Data subject access requests

Results from the 2023 EY Law survey

Building a better working world

Contents

Introduction

The enforcement of the General Data Protection Regulation (GDPR) in 2018 made it easier for individuals to gain back control of their personal data via eight data subject rights.

One of these is the right of access, granted through data subject access requests (DSARs).

Individuals can send DSARs to organizations to find out what personal data they hold, how and why it is used, and other information about data processing.

All controllers of personal data should be aware of their obligations to respond to DSARs, in accordance with the GDPR (and UK GDPR) as applicable. This means taking active steps to help data subjects exercise their rights; being ready, willing, and able to receive and respond to DSARs; and providing the requested information on personal data processing and access to a copy of that personal data within one month of the request.

Growing challenge

DSARs are not a new right, but they continue to be a challenge for many organizations. In addition to diverting staff from their day-to-day roles and placing immediate demands on the business when they are received, DSARs test a company's ability to locate personal data and can potentially expose policy, procedural and management failings.

As a fundamental right for data subjects, DSARs also give rise to potential risks when they are not handled properly and can lead to further complaints, compensation claims, scrutiny from regulators and enforcement action, including fines and other penalties.

Moreover, while DSARs are free to submit, they are most definitely not free to answer, with organizations and businesses collectively spending millions of pounds each year responding to them. Although the majority of respondents to our survey reported a relatively low annual spend on external support for DSARs, what hasn't been captured is the significant internal cost to the business, which will only increase as the prevalence of DSARs continues to rise.

As the volume and frequency of these requests are likely to grow, many organizations thus face mounting challenges in handling DSARs correctly and in a timely way.

In late 2022, EY Law professionals surveyed more than 500 data protection officers (DPOs) and legal, compliance and HR professionals across the global financial services industry, as well as those from the retail, property, telecoms and charity sectors, to understand how they handled DSARs in FY21-22.

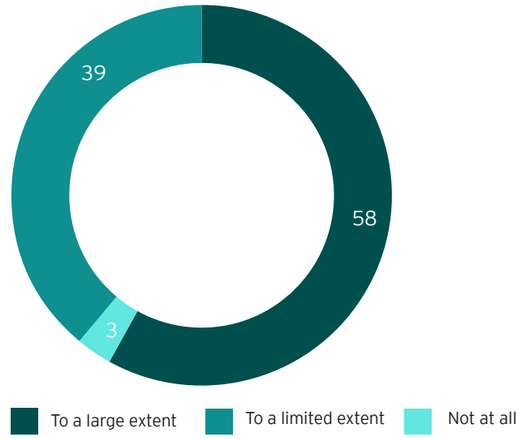
Survey highlights

- 60% of respondents reported an increase in DSARs over the past year.
- 51% had received complaints from data subjects about DSARs.
- Claims management companies (CMCs) make an increasing number of submissions on behalf of data subjects and are a growing source of concern for DPOs.
- 33% of respondents had received "bulk" DSARs.
- 88% handle DSARs in-house, mostly through dedicated data protection teams, but often splitting the work between HR, legal, IT and compliance.

Survey questions and responses

The survey was designed to gather key information on the impact of DSARs on recipient organizations, particularly the time, effort and cost involved in handling them.

1. Do you believe the risk of DSARs is fully understood by your organization?



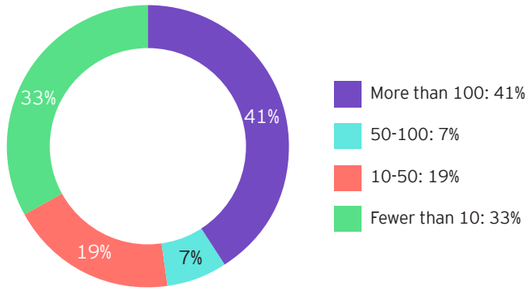
Nearly half of the respondents reported a limited or no understanding of the risks associated with DSARs. This is worrying given the number of risks involved, including the mishandling of the request by failing to recognize it as a DSAR, inappropriate scoping, missing response deadlines, and inadvertently sharing personal data (a personal data breach).

