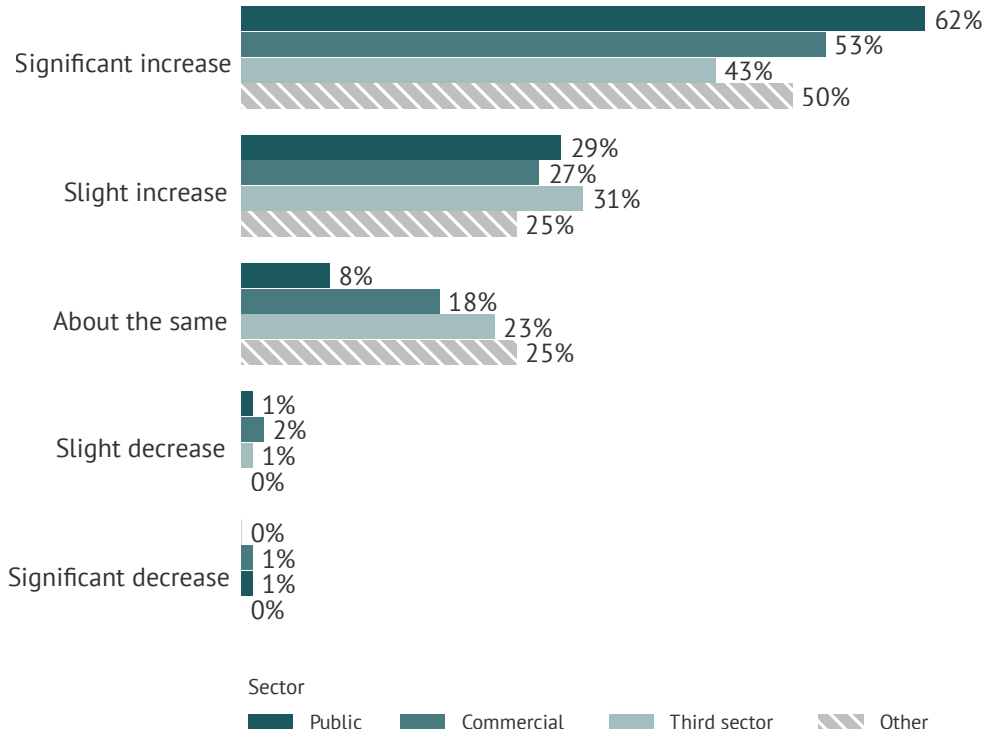
Change in volume by sector

While most respondents reported an increase in requests, their experience varies noticeably by sector.

- **The public sector** has been hit hardest. More than nine in ten public sector respondents (91%) reported an increase, and 62% described it as significant, compared with 55% across all respondents. Only 8% said volumes had stayed about the same.
- **The commercial sector** is closer to the overall picture. Four in five respondents (80%) reported an increase, with just over half (53%) describing it as significant.
- **Third sector** organisations have seen a less dramatic rise, although the trend is still upwards. Almost three-quarters (74%) reported an increase, fewer than half (43%) said it was significant, and almost a quarter (23%) said volumes were about the same.

Decreases in access requests were rare in every sector, at no more than 3% in any group.

Change in volume of DSARs compared with the previous year, by sector

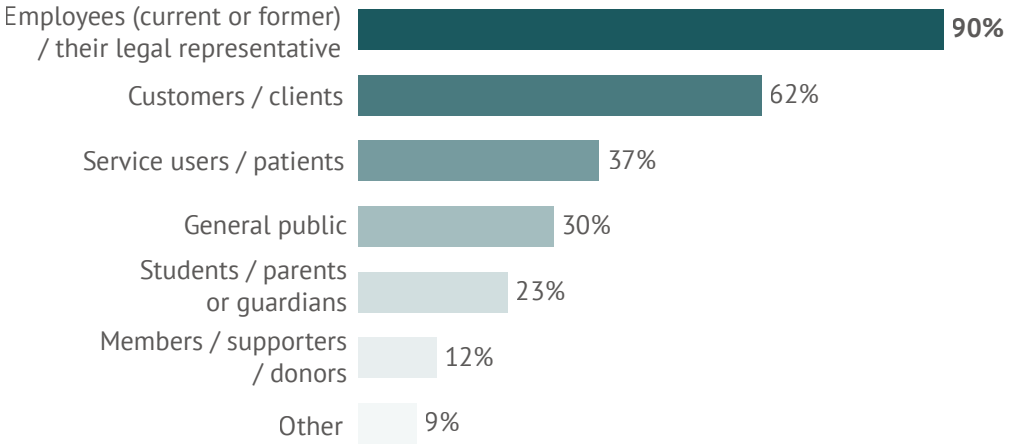


Base: all respondents (n=412). 'Other' is a small group, so its results are indicative only. Percentages are rounded. Differences between sectors are statistically significant (p=0.004), driven mainly by the difference between the public and third sectors.

Who submits requests?

Current or former employees were by far the most common source of requests, cited by nine in ten respondents (90%), followed by customers or clients (62%).

Who organisations receive DSARs from



Base: all respondents (n=412). Respondents could select more than one option, so totals exceed 100%.

Requesters by sector

Unsurprising, each sector has its own distinct mix of requesters.

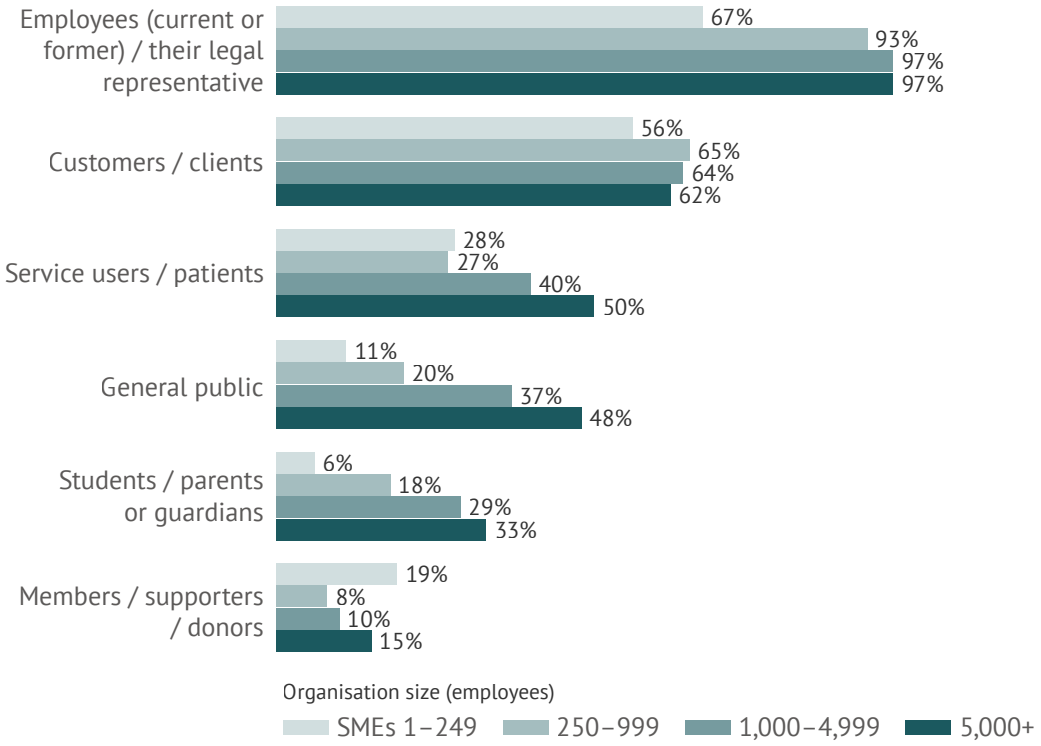
- **Employees** (current/former) are a common source of requests in all sectors (83 to 96%), and most common in the public sector. In addition to this:
- **Commercial organisations** receive most of their requests from customers and clients (84%). Relatively few come from service users (16%) or the general public (21%).
- **The public sector** has the widest range of requesters, receiving requests from service users or patients (54%), students and parents (48%) and the general public (46%).
- **The third sector** is unsurprisingly the only sector with requests from members, supporters and donors (36%), alongside service users (43%).

