Privacy Pulse Report

Monitoring the heartbeat of the data protection community

Publication date: 4th January 2022

Sponsored by

exterro®

DPN
DATA PROTECTION NETWORK

Foreword

We've taken the temperature of the UK data protection and privacy community and this report provides our findings.

Privacy professionals can sometimes feel isolated and don't always have someone to compare notes with. This report tries to fill this gap; you aren't alone in grappling with some common challenges.

Our report is based on our Privacy Pulse Survey conducted in November 2021, plus a series of more in depth interviews.

This report is another step towards our goal of creating a community where people can confidentially share their views and insights.

The Data Protection Network was founded in 2014 and was designed as a forum to support data protection and privacy professionals.

We have produced a variety of content from formal guidance documents (Legitimate Interest Guidance and Data Retention Guidance) through to a series of webinars which discuss topics of the day with our DPO and privacy colleagues.

We pride ourselves on providing down to earth, no-nonsense guidance and advice. You can find all of our published content at *dpnetwork.org.uk*.

I'd like to thank every single survey respondent and those who spared the time for a more detailed chat. Responses were confidential and no personal information will be shared.

Robert Bond

Chair
Advisory Group
Data Protection Network

Contents

Executive summary

We conducted an online survey between 1st and 29th November 2021. This was followed by a series of in depth interviews. Our intention was to 'take the temperature' of the UK data protection and privacy community and find some shared truths about working in this sector.

This report is divided into the following sections which include a spotlight on particular areas of interest.

Governance and accountability - We asked respondents to indicate the size of the team dedicated to data protection and privacy. Responses from our in-depth interviews suggest there are mixed views about the level of support for the team in terms of resources. There is an additional challenge around making sure teams are supported in the organisation.

We asked respondents about their approach to fulfilling accountability responsibilities, including views on the ICO's Accountability Framework, as well as obligations relating to Record of Processing Activities (RoPA) and Data Protection Impact Assessments (DPIAs).

Our respondents specifically highlighted a variety of challenges with completing RoPAs including:

- Organisation complexity
- Inability to explain the benefits of the exercise
- Time taken to gather & complete the information
- Getting teams to engage
- The limitations of using Excel for complex process mapping
- Struggling to keep records updated
- Difficulties with understanding the supply chain
- Lack of resources in team to complete RoPA

Training and external advice - We are reassured to see most organisations carry out regular online generic training, whilst some extend their activity to role-specific/departmental training. There are increasingly innovative approaches to embedding data protection good practice into organisations.

Adoption and use of technology - 30% of our respondents have outsourced some of their data protection mapping/documentation to third party technology providers. The most popular is cookie management whilst the second, by some distance, is RoPA management.

It is clear the adoption of technology is in the early stages. Organisations are finding a variety of challenges, including the need to deliver an effective Return on Investment (ROI), as well as the need to make disparate systems provide the necessary information.

Data breaches - These appear to endemic. By a swift calculation, based on the results from our survey applied to ICO data, it seems like there are around 20,000 data breaches per year. If we extrapolate further, only around 28% are cyber related incidents.

Data Subject Access Requests (DSARs) - The majority of our respondents had received multiple DSARs and their feedback highlighted a wide range of challenges:

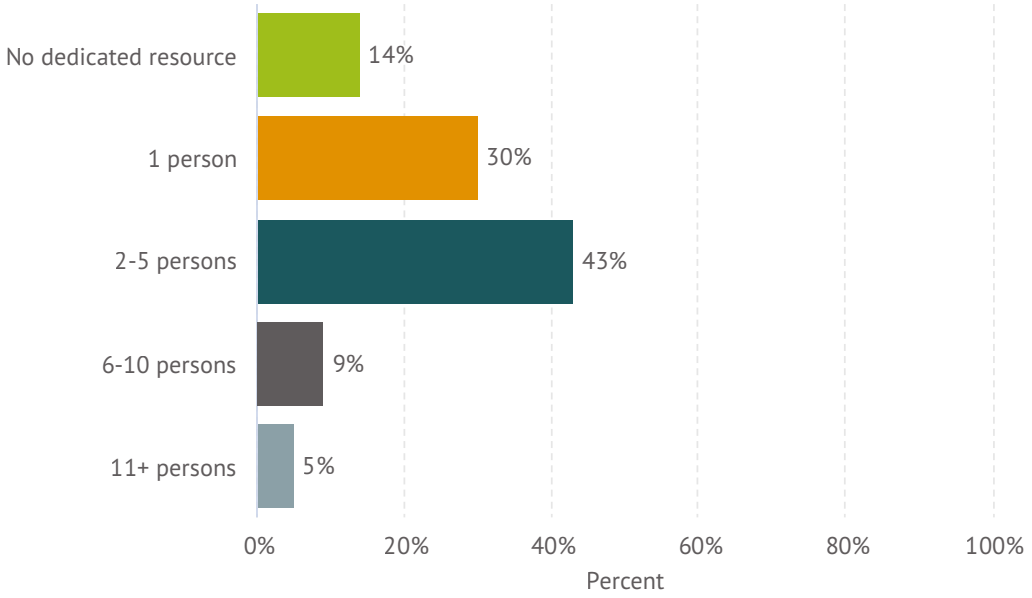
- Being able to recognise a DSAR in the organisation
- DSARs are time consuming, particularly complex HR requests
- Inclusion of email in searches
- Deciding what data to redact and how to do it
- Accessing all systems across the organisation
- The sheer volume of records
- For complex DSARs the timelines are short
- The scope is too wide
- DSARs have become weaponised

About the survey respondents - The respondents to our survey are drawn from the DPN community and are predominantly data protection and privacy professionals.

1. Governance and accountability

1.1 Size of the team dedicated to data protection

What is the size of the team dedicated to data protection?



There was a range of sizes of data protection teams. When we carried out a cross-tabulation between the size of the organisation and level of resource, it was clear bigger organisations had more resources available for privacy.

What is quite surprising is 14% of respondents had no dedicated resource for data protection and privacy, whilst a further 30% only had one person looking after privacy matters. Having said this, more than 76% of the organisations with no dedicated resource were smaller ones.

During in-depth interviews with respondents we asked whether the level of resource they had was appropriate. We received a mix of feedback on this point. It was also clear support from the wider business wasn't always forthcoming.