DSARs also give rise to potential risks when they are not handled properly, potentially leading to further complaints, compensation claims, regulatory scrutiny and enforcement action, including fines and other penalties.

Summary

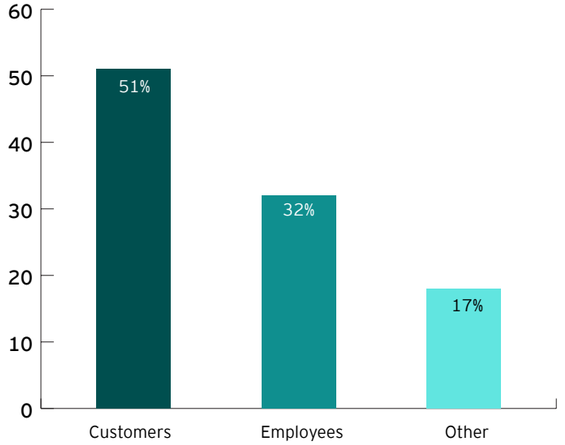
- There are many risks associated with DSARs, so it was open to our survey respondents to interpret this question for themselves.
- DSARs are likely to be received, no matter how compliant your organization, and you have a legal obligation to the data subject(s), to respond to their request for access to their personal data.
- In our experience, DSARs are a focus for data protection and compliance teams, as they often shine a light on everything an organization does with personal data.

2. How many DSARs did you receive in FY21-22?



In general, the larger the organization, the greater the number of DSARs received. Within the financial services industry, wealth and asset management, insurance, and retail banking clients received the most DSARs, while FinTechs and start-ups received the least.

3. What was the source of the majority of your DSARs?



Requests from customers accounted for more than half of DSARs, and we expect the numbers to grow for financial services institutions as the Financial Conduct Authority's consumer duty requirements come into play.

Employees accounted for about a third of DSARs. In our experience, most requests from employees are triggered by disputes related to terminations, unfair dismissal claims or organizational change; employees can routinely submit requests, and organizations can expect to receive these at any time.

"Other" includes DSARs from CMCs, an important and growing trend that will be discussed at length in responses to other questions in this survey. Some 17% of respondents in this category cited CMCs as an issue. "CMCs play a big part in demand on our time," one respondent said. Above and beyond that burden, and perhaps more concerning, several respondents expressed concern as to the underlying reason why CMCs might be gathering personal data.

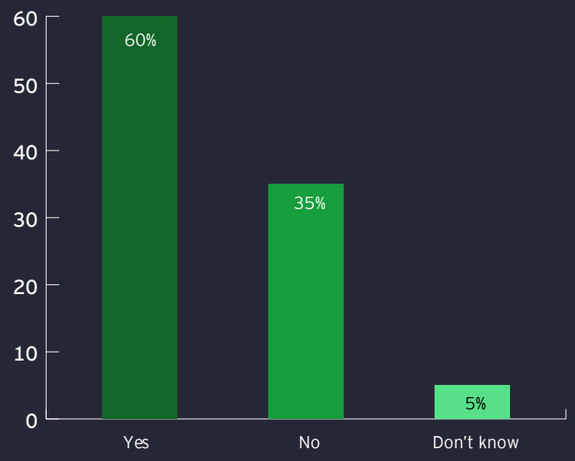
83% of respondents indicate employees and customers are their largest source of DSAR requests.

- In a follow-up interview with the DPO of a global financial services provider, he said his organization now receives about 1,000 DSARs a month, requiring a dedicated team of up to 20 people to process. (Please also see Question 7, which showed that a third of respondents are receiving requests "in bulk".) The requests are not ignored, and the firm acknowledges its duty to attempt to support a data subject in the right to make a request for access.

- He added that well over half of these DSARs cannot be linked to actual customers, which gave him concerns as to the use that such information – including personal and sensitive data that could potentially be used for profiling and monitoring. (Having to verify the validity of 1,000 DSARs and data subjects per month is a task in itself, without even starting on the search for and production of personal data).