Due to the limitations of this research, respondents may not be representative of all organisations handling DSARs. For example, organisations which receive requests from patients or students/parents may be under-represented.

Requesters by size of organisation

Employee-related requests are the most common type of DSARs for organisations of 250 or more employees, where 93% or more receive them. Among SMEs, the figure is 67%. Larger organisations receive requests for a wider range of people. Customers and clients are a steady source at every size. SMEs are the most likely to get requests from members, supporters and donors; it's likely this reflects smaller charities and membership bodies in this group.

Who organisations receive DSARs from, by organisation size



Percentage of respondents in each size band. Respondents could select more than one option, so totals exceed 100%. 'Other' not shown.

Source of increase in requests

Respondents were asked if they'd seen an increase in requests from a certain group of people. Of the 69% who answered this question, employees (current and former) were by far the most frequently cited group, named by almost half of respondents (46%).

This was more than three times as many as the next most common groups: customers and clients (14%) and complainants or individuals dissatisfied with an outcome (11%). Many respondents linked the rise in employee requests to grievances, disciplinary proceedings, dismissals or redundancy programmes.



Word cloud based on most common words in free text responses

Groups most often named as the source of an increase in requests

Group	%
Employees and former employees	46%
Customers and clients	14%
Complainants and people dissatisfied with an outcome	11%
Service users and members of the public	7%
Students and former students	6%
Solicitors, CMCs and other representatives	4%
Job applicants and candidates	3%
Tenants and residents	2%
Patients	2%
Parents	2%

Base: respondents who answered the question (n=283). Top 10 groups shown. Respondents could name more than one group, so the percentages are not expected to sum to 100%. Percentages are rounded to the nearest whole number.

A common theme was that requests are increasingly raised alongside a dispute, whether an employment related matter, an unsatisfactory complaint outcome or a legal claim. Some respondents noted in their free text responses requests are being made by solicitors or claims management companies.

However, not all organisations had seen a change: 16% report no increase from any particular group, and a further 10% describe a general increase across all groups.

In DPN's experience, and from discussions with other data protection professionals, the "weaponisation" of DSARs in employment disputes has been common for several years. What's new, according to our research, is that current and former employees now submit more requests than any other group, by a clear margin.

The survey did not ask respondents to identify education as a sector. Those who mentioned in free text comments they worked in schools and education establishments highlighted rising requests from parents, often linked to wider complaints, or to children with special educational needs. Their experience may be more common than our findings suggest. Further research focused on the education sector could help establish whether this is a wider trend.

For free text analysis methodology see Appendix 1

Claire Archibald, Legal Director at Browne Jacobson comments:

"Like other sectors, education has seen a significant rise in SARs, particularly employment-related requests and those from parents raising complaints. In my experience, schools can make this harder for themselves than it needs to be. Clear, well-maintained records management systems, and regular information sharing with stakeholders, so they never need to make a SAR, especially for pupils with SEND, are essential to responding efficiently."

AI-generated requests

92% of respondents said they were receiving requests likely to be generated by AI, more than half described this as a significant proportion of requests.

Are you receiving requests likely to be AI-generated?



Base: all respondents (n=412). Percentages are rounded to the nearest whole number. Combined figures, such as the bracketed total, are calculated from the underlying data and may differ by one point from the sum of the rounded figures.

While this research cannot definitively establish the use of AI is responsible for an increase in requests, the free-text responses suggest it is a major driver, alongside the growing use of DSARs in connection with employment disputes and complaints.

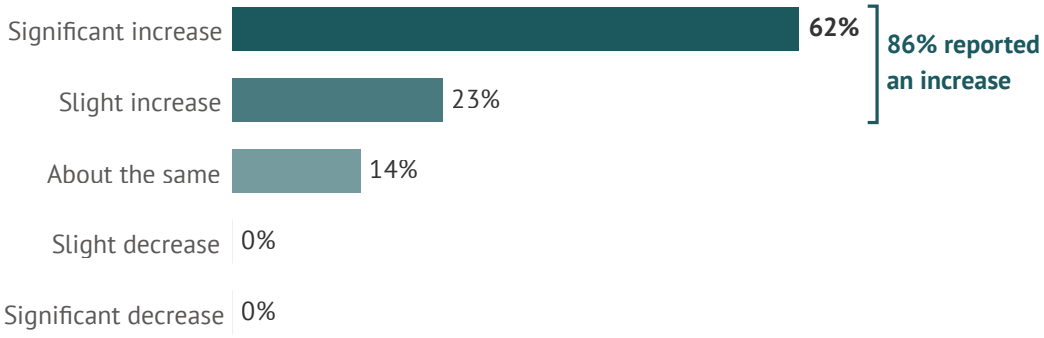
This mirrors a wider trend of AI-drafted correspondence increasingly being reported across many other activities, such as; complaints, consumer claims, job applications and correspondence with public bodies.

Also see Impact of AI-generated requests

Complexity of requests

Respondents were asked how request complexity had changed over the past 12 months. "Complexity" was not defined and was left to respondents' interpretation. Overall, 86% reported an increase, including 62% who described it as significant.

How has the complexity of requests changed in the past 12 months?

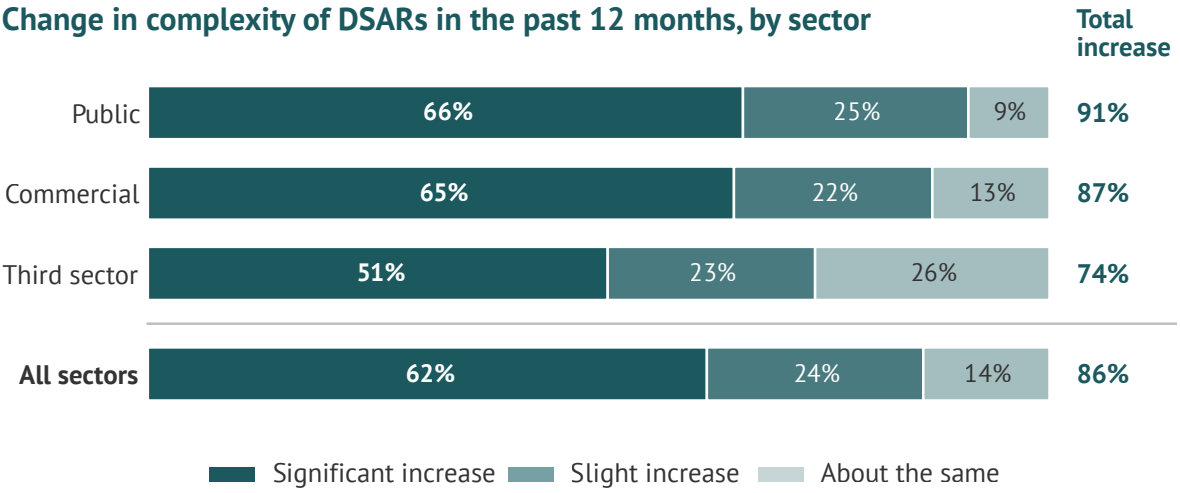


Base: all respondents (n=412). Percentages are rounded to the nearest whole number. Combined figures, such as bracketed totals, are calculated from the underlying counts and may differ by one percentage point from the sum of the rounded figures.

Complexity by sector

Complexity has risen most sharply in the public and commercial sectors, where around two-thirds reported a significant increase, compared with half (51%) in the third sector. No respondents reported a decrease.

Change in complexity of DSARs in the past 12 months, by sector



Base: all respondents (=412). "All sectors" also includes a small number of respondents from other sectors, not shown separately. Percentages are rounded; totals are the sum of the two increase figures.