> *Yes, I think we are supported. I think our challenge is getting the rest of the business to play their part. If you were to give me another six pairs of hands, I wouldn't be able to use them, but if I could get our project management team to complete DPIAs as a matter of course, that would make a difference!*
> **Compliance Manager, Charity Sector**

> *No I'm not well resourced. We could definitely do with more some more resources. I think it is an area where they will have to invest going forward. But whether that means more people, or whether it means we must become more sophisticated in the tools that we use, will have to be decided.*
> **DPO, Insurance Sector**

> *With Covid you've got instant data protection requirements. I do mean instant - the politicians think it, and it has to be on the ground the next day! But things take time if you want them to work.*
> **DPO, Health Sector**

> *At the moment we are seeking to expand our team to get another person on board to help take some of the pressure off. I spend a lot of my time in 'the maze' dealing with queries – 'Can I do that?' 'Can I do this?'. I never really have the time to be above the maze and actually see where we're going. We've now got incoming Transfer Assessments, that's an expanding area. You're sitting there thinking 'oh lord how am I going to do all of these things' and also deal with the normal day to day firefighting. I feel like I'm constantly lurching from one thing to another without really feeling like I'm doing any of it particularly well.*
> **DPO, Public Sector**

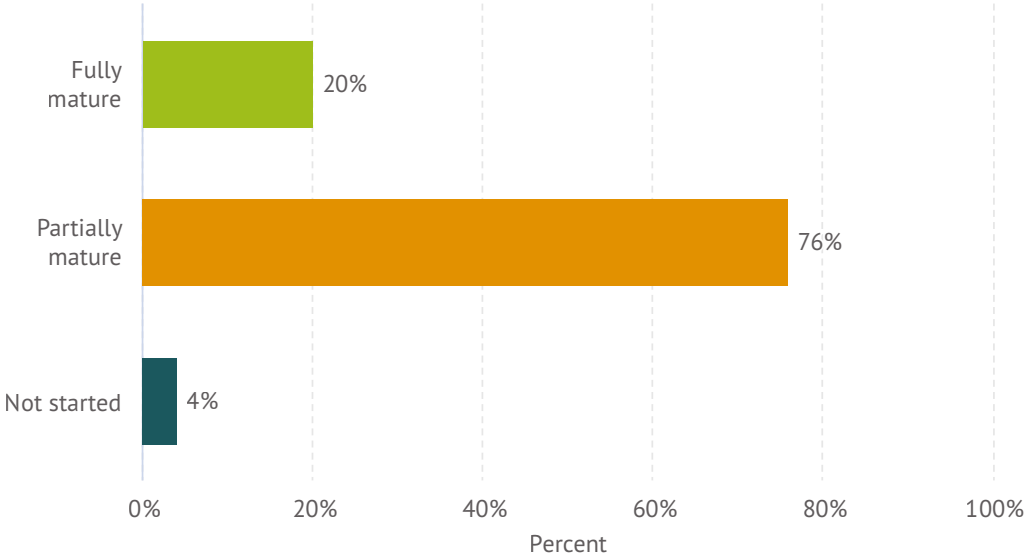
> *More resources have been forthcoming in the past 18 months, there's more Board support now.*
> **Information Governance Manager, Public Sector**

> *We approach it very much on a risk basis. We don't retain huge quantities of customer data, the biggest quantity of data we process is for our employees. Our risks are quite low, and we allocate resources accordingly. I feel confident we have a defensible position rather than a fully compliant position. I think full compliance is pretty much impossible to achieve.*
> **DPO, Defence Sector**

> *It all rests on my shoulders. I've got an internal team of champions who help, which I arranged myself. Generally there is an attitude [within the business leadership] of 'we want to comply and follow the law'. But then as soon as data protection prevents us from doing something we want to do, that attitude changes very quickly.*
> **DPO, Housing Sector**

1.2 Governance and the ICO Accountability Framework

In your opinion, how mature are your governance plans compared to the ICO Accountability Framework?



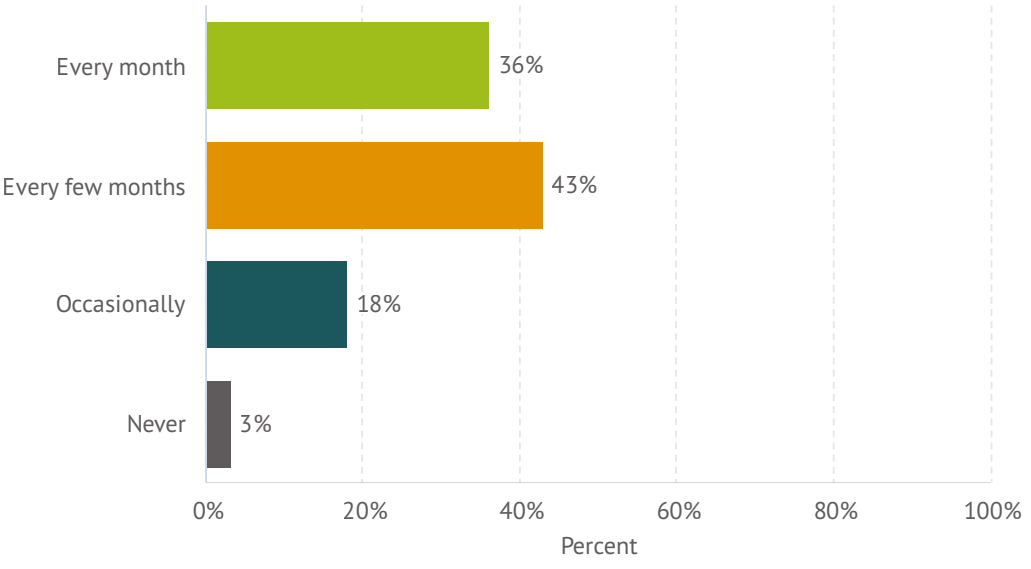
Our results suggest many organisations struggle to fully complete the ICO's Accountability Framework. The Accountability Tracker is particularly long and complex.

Although it's not mandatory, there's a sense the ICO would like organisations to use the Tracker. However realistically, most do not have the time to work through so many detailed questions.

For smaller businesses, the ICO has provided a simpler self-assessment tool which some may find more useful. The ICO also provides some explanation of what is expected.

1.3 Reporting data protection activity to the board

Do you report data protection activity to the board (or senior management)?