- A DPO from a retail and commercial bank echoed those concerns. He believes there has been an increase in DSARs from CMCs and is concerned about the involvement of third-party requestors. He feels privacy professionals may benefit from more parameters around requests and guidance on how controllers should respond. As there is no requirement to have a reason for submitting a DSAR, and data subjects may exercise their rights easily, and at reasonable intervals, the potential for these requests to continue is huge, and unfortunately, organizations are caught in the middle – they have to respond, even to verify these requests but they are also wary of the nature of these requests and the motivations behind them.

4. Have you seen an increase in DSARs over the past year?

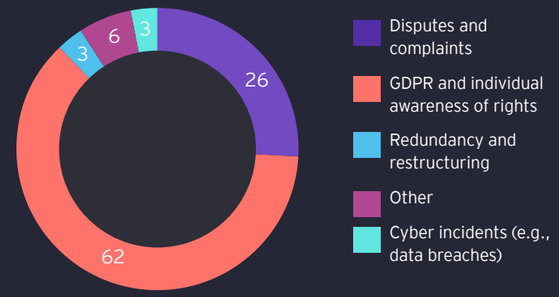


While only 5% of respondents said they did not know whether there has been an increase in DSARs, this lack of awareness may still be concerning. It may suggest poor governance of DSAR processes – or it may just reflect the fact that the process is managed by different business units.

60% of respondents indicate they had seen an increase in DSAR requests in FY22.

Some of these respondents had also answered that risks were only understood "to a limited extent" for the first question. Several others also reported not knowing whether they had received any complaints or notices about their DSAR responses and processes.

5. If you have seen an increase in DSARs, what do you believe is the cause?



62% of respondents indicated that the GDPR and individual awareness of rights was the main reason for the increase in DSARs.

The GDPR became applicable in May 2018, more than four years ahead of our survey. Awareness of data protection rights has grown in this time and no doubt contributes to the upward trend. The campaign by the Information Commissioner's Office (ICO) raising DSAR awareness for businesses and individuals is a likely factor here.

As for disputes and complaints, one respondent said that in a previous role, DSARs appeared to be being used as a tactic to get resolutions to claims. Among the 6% of respondents to this question that cited "other" reasons, most attribute the rise to CMCs for "promoting their services to customers to complain or challenge data controllers on their behalf."

Data subject rights and the importance of maintaining these were a central theme of the discussions we had with our post-survey interviewees. A DPO of a retail and commercial bank, who is also a former member of the ICO and can understand both sides of the issue; is supportive of data subjects' rights but understands the challenges posed to companies when handling requests said:

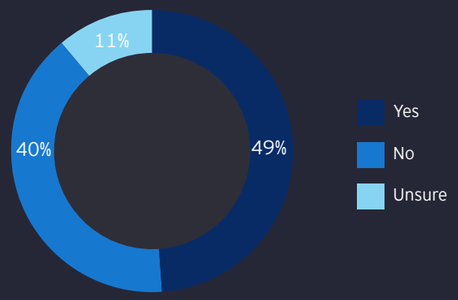
"We don't want to be obstructive – it is their information, but equally, it does appear that certain companies are using personal data access as a business-making enterprise and actively seeking individuals to request their information even where they may not want access to it."

Another DPO added that many individuals still lack understanding about the type of information they are entitled to access, with many falsely believing that a DSAR should give them access to any information they want, including information about the business. Data subjects should understand that they are only entitled to their own personal data. When providing copies of personal data to individual requesters, it is also important to ensure that the rights of other individuals are protected, otherwise there is a data breach.

The DPO said: "It's a balance. Provisions in the UK GDPR are incredibly important rights. We provide individuals with control and a process to hold the business to account, but there is a balance between supporting genuine claims and the resourcing being an unnecessary overhead on the business."

Employment disputes were seemingly less of a factor in responses to this question. There was a low number of DSARs apparently related to "redundancy and restructuring" exercises. However, those figures may well change in next year's survey, given the current economic crises and industrial action.