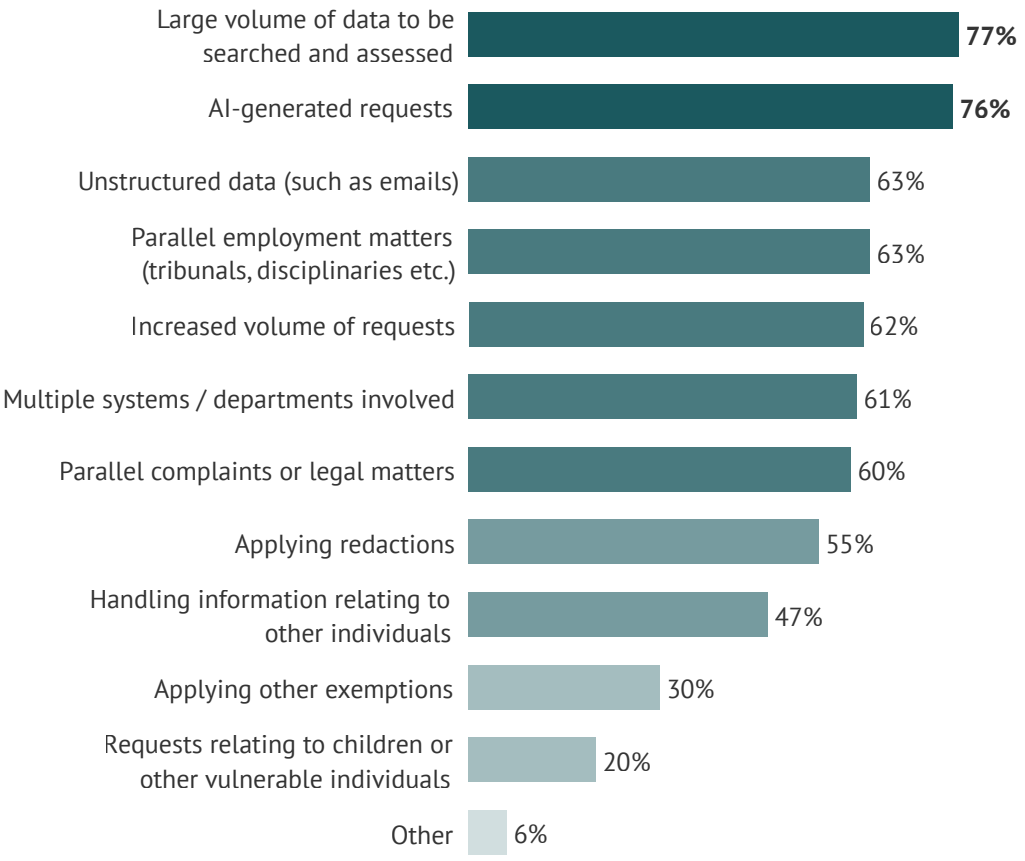
Factors making requests tricky to process

Respondents were asked to identify the main factors making requests 'tricky' to process, and could select more than one option. The two most frequently selected options were large volume of data to be searched and assessed (77%) and AI-generated requests (76%); each were selected by more than three-quarters of respondents.

A second group of factors was selected by around three in five respondents: unstructured data such as emails (63%), parallel employment matters such as tribunals and disciplinaries (63%), the increased volume of requests (62%), the involvement of multiple systems or departments (61%) and parallel complaints or legal matters (60%).

More than half (55%) identified applying redactions as a challenge, and almost half (47%) cited handling information relating to other individuals. Fewer respondents identified applying other exemptions (30%) or requests relating to children or other vulnerable individuals (20%) as key difficulties.

Main factors that make requests tricky to process



Base: all respondents (n=412). Respondents could select more than one option, so totals exceed 100%. Percentages are rounded to the nearest whole number.

Rising complexity and challenges

The findings point to AI adoption as one of the main drivers of growing complexity. This matches our own experience and what we are hearing from other data protection practitioners.

AI is not the only factor. Employee-related requests stand out as particularly complex to handle. Respondents' free-text comments describe employee requests often arriving alongside employment proceedings. Requests are described as "very complex", with requesters frequently wanting "everything" and being unwilling to narrow the scope. One respondent described a request from a long-serving employee where "the IT pulls from emails alone amounted to over 125GB of data". Reviewing large volumes of emails and messages which concern colleagues and other parties adds further time and requires specialist skills, e.g. to apply redactions.

Respondents also describe employees using AI tools to draft their requests, producing wide-ranging, legally framed demands. When AI-generated requests combine with an employment dispute, they can be among the most demanding requests organisations handle.

The findings suggest the challenges of fulfilling requests are perhaps less driven by the legal complexity of exemptions and more by the scale of data to be searched and reviewed, along with the context in which requests are made. Fewer than a third of respondents (30%) cited applying exemptions as a factor, compared with over three-quarters citing data volumes and AI-generated requests.

Respondents may not be representative of all organisations handling DSARs. For example, organisations in the education sector, which receive requests relating to children, may be under-represented. 20% of all respondents cited requests relating to children or other vulnerable individuals as a factor. Anecdotally DPN is aware DSARs are having a significant impact on schools.

Claire Archibald, Legal Director at Browne Jacobson comments:

"A particular challenge in education is that parents do not always exercise data subject rights genuinely in a child's best interests. It is a data subject right, not a parental one, yet many treat it as such. We see DSARs used in private family disputes with one parent attempting to get information about the other.

The application of safeguarding exemptions adds a further complexity; schools must carefully navigate whether disclosure could place a child at risk, while managing significant pressure from parents who may be determined to obtain information. Schools can find themselves caught in the middle of deeply difficult situations, with real consequences for the children involved."

B: Impact of DSARs on the organisations receiving them

Impact of AI-generated requests

Respondents were asked to share the impact AI-generated requests were having, either negative or positive. 88% answered this question.

In their own words: the impact of AI-generated requests

AI generated requests tend to be enormous, spanning multiple pages unnecessarily	*It is hard to determine exactly what information they are asking for*
Waste of time and resources unpicking requests	*Lengthy and cannot reason with the requestor and they believe AI is set in stone*
Senseless requests, incorrect assertions, extremely lengthy	*Data subjects become convinced that the AI slop is gospel and will argue until they are blue in the face that the AI is right*
We keep receiving lengthy follow-up requests generated by AI, asking for more data, including threats of making regulatory complaints and/or letters before claim	*Recently received a 21-page email request which was repetitive, demanding and confusing*
...they feel like a technical and legal minefield	*Most of the time the requester will run our clarifying email through an AI chat tool and ask it to respond, often presenting arguments against clarifying, then we end up stuck in a loop with the requester*

Most frequently cited themes in the free-text responses

- **The impact is overwhelmingly negative.** 86% described only negative effects. Less than 5% gave a mixed picture, and just one respondent described a purely positive impact. 6% saw little or no impact, and 3% answered 'N/A' or hadn't had an AI request.
- **The most common problem is simply getting through the request.** Nearly half of respondents describe AI requests as long and hard to understand.
- **What the requests ask for is often wrong.** 23% report inaccurate or misapplied law, including wrong timescales, foreign laws and invented regulation. 21% report requests for information which isn't personal data or isn't held. Metadata alone is mentioned in 34 responses, often with audit logs and system logs.
- **The work doesn't stop when the response goes out.** 23% describe AI-drafted follow-ups, challenges and complaints, sometimes within minutes of disclosure. 24% say AI gives requesters unrealistic expectations. 18% say clarification has become harder, with some caught in an 'AI loop'.
- **5% mention some positives.** Some mention that it's positive AI is raising awareness of the right of access. Others say AI can make some requests clearer or more structured. A couple of respondents said it has pushed their organisation to tighten its procedures.

Top 10 impacts of AI-generated requests

Impact	%
Long, verbose and hard to decipher	47%
Extra workload, time and resource strain	32%
Over-broad scope: 'everything' and more than they need	30%
Unrealistic expectations and requesters who don't understand their request	24%
Inaccurate or misapplied law	23%
AI-generated follow-ups, challenges and complaints	23%
Requests for non-personal data or data not held	21%
Clarification is harder and can become an 'AI loop'	18%
Aggressive tone and impact on staff wellbeing	6%
Linked to disputes, complaints and compensation	6%

Base: respondents who answered the question (n=361). Top 10 impacts shown. Respondents could describe more than one impact, so the percentages are not expected to sum to 100%. Percentages are rounded to the nearest whole number.

For free text analysis methodology see Appendix 1

Impact on teams and organisation

Respondents were asked to share the impact DSARs are having on their work, their team/ department and/or their organisation. 87% respondents provided a free text answer.