In our in-depth interviews we asked about the level of support provided by senior leaders:

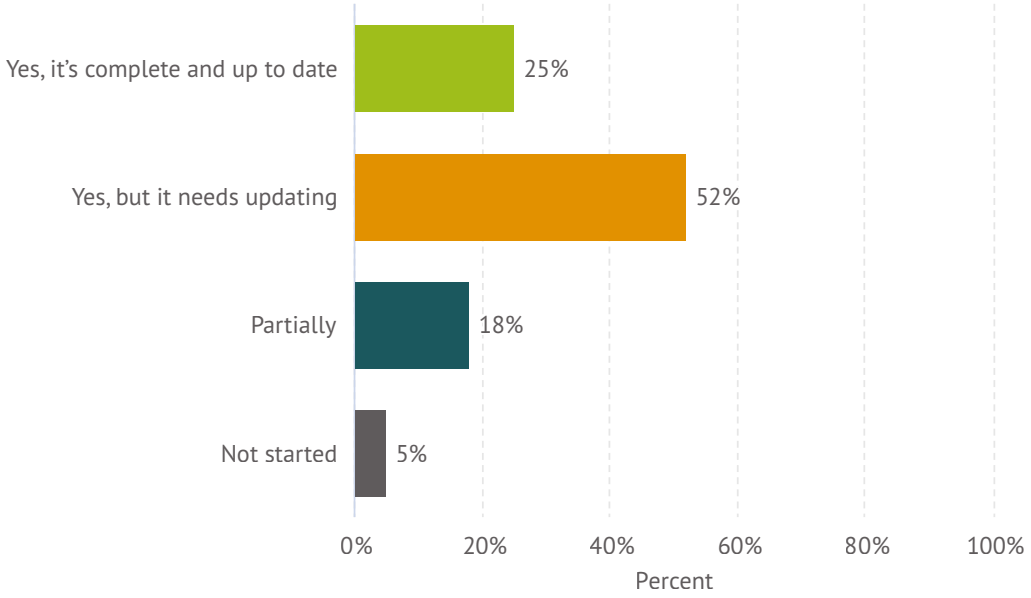
> *Yes, I feel supported, yes I feel heard, but I would like to see more engagement.*
> **Compliance Manager, Charity Sector**

> *I think its treated seriously when something happens. I think they think the problem is 'outsourced' to us as the team that deal with data protection. I think they make the right noises, they like to make reference to it but when it comes down to it NO.*
> **DPO, Public Sector**

> *These results show pretty high visibility to the board - 76% every month or every few months, yet a previous question shows teams are under resourced. There is visibility, but no buy in.*
> **Ray Pathak, Vice President Data Privacy, Exterro**

1.4 Record of Processing Activities (RoPA)

Have you created a Record of Processing Activities?



With a Record of Processing Activities (RoPA), the challenge is making sure all business areas are included, as well as keeping the RoPA up to date. 75% report that it is not complete and/or up to date. The format can appear daunting and there are hurdles to encouraging teams to provide the necessary information.

We have categorised the main responses from our free text question asking about the challenges with RoPAs:

- Organisation complexity
- Inability to explain the benefits
- Getting teams to engage
- The limitations of using Excel for complex mapping

- Difficulties with understanding the supply chain
- Lack of resources in team to complete
- Struggling to keep it updated

We had a significant number of individual comments on this questions, with over two thirds of our respondents providing specific feedback. Here is a selection:

> *Too little time to do it and maintain it. Hard to get answers from staff across the organisation. ROPA's are a great idea in theory, they are a pain in practice.*

> *The complexity of the business model and lack of resources.*

> *Ensuring teams remember to keep it updated beyond the annual review.*

> *Business does not want to do it.*

> *Lack of automated tools – it is a time-consuming process.*

> *Things are constantly changing, and the work involved in keeping a ROPA up-to-date compared with its corresponding usefulness is disproportionate.*

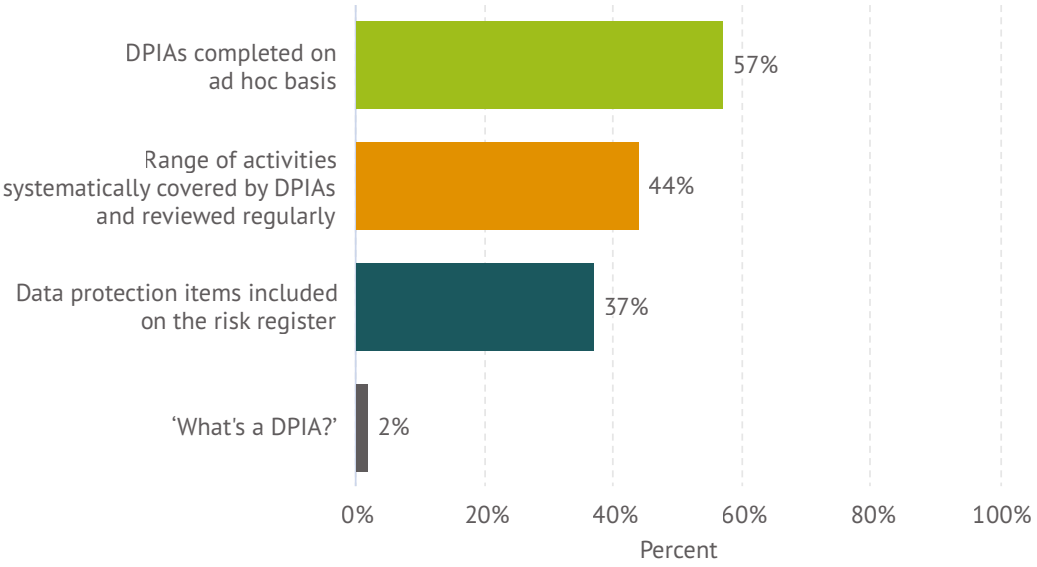
> *New processing can be documented easily as we have a greater understanding of the requirements. However, 'unpicking' long standing processes cause the biggest challenge for me.*

> *Using the ICO template from 2018 meant that we started off trying to achieve excellence when we should have simplified and built up from there. We now find that 3-4 years on it is out of date and requires updating.*

> *Showing it has any real value other than a tick box exercise. It is only utilised when we are forced to update it and no service user has ever fed back anything positive about it.*

1.5 How Data Protection Impact Assessments (DPIAs) are used

How mature is your organisation's approach to Data Protection Impact Assessments?