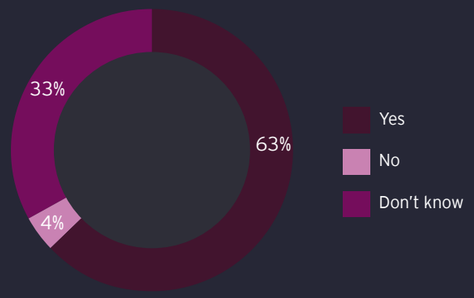
6. Do you expect to see an increase in DSARs over the next 12 months?



It is hard to predict how many DSARs will be received at any time, but we also believe the numbers are likely to increase, across all sectors and notably from customers, who seem more motivated to complain about their customer experience and follow up with DSARs. Increased data collection and processing through digital channels is another reason to expect more DSARs – with increased data processing and opportunities to interact with the public, organizations widen the potential for more data collection and requests. If strike action and economic unrest prompt more employee interest in the process, employee DSARs could also be likely to rise, as stated.

The FCA's Consumer Duty requirements may also trigger more customer requests and DSARs from CMCs.

7. Have you received DSARs in bulk?



While only 5% of respondents said they did not know whether there has been an increase in DSARs, this lack of awareness may still be concerning. It may suggest poor governance of DSAR processes – or it may just reflect the fact that the process is managed by different business units.

Respondents who said yes reflect the rise of CMCs.

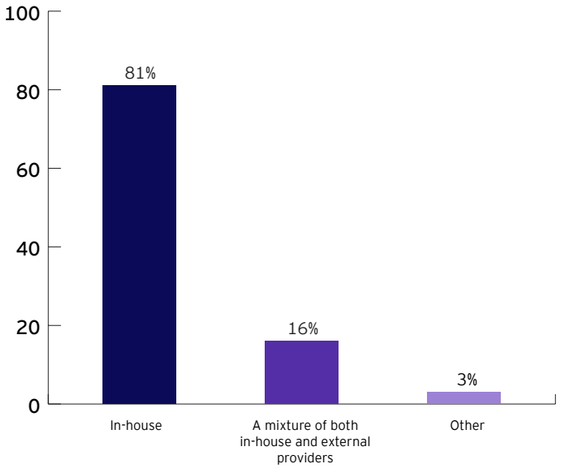
Receiving DSARs in bulk, usually from a representative of a group of data subjects (see also CMCs), is clearly another challenge for many organizations. A third of respondents told us they had received DSARs in bulk, which puts extra pressure on response times and resources. Although dealing with one representative may help with the coordination of responses and aid communication, the process of handling multiple requests during the same one-month period and ensuring that each data subject receives only their own personal data requires robust internal systems and processes.

One DPO said CMCs promote their services by offering to identify and pursue claims for mis-sold loans and other products. While individuals authorize the CMCs to submit a DSAR on their behalf, the DPO said many likely don't understand the extent to which CMCs can access and use their personal data. (He wonders if their privacy notices are sufficiently clear in explaining to individuals that if they sign up for this service, the CMCs, and likely third parties, will have access to their income and expenditure, bank account details, mortgage information and identity documents as a result.) Large-scale data breaches can also trigger "class action" - type DSARs from firms representing affected data subjects. This was a large concern for controllers; DSARs seem to be being used as tactics in disputes and litigations. Paying out a nominal sum in compensation for a data breach (and "settling" a DSAR) can be preferable to spending six-figure sums on responding to multiple DSARs.

In the UK, data protection reforms may help curtail the practice of using DSARs as leverage – where DSARs may be refused, or a fee charged if DSARs are "manifestly unfounded or excessive," as the word "excessive" may be replaced by the term "vexatious" (in line with the Freedom of Information Act). What is deemed to be "vexatious" is yet to be clarified, but even with this change, controllers will still bear the burden of demonstrating that the DSAR is manifestly unfounded or vexatious, as the GDPR currently requires.

Although dealing with one representative may help with the coordination of responses and aid communication, the process of handling multiple requests during the same one-month period and ensuring that each data subject receives only their own personal data requires robust internal systems and processes.