In their own words: the impact of DSARs

Taking the majority of our time	*Crushing*	*Individuals are facing real burnout from repeat AI requests*
Causing backlogs in other areas and causing stress to staff	*The DSAR workstream is relentless*	*...take up a disproportionate amount of time*
...small team working long hours and under stress to meet deadlines	*Exhausting*	*The increase is taking staff away from other duties, and causing frustration*
...causing stress and sickness in the team	*...impact on mental and physical health as it has been nothing short of a deluge*	*...we can't spend time on other privacy issues*
...increasingly unsustainable demand	*We are constantly fire fighting*	*...it can easily derail other projects*
The sheer volume is disheartening	*Overwhelming the team*	*...getting behind on many requests due to size, number and complexity*

Top 10 impacts on team and organisation

Before reading on, it should be noted respondents had previously been invited to share free text comments on the impact of requests likely to be AI-generated and the factors causing requests to be tricky to process. This may have made them less likely to repeat points already made. In DPN's opinion, "AI increasing volume and complexity" (shown as point 9 in the top 10 below) may otherwise have appeared much higher up the order.

1. **Major increase in workload**
   Requests are described as time-consuming, relentless, dominant or a "conveyor belt," often requiring days or weeks of work per complex case.
2. **Loss of capacity for other data protection work**
   Respondents report less time for Data Protection Impact Assessments (DPIAs), providing privacy advice, training, governance, data breach management, privacy notices and proactive risk management.
3. **Pressure on individuals and small teams**
   Where there is a sole person responsible, or a very small team, a single complex request can pause almost all other work.
4. **Cost of additional resources**
   Respondents report new dedicated roles, overtime, temporary support, outsourcing, legal advice, redaction tools and additional IT capacity.
5. **Staff stress, burnout and morale problems**
   The workload, statutory deadlines, difficult requesters and repeated challenges can result in stress, sickness and low morale.
6. **Difficulty meeting deadlines and rising backlogs**
   Respondents say extensions are more common, responses are routinely late and/or backlogs are growing.
7. **Burden created by broad, unclear or "all data" requests**
   Respondents highlight extensive searches across email, messaging services, archives and multiple systems, followed by lengthy review and redaction.
8. **Complaints and post-response challenges**
   Substantial follow-up work is reported responding to dissatisfaction, disputes about redactions, further requests and complaints.
9. **AI increasing volume and complexity***
   AI-generated requests are seen as broader and more demanding, while AI is also used by requesters to challenge the response they received, sometimes quickly and repeatedly.
10. **Operational teams pulled away from core services**
    HR, IT, clinical, social-care, education and customer-service teams spend time locating, reviewing and redacting records instead of their main roles.

This research strongly indicates DSARs have shifted from being an occasional compliance task to a major, often unpredictable workload. Respondents described requests as relentless and all-consuming. Other data protection compliance tasks are being pushed to the side, and requests pull in colleagues from other departments, taking them away from their day jobs. In DPN's opinion, it's very likely a disproportionate amount of time is being spent handling this single aspect of data protection compliance. It isn't surprising deadlines are slipping and backlogs are growing, and it's disheartening to hear how DSARs are causing stress and impacting on morale.

For free text analysis methodology see Appendix 1

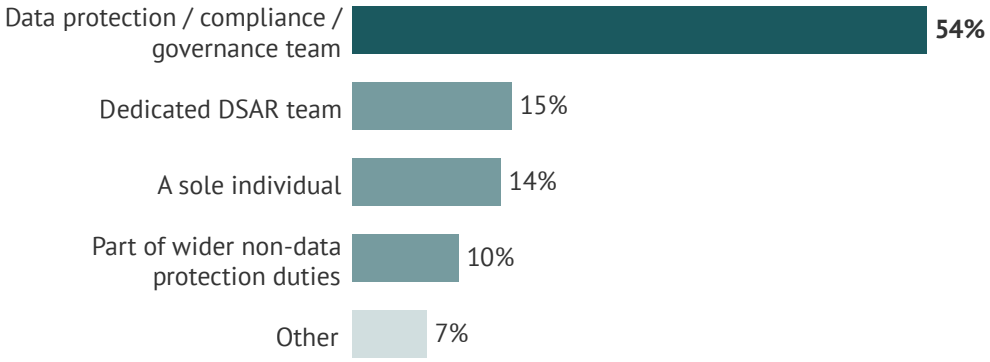
C: Resourcing, handling and performance

Resourcing

Respondents were asked how the management of DSARs is resourced in their organisation. In more than half of organisations (54%), responsibility rests with a data protection, compliance or governance team. Only 15% have a dedicated DSAR team.

Taken together, around a quarter of respondents (24%) rely on either one person, or staff for whom data protection is not their main role. This may leave these organisations particularly exposed to the rising volume and complexity of requests reported elsewhere in this survey.

How DSAR management is resourced

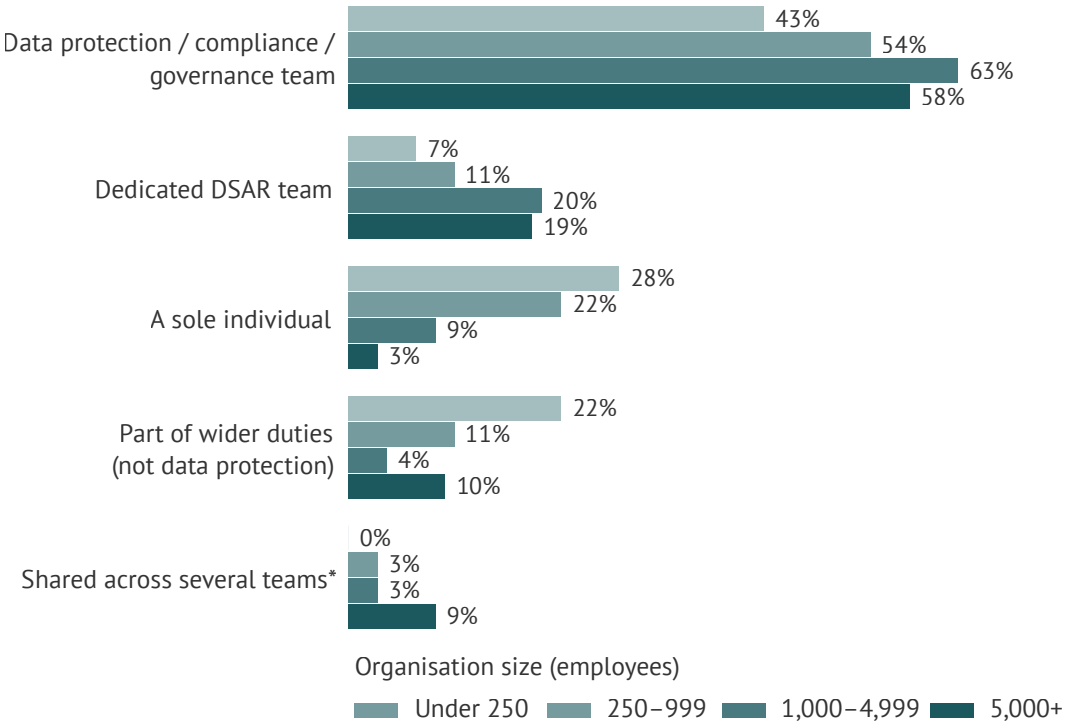


Base: all respondents (n=412). Percentages are rounded to the nearest whole number and may not total exactly 100%.