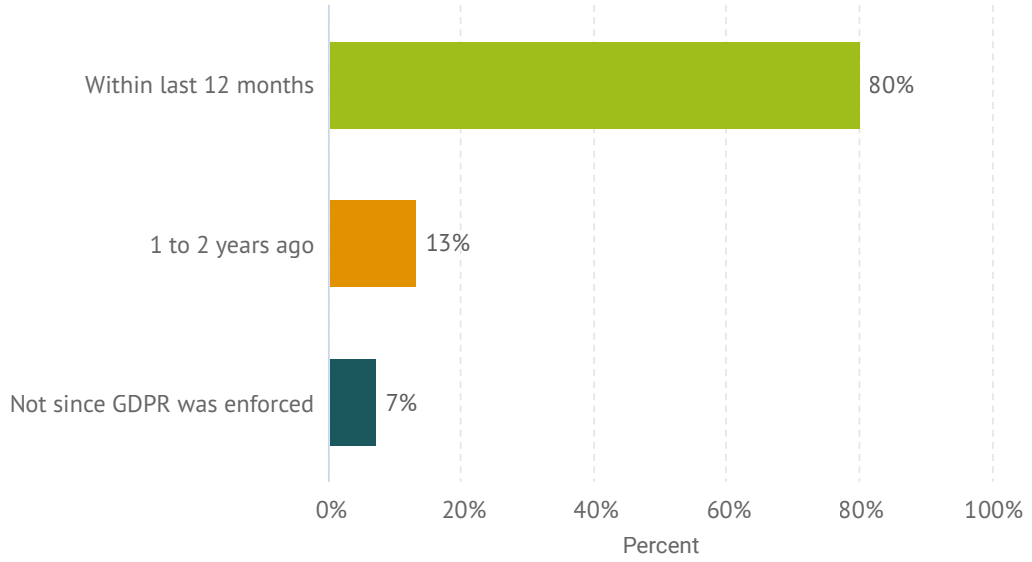
DPIAs are widely used, with the majority completed on an ad-hoc basis.

As with many data protection processes, the requirement to keep them up to date can place a significant burden on organisations, but it's encouraging to see that 44% have a focus on regularly reviewing DPIAs.

2. Training and external advice

2.1 Frequency of data protection training

When did your organisation last provide data protection training to the wider business?

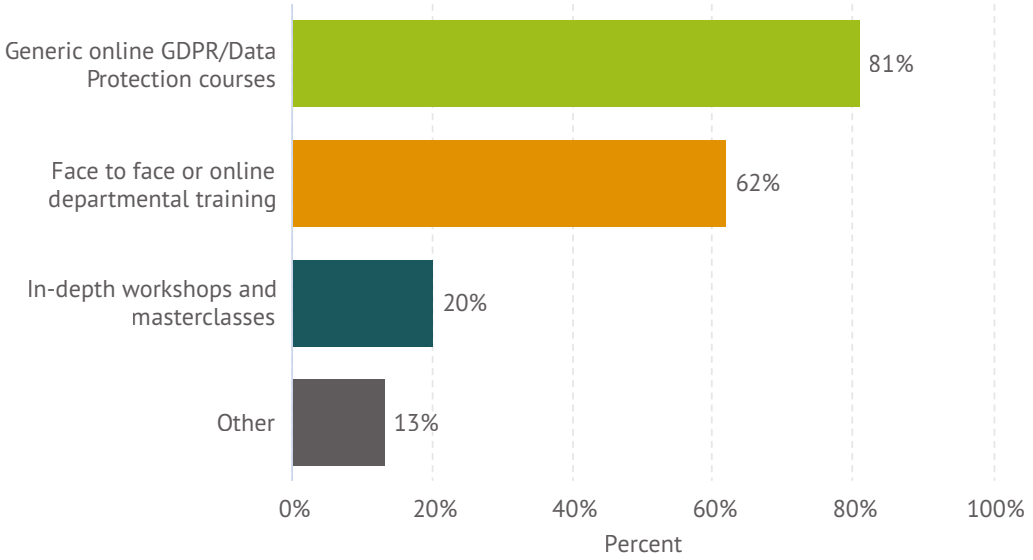


80% of organisations have recently carried out privacy training. This routine requirement is clearly being taken seriously by most organisations.

"It seems organisations are getting the message about training and awareness, as the easiest tool in the privacy programme management toolbox."
Ray Pathak, Vice President Data Privacy, Exterro

2.2 Types of training provided

What type of data protection training do you provide?



Respondents were able to tick more than one answer. It's not entirely unexpected to see online GDPR training is the most common approach, but also encouraging that face to face or online role-specific/departmental training has also scored highly. Clearly the pandemic would have made face to face training more difficult to deliver.

One of the best ways of helping individual teams to understand and support the data protection team is to train them to understand what is expected of them and make sure teams understand their responsibilities.

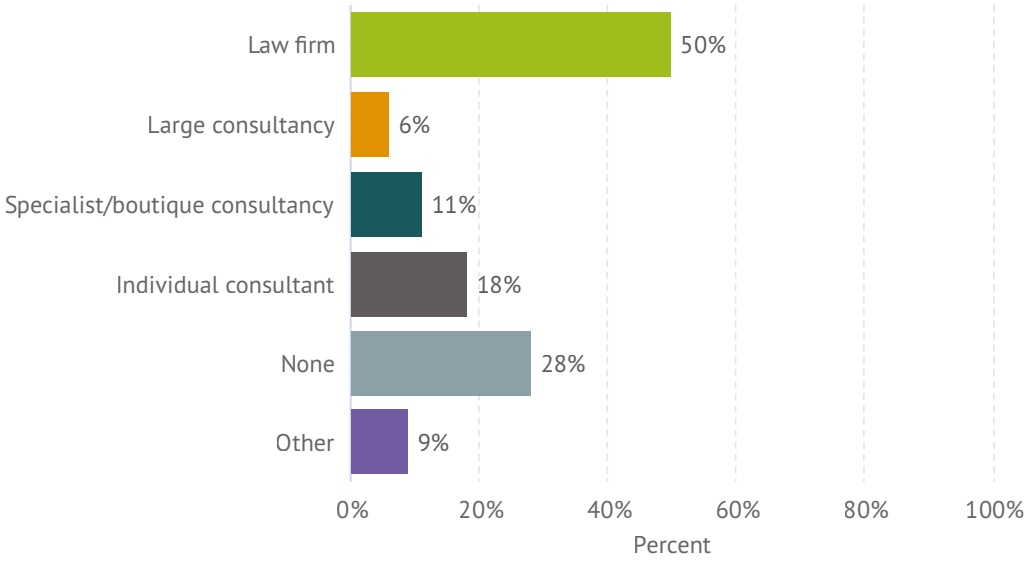
In the comments, we noted a variety of engaging training and awareness tools are being used including:

- Delivering short bursts of information through "privacy moments"
- Case studies
- Bulletins and newsletters
- Bite-sized training modules
- Bite-sized awareness emails
- Regular posters, flyers and reminders
- Ad hoc sessions for specialist areas
- Quizzes using online platforms

Getting the organisation to engage with data protection can be challenging. Effective training and awareness provide a gateway to understanding and building privacy considerations into day-to-day activities. This helps the organisation to understand and manage privacy risks.