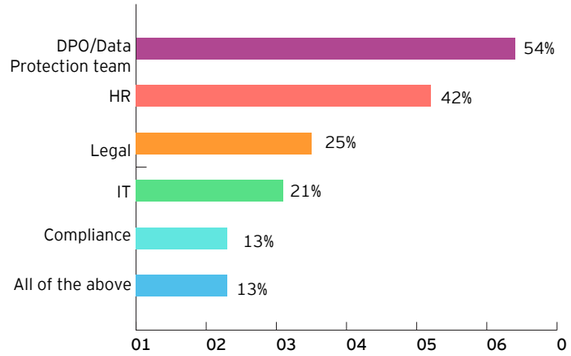
8. How do you handle DSARs?



Our survey did not query the type of external service providers used by respondents, but our experience tells us that these are likely to be external lawyers and e-discovery, forensics or technology services.

A DPO from a UK insurer said DSARs filed by employees are the most "problematic" due to difficulties processing personal data that is HR-related and private. In this situation, he said he limited his involvement to a "need to know" basis.

9. Which internal departments manage DSARs?

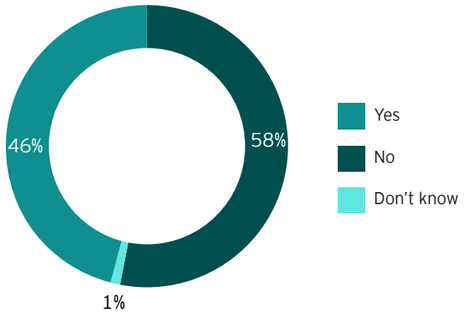


More than half of respondents have a dedicated DSARs team handling requests internally, of which the majority consist of fewer than 10 employees. A small number of respondents (7%) have a team of 21 to 30 people working on DSARs.

Among those that do not have a dedicated DSARs team, the work is split across several departments, including HR, legal, IT and compliance. Our survey also revealed that 35% of respondents recruited staff in the past year just to process DSARs.

For larger companies represented in our survey, the need to employ large teams of staff just to handle DSARs is very real, but it is also a huge expense and probably has an added impact on staff morale and development. Internal teams mean fixed costs that are difficult to scale, so although external support may appear costly, those costs can be more flexible. External support can also free up internal resources to do more interesting and strategic work, leading to a better workforce engagement.

10. Do you use technology to handle DSARs?



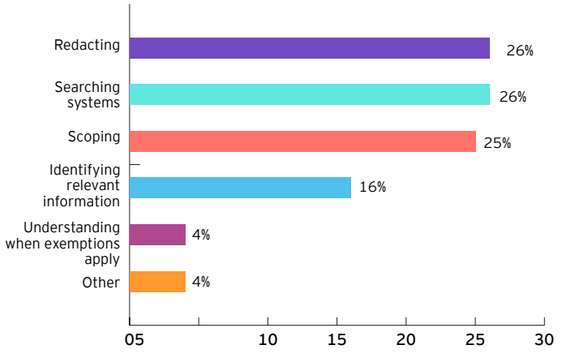
More than half of the respondents use technology to process DSARs. This likely reflects the size of the organization responding to the survey. In many cases, the low volume or types of personal data to be produced may not call for sophisticated technology to be implemented, and it can be simpler to undertake the process of collating, reviewing and redacting information manually.

However, for higher volumes of DSARS, given the tight timeframes and accountability requirements, technology platforms and specialist e-discovery and forensics teams can provide significant assistance and help present the results of searches and production of personal data in a systematic and verifiable way, saving time and resources throughout the process.

No two DSARs are the same, and every organization approaches them differently. Our retail and commercial bank DPO told us that organizations will be aware of the ICO's expectations, but this can still prove challenging, particularly when organizations receive bulk requests or have to deal with incredibly high volumes of unstructured data, to produce DSAR responses within one (or even three) months of the request. He thinks that software can help, and this can provide some level of automation, but the way that organizations' systems and processes are configured, it is very difficult to fully automate processes.

We agree – DSARs cannot be responded to at the push of a button, without any human involvement, and although technology helps filter results from searches, the need to verify personal data, consider third parties and apply exemptions does require time and effort.