Resourcing by size of organisation

- **A data protection, compliance or governance team is the most common model at every size** (56% overall). It peaks at 63% among organisations with 1,000–4,999 employees.
- **Management of DSARs within SMEs depends heavily on individuals:**
  - Half of SMEs (50%) have a single person responsible (28%) or handle DSARs as part of wider duties unrelated to data protection (22%).
  - In organisations of 1,000 or more, this falls to around 13%.
  - Unsurprisingly, having a sole individual responsible drops steadily with organisation.
- **Dedicated DSAR teams appear most frequently in organisations of 1,000 or more** (about 20%)

How the management of DSARs is resourced, by organisation size



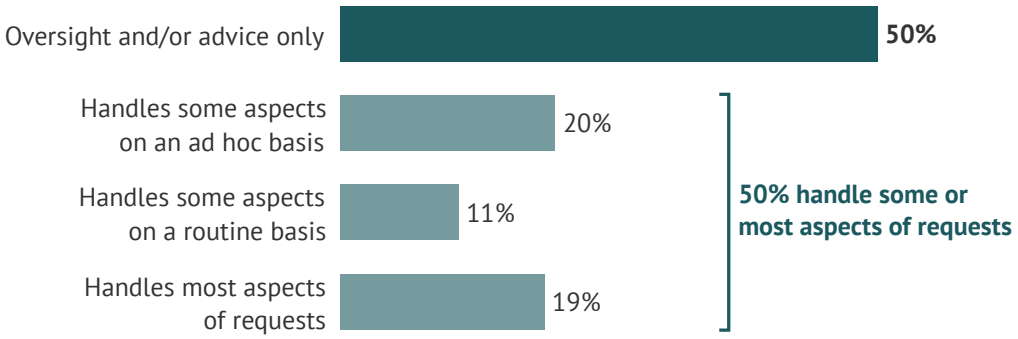
*Base: 412 respondents. Single-choice question, so each size group adds to 100%. *Coded from 'Other' answers describing responsibility shared across several teams or departments. Percentages are rounded to the nearest whole number.*

Role of DPO

Almost two in five respondents (39%) are themselves a DPO or Privacy Officer. Most respondents (92%) said their organisation has a Data Protection Officer, and these respondents were asked what role the DPO plays in handling DSARs.

Responses were evenly split. Half said the DPO provides oversight and/or advice only in relation to DSARs. The other half said the DPO is directly involved in handling requests: 20% handle some aspects on an ad hoc basis, 11% handle some aspects on a routine basis, and almost one in five (19%) handle most aspects of requests.

Role the DPO plays in DSAR



Base: respondents who answered the question (n=378). Percentages are rounded to the nearest whole number.

This hands-on involvement raises concerns DPOs are being drawn away from their other core duties. Under the UK GDPR, the DPO's role is clearly defined: to inform and advise the organisation, to monitor compliance, and to act as a point of contact for the regulator. Where DPOs routinely handle requests themselves, the time involved may limit their capacity to carry out these core tasks.

In free text comments, some DPOs described spending the majority of their time on DSARs, with one estimating as much as 90%. Others said strategic and proactive work, such as Data Protection Impact Assessments (DPIAs), policy updates, training and privacy-by-design advice, had been delayed or set aside.

Extending timescale

Respondents were asked how frequently they need to extend the timeframe for responding to requests due to complexity. Almost two-thirds (64%) said they need to do so often (25%) or sometimes (40%). A further 28% said they rarely extend, and only 8% said they never need to.

Respondents who extend deadlines were then asked how confident they are that these extensions are justified. Just over half (58%) said they were confident and a third (33%) said they were only somewhat confident, while 7% said they were not confident.

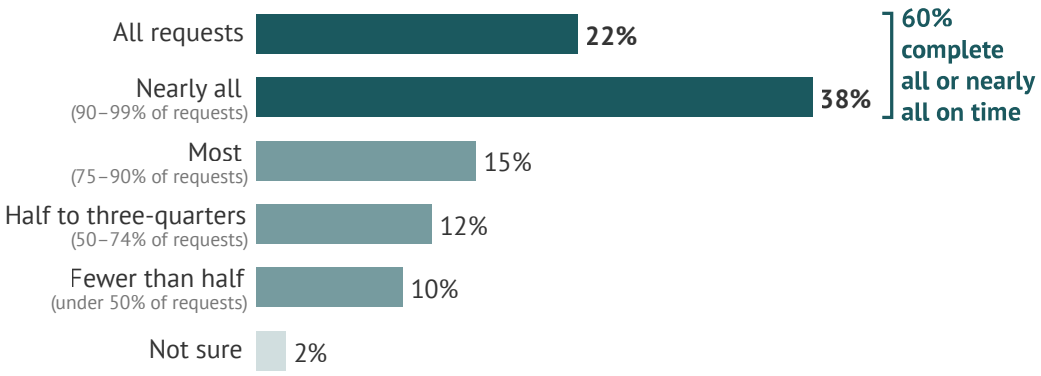
The findings suggest extending the timeframe beyond the one calendar month is now a routine part of handling requests for many organisations. A significant minority of respondents are not sure their use of an extension would hold up to scrutiny. This is consistent with free-text responses calling for clearer guidance on what constitutes a 'complex' requests, and whether factors such as the time needed for redaction can justify an extension.

Meeting the deadline

Respondents were asked what percentage of requests were being completed within the one-month deadline (unless an extension had been applied). Three in five respondents (60%) said they complete all or nearly all requests within the one-month deadline, including 22% who complete every request on time. However, more than one in five (22%) complete fewer than three-quarters of requests on time, and one in ten (10%) complete fewer than half.

How many requests are completed within the one-month deadline?

Percentage of respondents



Excluding requests where an extension has been applied. Base: all respondents (n=412). Percentages are rounded to the nearest whole number.

The results present a mixed picture. On a positive note, most organisations are meeting the statutory deadline for the majority of requests. Free-text responses suggest this is often achieved at considerable cost: respondents described working long hours and weekends, putting other data protection work on hold, and redeploying staff to meet deadlines.

However, 40% are not completing at least 90% of requests on time, and more than one in five complete fewer than three-quarters within the deadline.

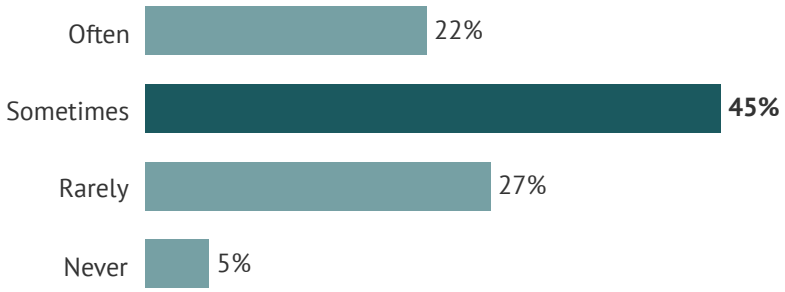
These figures are likely to understate the pressure on organisations, as they exclude requests where the deadline has been extended. Almost two-thirds of respondents are extending often or sometimes due to complexity, this means a significant proportion of requests are taking longer than one month to complete.

These findings taken together suggest the one-month timeframe is proving increasingly difficult for many organisations to meet. This is reflected in free text calls for longer or more flexible response times. *Also see Views on legislative change*

Dissatisfaction and complaints

Respondents were asked how frequently requesters reply to say they are not satisfied with the response to their DSAR. 22% say this happens often, while 45% say this happens sometimes. A further 27% say it happens rarely, and only 5% say it never happens.

How often requesters say they are not satisfied with the DSAR response



Percentage of respondents (n=412). Figures do not sum to 100% due to rounding.

Complaint escalation

Respondents were also asked whether they had received correspondence from the ICO about DSAR complaints raised with the regulator in the past 12 months. Almost three in ten (29%) said they had, 68% had not, and 3% were unsure.

Dissatisfied requesters

The findings suggest it's not uncommon for those submitting DSARs to be dissatisfied with the response they get. Free text responses indicate some factors which may contribute to this dissatisfaction, such as;

- Requesters having expectations which go beyond the scope of the right of access, particularly where requests have been drafted using AI.
- Using DSARs alongside a wider complaint or dispute, where the disclosure doesn't resolve the underlying issue.
- AI being used to generate rapid challenges to responses, sometimes within minutes of disclosure.

Handling this dissatisfaction places a further burden on already stretched teams. Several respondents noted where complaints reach the ICO, their original response is frequently upheld.

It should be noted these findings represent the views of those receiving requests and offer no insight into the experience of those submitting them.

The new data protection complaints process

Since 19 June 2026, organisations have been required to have a data protection complaints process. This survey was conducted around three months after this requirement came into force. While respondents were not asked about it directly, some raised this in free text responses, and their comments suggest it may already be adding to the workload associated with DSARs.