2.3 Seeking external advice to support your team

Have you sought external advice to support your team?



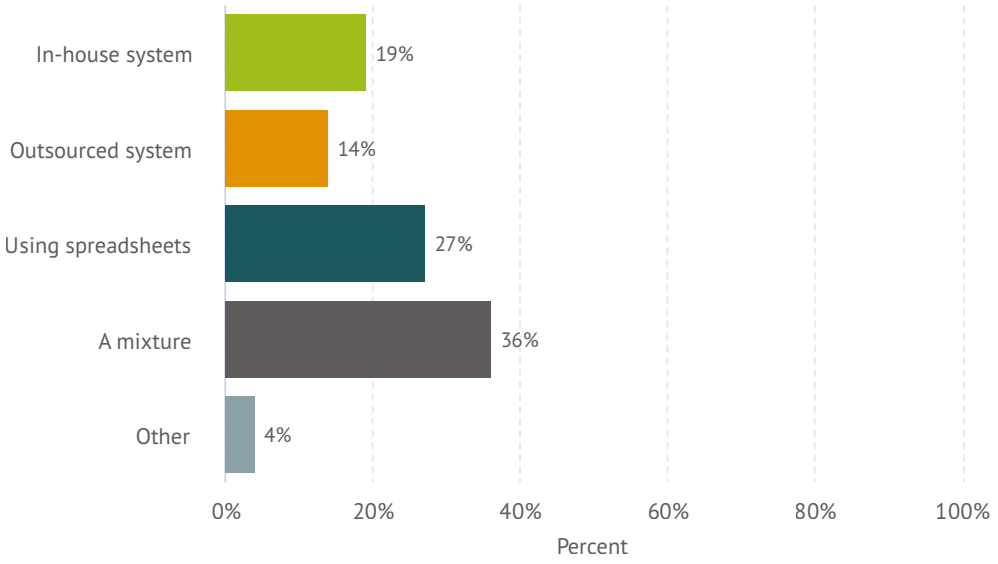
It's not surprising law firms are the most popular source of external advice. Following this, the large/specialist consultancies and individual consultants in aggregate represent another 35% of the responses. More than a quarter seek no external advice at all.

When we reviewed the 'other' option answers, webinars and seminars are mentioned, whilst the ICO website is also cited as a useful resource. Informal networking with peers also plays a part.

3. Adoption and use of technology

3.1 Adoption of technical solutions to support privacy work

In what way have you adopted technical solutions to support your privacy work?



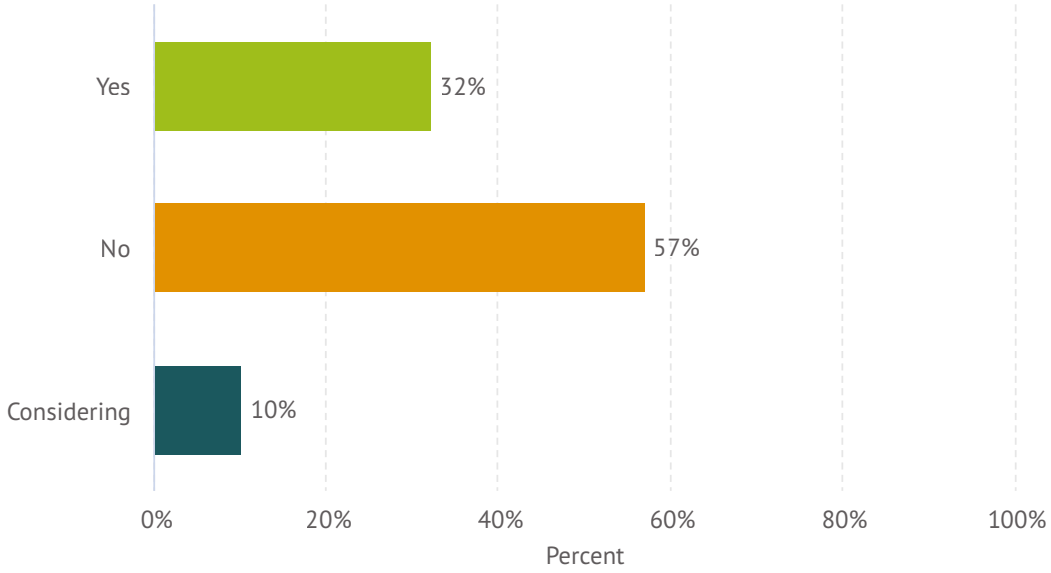
Our respondents indicated they have adopted a variety of methods to manage their data protection programme and content. There is still a high reliance on spreadsheets which is not necessarily a bad thing.

When considering how to use technology, an assessment of proportionality is essential. A small organisation processing a relatively limited amount of personal data simply does not need to invest in a complex outsourced system.

Having said this, we have sufficient comments to indicate respondents are grappling with complexity in medium to larger organisations and a technical solution may suit them better.

3.2 Third party technology vs in-house solutions

Do you use outsourced suppliers to provide privacy technical solutions?