11. What are the biggest challenges when responding to DSARs?



The first step to processing a DSAR involves "scoping" the request, which a quarter of the respondents found the most challenging. Typically, DSARs come from data subjects seeking access to all their personal data without supplying the relevant information needed to help locate it. (While organizations may attempt to guide data subjects toward date ranges or topics to help locate the personal data they are seeking, data subjects do not have to agree with that approach and may insist on a much wider search. They do not have to explain their motivation or reasoning.)

For another quarter of respondents, the following step – "search" – is the most challenging. If the search is too narrow, it risks excluding all the relevant data requested; if it's too wide, it risks over-processing personal data and infringing the rights of other data subjects.

It should be remembered that those dealing with DSARs are quite often not in the team or department which is the focus of the data subject's request, so will need to liaise with others across the business to determine what personal data is being processed and where.

Having settled on, or at least asserted, the scope, the actual search (or trawl) for personal data can begin. 26% of respondents to our survey found this part of the process difficult. This is where technology can help, and IT departments play a huge part at this stage of the process; they should know where the data sits across the business, and with the right information, they can and should be able to retrieve it. This is where Records of Processing come in – organizations need to understand if data has been sent on to or held on a third-party system and have the means to extract it. But it takes time and effort.

Searches can also become complicated when DSARs include requests for access to personal data in text messages, social media and messaging apps.

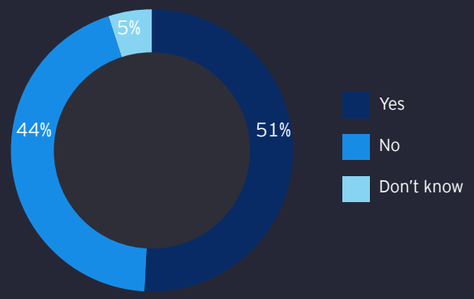
Redacting information was cited as the biggest challenge by a further 26% and we understand why. Even with the use of technology tools, applying redactions (to hide information that should not be provided to the data subject) is a time-intensive process and requires knowledge and skill to do it properly. Technology may spot recurrent names or other identifiers in documents, saving time by locating those that are potentially relevant to a DSAR, but it takes an understanding of what is personal data, (including an assessment of the context of the information available) and the application of any exemptions, or restrictions under appropriate legislation (e.g., the DPA 2018, in the UK), to know when those redactions should be applied.

Several respondents found identifying relevant information to be a struggle. There is some guidance available, but examples of how to determine what is relevant and what is not are limited and most DSARs involve unique queries at some stage of the process.

Exemptions may apply in certain cases, and it is worth getting to know these and their limitations, depending on the local legislation. 4% of respondents to our survey reported that understanding when exemptions apply was a challenge, and we agree that they are often not straightforward nor well understood, especially by data subjects.

Emails presented special problems in all the fields listed. There is an exponential volume of emails generated by organizations and people. They may contain business and confidential information and personal data of other people. They can be a source of embarrassing comments and opinions and judgments about data subjects. These are the holy grail for data subjects embroiled in a customer complaint or employment dispute. Usually, a data subject will ask for emails between certain individuals. How do you give access with respect to the data subject's fundamental rights and those of others? That is where the lengthy but necessary review and redaction phase comes in. In our experience, this stage of the DSAR process is where the most time, money and resources are spent.

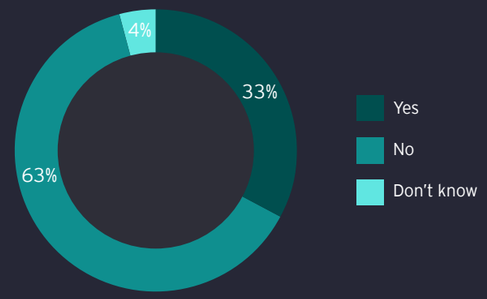
12. Have you received complaints from individuals about your DSARs response?