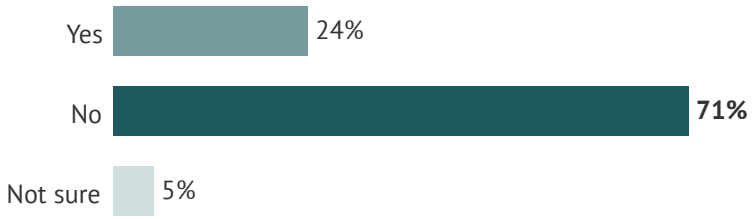
Some respondents described the complaints route as an additional stage requests now commonly pass through. One expected the new requirement to "likely double the load", and another anticipated some requesters would routinely lodge both a service complaint and a data protection complaint. Others reported a rise in AI-generated data protection complaints following DSAR responses since June, and described requests being handled two or three times over as they moved through internal complaints and then to the ICO.

It's widely believed the new complaints process was introduced to ease the burden on the ICO. It means in most circumstances the ICO is likely to expect individuals to go through an organisation's complaints process first. It's too early at this stage to assess the impact of this change but some respondents' comments suggest it may, in practice, increase the burden on already over-stretched teams and extend the lifecycle of requests.

Use of DSAR tools

Respondents were asked whether they use purpose-built tools to manage all or most of the DSAR lifecycle. Fewer than a quarter (24%) said they do. The large majority (71%) do not, and a further 5% were unsure.

Use of purpose-built tools to manage the DSAR lifecycle



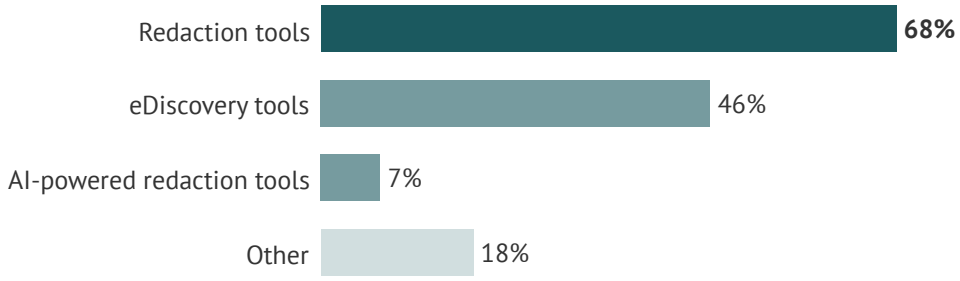
Percentage of respondents (n=412). Percentages are rounded to the nearest whole number.

Unsurprisingly, further analysis of organisation size found those with 250 or more employees are around three times as likely to use a purpose-built tool than smaller organisations, rising to 36% among those with 5,000 or more employees.

Respondents were asked to indicate which tools they used to assist with requests. Redaction tools are by far the most widely used, with more than two-thirds of respondents (68%) using them to help with requests. Almost half (46%) use eDiscovery tools to help search for and gather information across systems. AI-powered redaction tools remain rare, used by only 7% of respondents.

Almost one in five respondents (18%) selected "Other". Around four in five of these said they use no dedicated tools at all. They rely on manual processes or standard PDF software such as Adobe Acrobat.

Tools used to assist with requests



Base: all respondents (n=412). Respondents could select more than one option, so totals exceed 100%.

Mark Roebuck, Founder of ProvePrivacy comments:

"This research confirms what we see in practice: as request volumes and complexity rise, manual processes and spreadsheets are becoming unsustainable for many teams. It's striking that fewer than a quarter of organisations use purpose-built tools to manage DSARs, and only 7% use AI-powered redaction. Giving teams the right tools to handle requests can significantly improve the efficiency of the process and get the time back for other data protection work."

The findings suggest most organisations manage requests using manual processes or general-purpose systems, such as system-specific searches, spreadsheets and document software, rather than using dedicated case management solutions. Where tools are used, they tend to be to assist with specific stages of the process, such as redaction, rather than to manage the request from start to finish.

SMEs are the least likely to use purpose-built tools (just 9%) and are most often reliant on one person or on staff with other duties. This leaves them particularly exposed. Although larger organisations are likely to be experiencing the challenge of substantially higher volumes.

Use of external DSAR services

Respondents were asked whether they ever use an external DSAR service to support them in handling requests. The large majority (77%) do not. Around one in seven (14%) do: 12% use an external service for part of a request, and only 2% for the whole request. A further 9% are considering doing so.

The respondents who use an external service were asked how often they rely on it. More than half (55%) use it from time to time, and 22% have done so only once or twice. Fewer than a quarter (23%) rely on an external service for most requests.

Those which use external services mostly do so to add capacity and get the tools to handle large, email-heavy and often employee-related requests. A smaller number of respondents use them for expert advice on complex or legally sensitive cases, or to be seen as impartial. Most respondents describe outsourcing as something they turn to when demand exceeds what the internal team can handle.

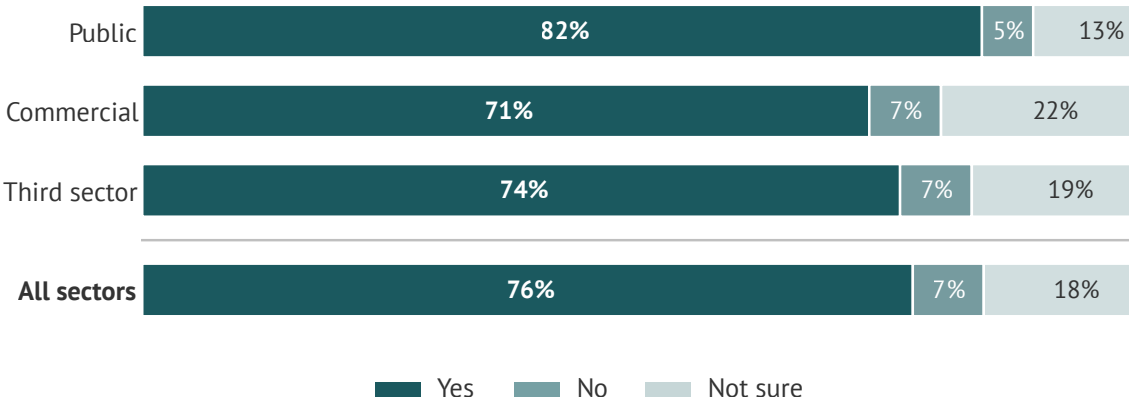
D: Views on legislative change

Views on changing the law

Respondents were asked if the law should change to reduce the burden of requests on organisations. The answer was clear. Three in four (76%) said 'Yes', and only 7% said 'No', so those in favour of change outnumber opposers by more than ten to one. Those working in the public sector were most strongly in favour of change.

A further 18% were not sure. This may reflect uncertainty about what form any change should take.

Should the law be changed to reduce the burden of DSARs? By sector



Base: 412 respondents. "All sectors" also includes a small number of respondents from other sectors, not shown separately. Percentages are rounded, so some rows may not add to exactly 100%.

These findings are noteworthy given the timing. Changes to UK GDPR introduced by the Data (Use and Access) Act 2025 have only recently come into effect. These put "reasonable and proportionate searches" and "stopping the clock" on a statutory footing. The findings suggest those on the ground handling or overseeing requests do not feel these changes go far enough to ease the pressures described elsewhere in this report.

What respondents would change

Respondents who indicated they'd like to see a change in the law were asked what single legislative change they'd like to see. Two thirds (67%) answered this question, with most raising more than one point. The following comments are indicative of those we received.

In their own words: what respondents would change

Remove the blanket right of access. A data subject must specify precisely what they want and not 'everything you hold about me'	*A clear definition, with examples, of what constitutes a 'reasonable and proportionate' search*
...they need to be purposeful and not able to request everything	*More guidance from the ICO on what is reasonable and proportionate*
Something about 'acceptable limits' for requests, similar to Freedom of Information Act requests	*Decrease the threshold for requests to be deemed manifestly unfounded or excessive*
...define threshold for both manifestly excessive and unfounded - particularly excessive	*Extension to the deadline - one calendar month as standard is not feasible*
Time limits like FOI	*Re-introduce fees but caveated with being affordable*
Given the recent increase in AI-generated DSARs, I think it would be sensible to reintroduce a reasonable fee for DSARs that require extensive searches	*Not allow DSARs to be made if there is an ongoing complaint/legal dispute or employment matter. In these circumstances DSARs are being weaponised with individuals asking for years of irrelevant data*
The deadline for response should be longer than one month	*Stop the use of AI with a request*
Stop it being a fishing expedition in disciplinaries etc - they should get the info they require through that route	*There should be more (simple) guidance for individuals to understand what they are entitled to*
I'd tighten up the definition of structured vs unstructured data to limit structured data to personal data held in databases, e.g. our HR systems, where the vast majority of personal data and official records are held; and exclude the need to even search emails and messages	*I would exclude email or other unstructured data. We should only be required to disclose the personal data that has been collected for a specific purpose*

The free-text answers point to one dominant message: respondents broadly support the right of access but want the law to make requests more targeted, proportionate and manageable.