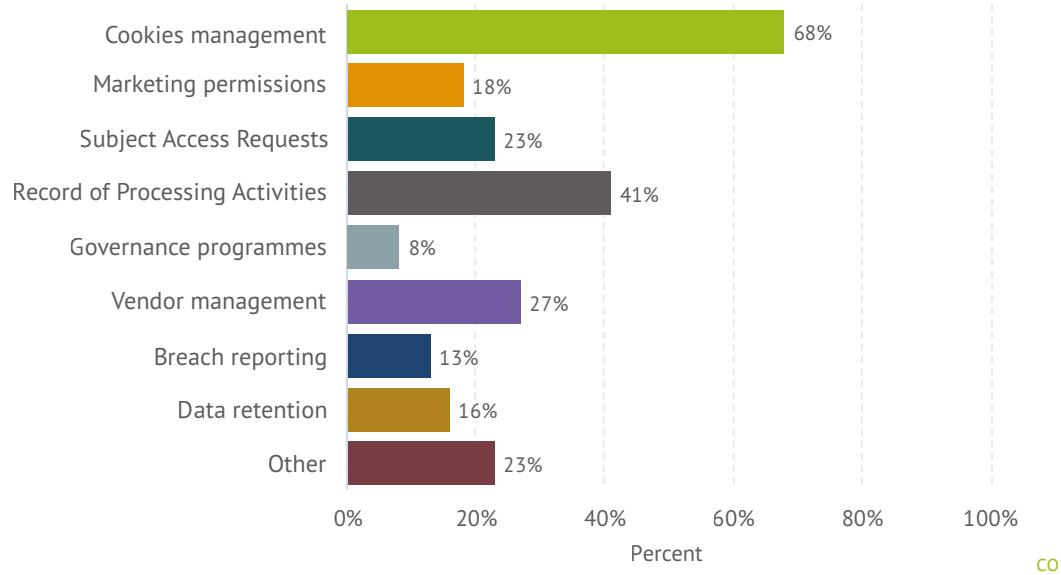


When explicitly asked whether outsourced privacy solutions were used, the majority of respondents have not made the investment yet. Interestingly, 10% are currently considering sourcing a solution. It's hard to tell how long it takes to identify an appropriate partner, but anecdotally we'd suggest that these procurement processes are not quick.

> *"Nearly 70% not having adopted technology is a surprising number based on the number of new laws being introduced, existing ones being updated, laws in general becoming more complex, regulatory fines increasing and breaches increasing."*
> **Ray Pathak, Vice President Data Privacy, Exterro**

3.3 Most popular data protection tasks using third party technology providers

What data protection tasks do you use outsourced technical solutions for?



When we asked what external solutions were used for, the outright winner was cookie management. Not entirely surprising as there are a variety of free, easy to configure solutions for small businesses, whilst paid for solutions are accessible and take the heavy lifting when it comes to managing cookie preferences. Conversely, it's interesting that the number who don't use external cookie management solutions is as high as 32%.

The next most popular solution is to serve the production of the RoPA. This is consistent with our respondents' comments about the complexity of capturing all the necessary information in one place. After that, vendor management is popular with 27%.

Overall though, this sector is nascent. Beyond cookie management, the adoption of technology is relatively low. We expect these numbers to increase over the next few years as solutions are proven and privacy teams are able to demonstrate a positive ROI.

In the responses to the "other" category the highest scores were for information security and completion of DPIAs.

In our in-depth interviews, it was clear some organisations were finding the introduction of third party technology to be problematic. It's a slow process with difficulties managing the integrations with existing systems:

> *"We're looking at technology solutions and have a shortlist of 10. We need to look at our requirements to establish what we need."*
> **DPO, Hospitality Sector**

> *"I think the challenge for any DPO is trying to get the business to understand it has to invest in privacy tools. And there is actually a business benefit for it. I think DPOs struggle trying to evidence what the ROI will be."*
> **DPO, Insurance Sector**

> *"Training is an issue, because they've all got their own ways of doing things at the moment, and none of them are the same, so trying to consolidate that has been a bit of a challenge.....A lot of people are very precious about their processes and don't want to change, so you end up with 40 shades of green."*
> **DPO, Health Sector**

> *"We have largely internal systems, using spreadsheets. Although we have a bought in system for the RoPA. We bought in a relatively inexpensive platform that does the job for us."*
> **DPO, Charity Sector**

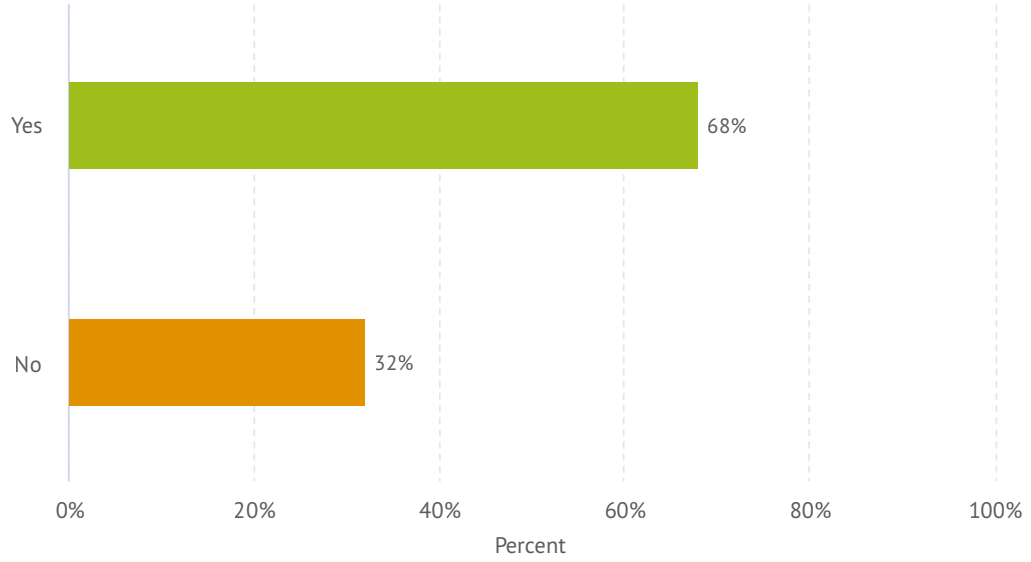
> *"We are very manual, part of the reasoning is some of our systems are fairly old and there's a bit of a concern that if you put something on top of it, it would negatively affect it."*
> **DPO, Public Sector**

> *"We have no external solutions, but I think there's perhaps an appetite now for tech solutions."*
> **Information Governance Manager, Public Sector**