Just over half of the respondents (51%) said they had received complaints from individuals about their responses to DSARs. This is not surprising as DSARs are often associated with existing disputes and grievances, whether from employees or customers and aggrieved data subjects are likely to pursue complaints if they feel that they have not received a proper response to their request. Unfortunately, the interpretation of what is a reasonable response and the level of understanding of the process for DSARs is inconsistent, so controllers remain exposed to further correspondence to answer and repeat DSARs in many cases.

Whatever the complaint, ignoring a data subject is never a good option and only serves to harm a controller's image and reputation with the ICO. Notwithstanding their validity, controllers are obliged to at least respond, even if it is to decline to answer further, as they otherwise risk further action.

13. Have you received any notices from the ICO about your DSARs process or previous responses?



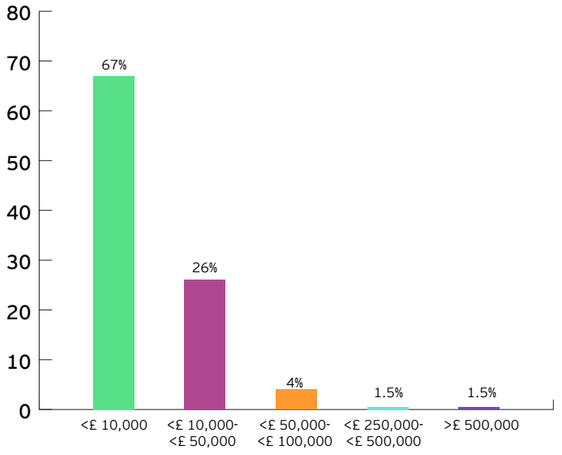
A third of respondents (33%) replied "yes" to this question. We expect most of the notices involved asking controllers to contact the data subject and follow up on their requests, e.g., to explain a decision not to provide certain information. All respondents said the ICO's involvement had been limited to just one such letter and there had been no further action against them once they had replied. This is positive news but it still shows that controllers are obliged to respond, probably for fear of repercussions and a wider assessment of their data protection compliance, by the ICO.

One DPO we spoke to was aware of the potential problems that complaints raise for all parties involved. In his view, and many other fellow interviewees, the ICO takes a balanced view of complaints and is interested in seeing how organizations have taken action to comply with the law. However, there can be occurrences where data subjects approach the regulator and provide only a selective history of events surrounding their DSAR, or equally, for organizations to fail to provide full cooperation with an investigation. Routine, individual complaints to the ICO about different controllers' handling of DSARs take up time and resources as correspondence is sent back and forth over a period of several weeks. He questioned whether this was a good use of anyone's time, as the ICO may find that the organization has done nothing wrong. He argued that monitoring compliance by checking statistics or checking 10 or 20 cases together and benchmarking responses could be a better approach to ensuring data subjects' rights are properly protected.

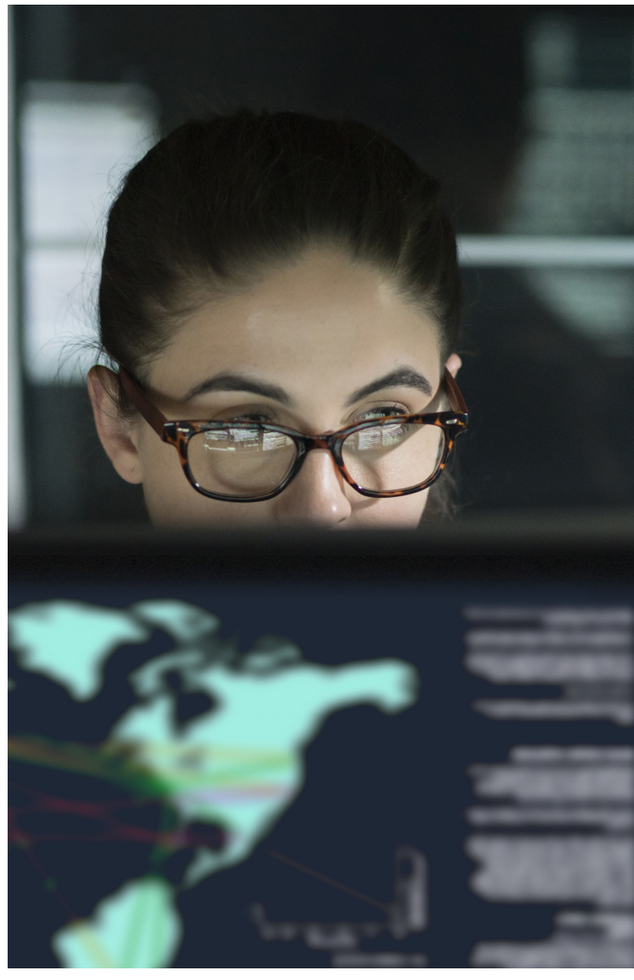
What this DPO believes is important is that the business is cooperative and handles data subjects' rights requests fairly. Being open and honest with data subjects about the process as well as supporting them helps to demonstrate the right approach to the ICO if required.