Changes to the law respondents would like to see

Theme	Approx. share	What respondents want
Narrower, more specific requests	40%	Require requesters to identify the information, topic, date range, system or purpose sought; prevent blanket "everything you hold about me" requests
Proportionality and reasonable-search limits	25%	A clearer statutory test for "reasonable and proportionate" searches, with FOI-style limits on effort, volume or records reviewed
Easier refusal of excessive or unfounded requests	22%	Lower or clarify the "manifestly unfounded or excessive" threshold; give controllers more confidence to refuse speculative, abusive or disproportionate requests
Reintroduce fees	20%	A nominal or scaled fee, often likened to the former £10 charge, to deter "fishing" requests, usually with suggested exemptions for vulnerable people or simple requests
Longer response period	20%	Extend the one-month deadline, commonly to two or three months, particularly for complex, high volume or redaction-heavy cases
Employment disputes and litigation	16%	Exclude, pause or restrict DSARs used alongside grievances, disciplinaries, tribunal claims or other disputes; respondents see DSARs being used as an early disclosure tool
Clearer definitions and guidance	13%	Define personal data, "copy", reasonable search, third-party data and exemptions more clearly; several want simpler ICO guidance for requesters as much as legal change
AI-generated requests	11%	Regulate, require human verification of, narrow or in some cases refuse AI-generated requests; respondents link these to overly broad requests and low requester engagement
Limits on repeat requests	8%	Cap the number of DSARs per person per year, or prevent repeated requests for the same material
Narrower treatment of emails and informal communications	8%	Exclude or limit emails, messages, metadata, system logs and other unstructured data, or focus disclosure on records about the individual rather than every mention of their name

Base: respondents who answered the question (n=275). Shares are approximate. Answers could be coded to more than one theme, so the percentages are not expected to sum to 100%.

Sarah Howers, Privacy Business Partner at a global technology company, comments:

"It's been very reassuring to know that so many of the wider privacy community is experiencing the same challenges, and to be able to see if there's better ways of responding to this tsunami of requests and increased complaints. It would be fabulous if this research could help to drive conversations with our Regulator to improve guidance and confirm some guardrails to assist with managing data subjects' expectations."

Stephen McCartney, Independent consultant, former DPO in fintech and edtech sectors, comments:

"This report makes it clear that those who work in data protection still value and want to protect the individual's right to access their information. But it should be a wake up call that so many data protection professionals think the balance of rights has tipped too far."

Data protection professionals don't always agree on which changes would be most effective, A fee, for example, might deter speculative requests but could create a barrier for genuine requesters. The suggestion of a fee for more complex requests, might be more palatable.

No single change is likely to transform the picture. Any potential reform would need to balance the concerns raised in this report with what's still regarded as an important individual right. Some improvements may not need legislative change. Respondents' comments point to several areas where clearer guidance and better awareness could make a difference:

- **Clearer guidance on "reasonable and proportionate searches"** with examples of what this means in practice could help organisations apply this with more confidence.
- **Increased clarity on what makes a request "complex"** could provide more certainty about when the deadline can be extended.
- **Promoting greater public awareness of what the right of access is (and what it is not)** could lead to more focused requests and fewer disputes about the outcome.
- **Discouraging the use of DSARs as a tactic in employment disputes** by employees and their legal representatives, and clear messaging the right of access is not intended as a substitute for the disclosure process could potentially help reduce this pressure.

One of the key challenges is how nuanced compliance with the legal requirements and regulator guidance can be. Responding to requests requires specialist knowledge, skills and good judgement. Many decisions have to be made case-by-case, often under time pressure, and with the prospect of a possible complaint or legal challenge.

It may be unrealistic to expect everyone involved to have the depth of knowledge the current framework requires; especially SMEs.

If the volume and complexity of requests stay at current levels, or continue to rise, there's a risk the gap between what the law requires and what organisations can realistically deliver will widen further. A combination of targeted changes to the law, practical guidance, and a drive to promote greater public understanding could ease the burden and result in better outcomes for individuals.

For free text analysis see Appendix 1

E: Additional respondent comments

A third of respondents completed a final free text box, which invited them to share any other points not covered in the survey. 134 made a substantive comment; the rest had nothing to add or thanked us for the survey. Because the question was open, comments range widely, and many wished to reinforce themes from earlier questions.

- Calls for change dominate: 27% reiterate proposed changes to the law.
- The ICO is a target for criticism: 10% criticise the regulator as inconsistent, unhelpful or out of touch with the pressure on organisations. One describes the complaints process as a 'doom loop'.
- AI concerns: A fifth mention AI again and describe DSARs used for fishing, leverage in disputes or simply to cause inconvenience.
- Resource pressure and its human cost come through strongly again: 16% describe budget and staffing pressure or a lack of affordable tools. Others reiterate the emotional toll and say senior management doesn't recognise the burden they are under.
- 6% make a point of calling for the right to be protected. Some say motive is irrelevant and AI is a legitimate accessibility tool. Several argue for simply changing the timescales rather than more significant changes.

For free text analysis see Appendix 1

Appendices

Appendix 1: Methodology for open text analysis

Source of increase in requests *(page 15)*

Methodology: Free-text responses (n=283) were analysed thematically. Each response was read in full and coded to every group of requesters it mentioned, with categories developed from the responses rather than a predefined list. Responses that did not identify a specific group were coded as either "no increase" or "increase across all groups". Percentages are calculated from the 283 respondents who answered the question. Because some responses named more than one group, percentages total more than 100%. Initial processing was carried out with the assistance of an AI tool and reviewed by the research team.

Impact of AI-generated responses *(page 22)*

Methodology: Free-text responses (n=361) were analysed thematically. Each response was read in full and coded to one or more themes, with themes developed from the responses rather than a predefined list. Each response was also given an overall rating of the impact described: negative, mixed, little or no impact, or not applicable. A response was rated as mixed only where it identified a genuine positive effect. Percentages are calculated from the 361 respondents who answered the question. Because responses could be coded to more than one theme, percentages total more than 100%. Initial processing was carried out with the assistance of an AI tool and reviewed by the research team. AI was not used to select the respondent quotes provided.

Impact on teams and organisations *(page 24)*

Methodology: Free-text responses (n=348) were analysed thematically. Each response was read in full and grouped into recurring consequences. Many respondents describe several impacts at once, so the top 10 impacts reflect the share of respondents mentioning each theme, rather than mutually exclusive categories. Initial analysis was carried out with the assistance of an AI tool and reviewed by the research team. AI was not used to select the respondent quotes provided.

Change to the law *(page 35)*

Methodology: All free text responses (n=275) were read and grouped by the single legal or practical change requested. Because many answers raise more than one issue or proposed change, the percentages provided are approximate shares of respondents mentioning a theme, not mutually exclusive categories. Initial processing was carried out with the assistance of an AI tool and reviewed by the research team.

Additional respondent comments *(page 38)*

Methodology: Each of the 143 comments were read in full and coded to one or more themes, developed from the comments themselves. Percentages are of the 143 who answered; one comment can be coded to several themes, so they add up to more than 100%. The initial processing was done by an AI tool and reviewed by the research team.

Appendix 2. Research limitations

As with any voluntary survey, this research should be read with some limitations in mind. Despite these limitations, the size of the sample and the consistency of themes across responses provide a strong indication of the pressures organisations are currently experiencing.

Self-selection. Respondents chose to take part in the research. The survey was promoted mainly through DPN's own network and LinkedIn, so the sample reflects people in those circles. It does not represent a random sample of all organisations.

Self-reported data. Figures on volumes, changes over time and deadline performance are based on the respondents' own estimates and recollections, not on organisational records. Some answers will be affected by recall and may be approximate, particularly when comparing current volumes with previous years.