4. Data breaches

4.1 Personal data breaches experienced in the last year

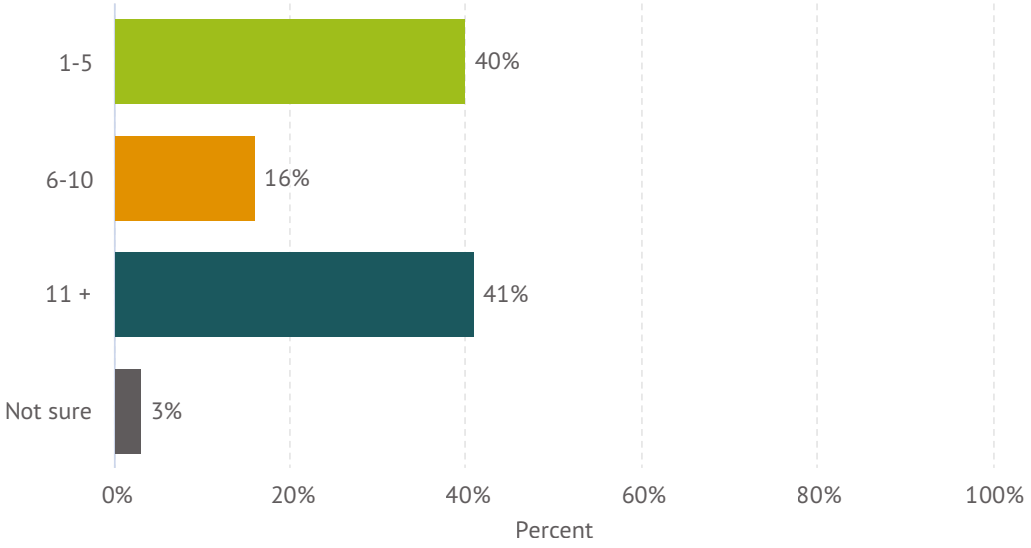
Has your organisation experienced any personal data breaches in the last year?



68% of organisations say they have suffered a data breach in the past year. Clearly the severity will vary enormously and a look at the breaches received and classified by the ICO shows it can extend from accidental disclosures, use of incorrect email recipients, through to large orchestrated phishing attacks. It seems fair to say that data breaches are endemic.

4.2 Volumes of personal data breaches experienced in the past 12 months

How many personal data breaches have you experienced in the past 12 months?

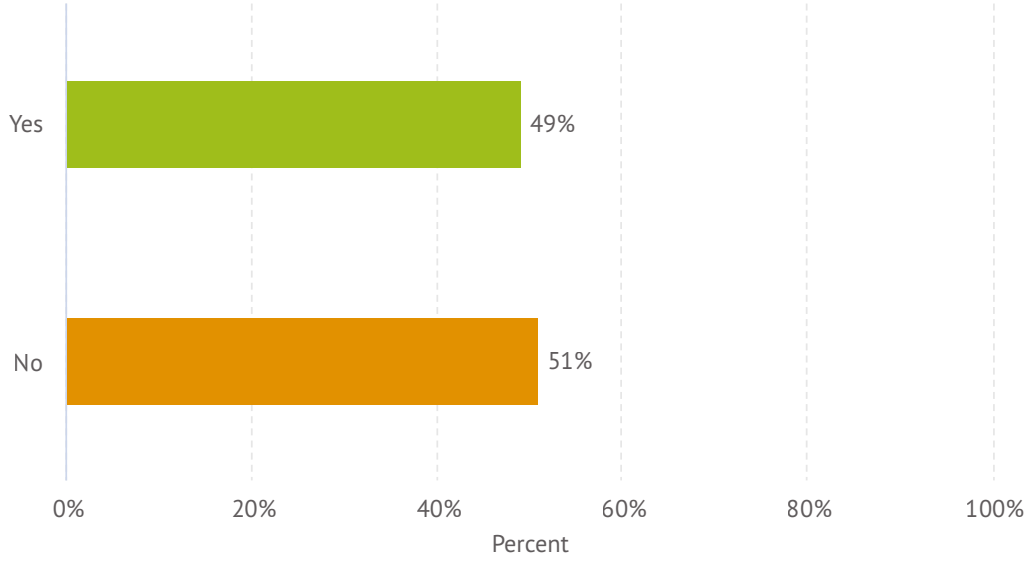


It's not just one breach – for many organisations the volumes are higher, and we were slightly surprised to see over 40% of our respondents had experienced eleven or more.

This also reflects the positive news that organisations are continuing to build better awareness of breaches and internal reporting.

4.3 Breach notifications to Regulator

Did you report any breach to Information Commissioner's Office (or other Data Protection Authority)?



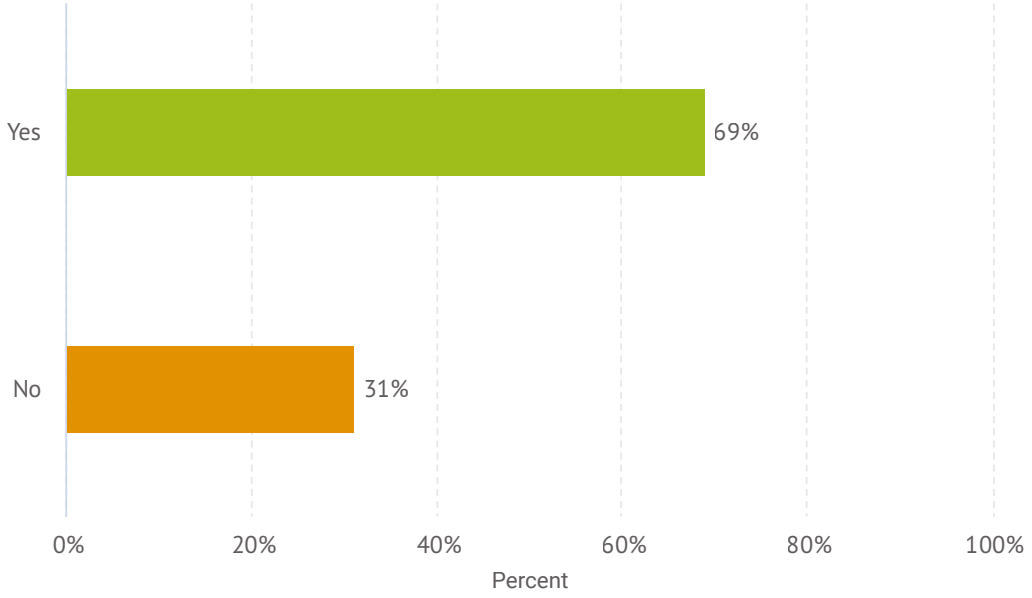
Nearly half of our respondents had reported breaches to the ICO (or other DPA) in the last year.

In the year up to June 2021, a total of 9,921 breach incidents were reported to the ICO. Of these, a total of 2,757 (28%) were cyber related, whilst the vast majority (72%) were not cyber related incidents. This will include data emailed to the wrong recipients, failure to redact, or disclosure of other email recipients in a broadcast email (e.g. misusing the bcc method).