Very few controllers actively ignore DSARs, and we believe that most recognize their obligations to data subjects. Controllers may feel that the DSAR is not justified or that it is (as currently put in the legislation, at Article 12(5)) "manifestly unfounded or excessive" and seek to refuse the request or charge a fee, but even those situations are rare. However, some controllers have been known to take a more cavalier approach to DSARs and either ignore or refuse to respond to them altogether.

14. What was your external spend on DSARs in FY21-22?



The key to understanding these results is to recognize that this represents external spend on DSAR support. Most of the survey respondents handle DSARs internally and spend their own resources and team budgets on responding to DSARs themselves. That may be because they have relatively few DSARs, or because they have no budget to spend on external resources. The ability to outsource DSAR support may be due to the volume of DSARs received, the skill and capabilities of internal teams, or the financial means to secure that support. Clearly, larger businesses benefit from larger privacy teams and are also much more likely to have the available funding to seek assistance from external service providers.



Conclusion

We understand the challenges organizations face when dealing with DSARs, and the results of our survey reflect many of these, from the overall increase in DSARs received over the last year to the number of complaints submitted by data subjects and notices received from the ICO. As discussed in this report, we believe that DSARs will continue to increase, with more to come from CMCs, more customer-related DSARs as a result of legal and regulatory changes, and more employee DSARs, following the impact of economic unrest.

Although awareness of data subject rights and the GDPR is cited as the main reason for the increase in DSARs, it seems that data subjects' awareness of what they are actually entitled to receive in response to their requests is often lacking. This does not mean that organizations ignore their obligations or take advantage of data subjects' ignorance – on the contrary, the respondents we spoke to all confirmed their support for data subjects' rights. Unfortunately, the resultant burden on organizations is evident in the need for dedicated teams of staff to process DSARs and other areas of the business, such as HR and legal teams find that more of their time is spent supporting on them. We believe the apparently low external spend on DSAR support masks the actual internal spend and the long-term impact of dealing with DSARs on a day-to-day basis.

Many DSARs are presented as broad requests for "all of [their] personal data", which is often a huge task (particularly for employers, who can process significant amounts of personal data in emails, for example), and without further clarification on scope, necessitates a wide search, with review and redaction of the results to follow. All of these stages are tricky, time-consuming and costly. They also impact other data subjects, which may not be fully appreciated by everyone.

It is difficult to see a resolution to the challenges - as more DSARs are received, organizations may find it harder to respond within the one-month timeframe, and data subjects are likely to be frustrated by any delays or perceived failures, which may lead to more complaints. However, it is possible to anticipate the likelihood of DSARs, plan the process and manage the risks.

Contacts

Gita Shivarattan
Partner, Ernst & Young LLP
Head of Data Protection - EY Law
Email: gita.shivarattan@uk.ey.com

Andrea Ward
Partner, Ernst & Young LLP
EY Law - Data Protection
Email: andrea.ward1@uk.ey.com

Peter Given
Partner, Ernst & Young LLP
EY Law - Data Protection
Email: peter.given@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

What makes EY distinctive in financial services
Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

EYG no. 002668-23Gbl
ED NONE

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com