Subjective definitions. Terms such as "complexity" were not defined, so respondents applied their own judgement. Similarly, whether a request was "likely" AI-generated reflects respondents' perceptions, which cannot be independently verified.

Broad sector groupings. Organisations were grouped into broad sectors: public, commercial, third sector and 'other' for those which could not be categorised with confidence. Respondents who selected 'consultancy' were merged into 'other'. Each of these covers a wide range of organisations. For example, the public sector includes local government, health, education and central government. Particular sub-sectors may be under- or over-represented, and the experience of individual sectors may differ from the broad picture presented here.

Organisation size and role. Most respondents worked in larger organisations; fewer than one in five came from organisations with under 250 employees. Respondents were also mainly DPOs and data protection professionals, so the findings reflect their perspectives, not those of senior leaders or the people making requests.

Appendix 3. Survey questions

TYPE OF ORGANISATION AND ROLE

1. Your role:

- [ ] DPO / Privacy Officer
- [ ] Data protection manager/lead (or similar)
- [ ] Data protection team member
- [ ] Legal/compliance team
- [ ] HR Manager or HR team member
- [ ] Other (please specify):

Free text box

2. What role do you play with DSARs?

- [ ] Handle directly
- [ ] Oversee
- [ ] Both
- [ ] Neither
- [ ] Other (please specify):

Free text box

3. Your sector:

- [ ] Public
- [ ] Commercial
- [ ] Third Sector
- [ ] Consultancy
- [ ] Other (please specify):

Free text box

4. Size of organisation (based on number of employees):

- [ ] 1-9
- [ ] 10-99
- [ ] 100-249
- [ ] 250-999
- [ ] 1,000-4,999
- [ ] 5,000+

VOLUME AND NATURE OF REQUESTS

5. How many DSARs have you received in the past 12 months?

- [ ] Up to 5
- [ ] Up to 10
- [ ] Up to 25
- [ ] Up to 50
- [ ] Up to 100
- [ ] 100+
- [ ] Not sure

6. How does this compare with previous year?

- [ ] Significant increase
- [ ] Slight increase
- [ ] About the same
- [ ] Slight decrease
- [ ] Significant decrease

7. Who do you receive DSARs from?
(Check all that apply)

- [ ] Customers / clients
- [ ] Service users / patients
- [ ] Employees (current or former) / their legal representative
- [ ] Students / parents or guardians
- [ ] Members / supporters / donors
- [ ] General public
- [ ] Other (please specify):

Free text box

8. Have you seen an increase in requests from a certain group of people, if so who?

Free text box

9. Are you receiving requests which are likely to be AI-generated?

- [ ] Yes, a significant proportion of requests
- [ ] Yes, some
- [ ] No
- [ ] Not sure

10. Please share the impact AI-generated requests are having, either negative or positive

Free text box

COMPLEXITY OF REQUESTS

11. How has the complexity of requests changed in the past 12 months?

- [ ] Significant increase
- [ ] Slight increase
- [ ] About the same
- [ ] Slight decrease
- [ ] Significant decrease

12. What are the main factors which can cause requests to be tricky to process?
(Check all that apply)

- [ ] AI-generated requests
- [ ] Increased volume of requests
- [ ] Large volume of data to be searched and assessed
- [ ] Unstructured data (such as emails)
- [ ] Multiple systems / departments involved
- [ ] Handling information relating to other individuals
- [ ] Applying other exemptions
- [ ] Applying redactions
- [ ] Parallel matters such as tribunals, disciplinaries or other employment matters
- [ ] Parallel matters such as complaints or legal matters
- [ ] Requests related to children or other vulnerable individuals
- [ ] Other (please specify):

Free text box

TIME AND RESOURCING

13. How is the management of DSARs resourced in your organisation?

- [ ] Dedicated DSAR team
- [ ] Responsibility rests with data protection/ compliance/governance team
- [ ] It forms part of wider non-data protection related duties
- [ ] A sole individual has responsibility
- [ ] Other (please specify):

Free text box

14. Do you have a Data Protection Officer?

- [ ] Yes
- [ ] No
- [ ] Not sure

15. What role does the DPO play in DSARs?

- [ ] Oversight and/or advice only
- [ ] Handles some aspects of requests on an ad hoc basis
- [ ] Handles some aspects of requests on a routine basis
- [ ] Handles most aspects of requests

TIME AND RESOURCING *(continued)*

16. Please share the impact DSARs are having on your work, your team/department and/or your organisation.

Free text box

17. How frequently do you need to extend the timeframe for responses due to complexity?

- ☐ Often
- ☐ Sometimes
- ☐ Rarely
- ☐ Never

18. How confident are you timescale extensions are justified?

- ☐ Confident
- ☐ Somewhat confident
- ☐ Not confident
- ☐ Not applicable

TOOLS AND PROCESS

19. Do you use purpose-built tools to manage the DSAR lifecycle (or the majority of it)?

- ☐ Yes
- ☐ No
- ☐ Not sure

20. Do ever use an external DSAR service to support with handling requests?

- ☐ Yes for the whole request
- ☐ Yes in part
- ☐ Considering
- ☐ No

21. How often do you rely on an external DSAR service?

- ☐ For most requests
- ☐ From time to time
- ☐ Once or twice

22. Why do you rely on an external service?

Free text box

23. Do you use any of the following?
(Check all that apply)

- ☐ eDiscovery tools
- ☐ Redaction tools
- ☐ AI-powered redaction tools
- ☐ Other (please specify):

Free text box

THE DSAR RESPONSE

24. What proportion of requests are completed within the one-month deadline? (Unless an extension has been applied)

- [ ] Under 50%
- [ ] 50-74%
- [ ] 75-90%
- [ ] 90-99%
- [ ] 100%
- [ ] Not sure

25. How frequently do people reply saying they are not satisfied with your DSAR response?

- [ ] Often
- [ ] Sometimes
- [ ] Rarely
- [ ] Never

26. Have you received correspondence from the ICO in relation to DSAR complaints raised with the regulator in the past 12 months?

- [ ] Yes
- [ ] No
- [ ] Not sure

27. Do you believe changes to the law should be introduced to reduce the burden of requests on organisations?

- [ ] Yes
- [ ] No
- [ ] Not sure

28. If you could make a single change to the law regarding DSARs, what would be it be?

Free text box

29. Please share anything else you feel is relevant and hasn't been covered by questions above.

Free text box

DATA PROTECTION NETWORK

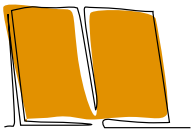
About DPN

Founded in 2014 we regularly publish news, insight and guides. Our experienced team work across a range of sectors providing tailored data protection training, data protection gap analysis reviews and helpdesk support.



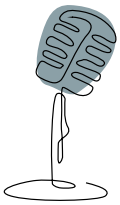
Consultancy

No-nonsense, practical data protection cunsultancy from our experienced team



Articles

News, insight and how-to-guides to support your day-to-day protection work



Events

Expert speakers share knowledge and tips on a range of privacy topics



Training

Down-to-earth data protection training workshops focused on developing your team's skills

Get in touch

Simon Blanchard
simon@dpnetwork.org.uk

Philippa Donn
phil@dpnetwork.org.uk

Sign up for DPN email updates
dpnetwork.org.uk/newsletter-sign-up/

ProvePrivacy

About ProvePrivacy

ProvePrivacy is a GDPR compliance platform built for data protection teams in large SMEs and mid cap organisations. It is designed to take the strain out of Data Subject Access Requests, which are often among the most time-consuming tasks a small team faces.

Our DSAR case management tracks every request and deadline from intake to response, while the built-in redaction tool uses AI-based detection to find personal data across thousands of pages in a single run. It handles PDFs, Office documents, images and email archives, reducing the hours spent on manual redaction and giving teams time back for other priorities. Dashboards show volumes, timeliness and exemptions at a glance.

The same ProvePrivacy platform brings Records of Processing Activities, DPIAs, risk, incident and breach reporting, FOI, policy management and technical controls together in one place, replacing spreadsheets and disconnected processes. Operational staff can use it without specialist knowledge, and DPOs can demonstrate compliance to boards with confidence.

ProvePrivacy Lite offers DSAR and FOI case management with redaction on its own. Both options include unlimited users and can be live in a day.

www.proveprivacy.com