If we apply a simple extrapolation from our respondents replies it seems there were near to 20,000 breach incidents in UK in the year up to June 2021. We wonder whether there is an element of over-reporting out of an abundance of caution.

4.4 Breach notifications to affected individuals

With any breach, did you notify affected individuals?

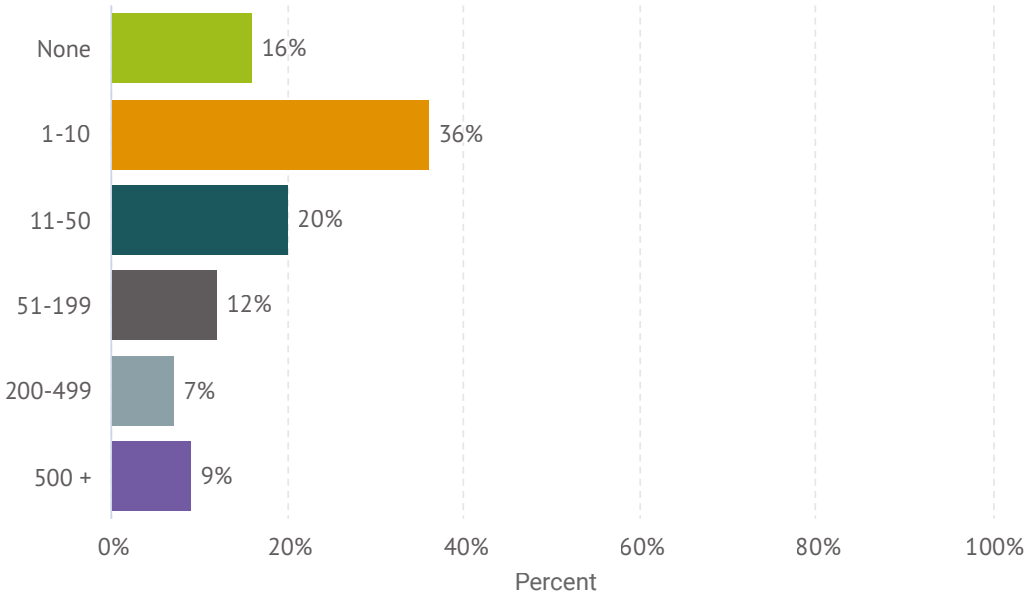


At least one breach was reported to affected individuals by over 68% of organisations. There is an argument that over-reporting to individuals, where the risk is low, may introduce greater level of anxiety amongst individuals. Once again, it is clear organisations are trying to make sure they are 'doing the right thing' for individuals.

5. Data Subject Access Requests (DSARs)

5.1 Number of DSARs received in the last 12 months

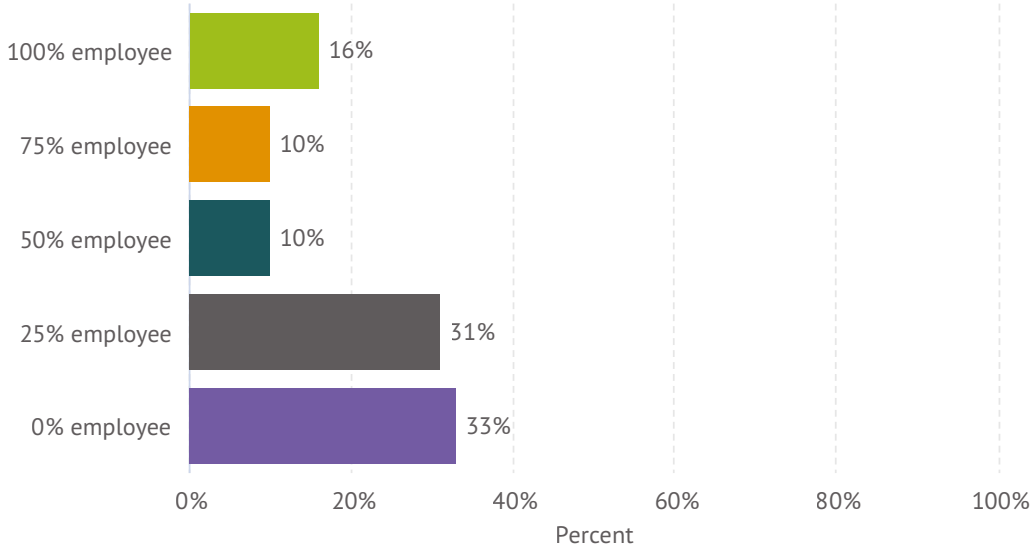
How many DSARs have you received in the last 12 months?



Most organisations have received at least one DSAR. It was quite alarming to see the large volumes received by some organisations, although this may be for a number of reasons including the sheer scale of the organisations and/or being the target of requests via third party portals.

5.2 Split between consumer and employee DSARs

What was the approximate split between consumer and employee DSARs?



Overall, the majority of DSARs would have been received from customers, although anecdotally, we're aware employee-related DSARs can be the most difficult to handle.

We asked our respondents to comment on the challenges they faced when managing DSARs. We categorised the main responses as follows:

- Being able to recognise a DSAR within the organisation
- DSARs are time consuming, particularly complex HR requests
- Inclusion of email in searches
- Deciding what to redact and how to do it
- Accessing all systems across the organisation
- The sheer volume of records
- For complex DSARs the timelines are short
- The scope is too wide
- DSARs have become weaponised

Here is a selection of the individual comments:

> *"Time taken to complete requests – there are no shortcuts."*

> *"The cost and time involved in redaction exercises."*

> *"Finding the relevant information – partly due to wide ranging requests, especially where they include a request for email."*

> *"The number of different systems to check for records. In addition, our main system doesn't easily enable full records to be extracted and we have to extract object by object within the database and then combine."*

> *Time – especially in relation to employee DSARs. There is so much data to manage, when emails are requested.*

> *Gathering data, redacting confidential data or covered by exemptions, multiple requests from same data subject, unable to prove when we don't have data.*

> *Third party 'facilitated' DSARs from the likes of Saymine or Privacy Bee make up the majority of our DSARs. Unclear if these services are adding value to the data subjects, or if they are introducing needless noise that distracts our limited resources from focusing on 'true' DSARs and other privacy related matters.*

Views about DSARs were mixed with our in-depth interviewees. Here is a sample of their comments:

> *The point of a DSAR is to hold an organisation to account for its processing of data, protecting the disenfranchised and the vulnerable. There are provisions in law, they need to be applied properly.*
> **DPO, Hospitality Sector**

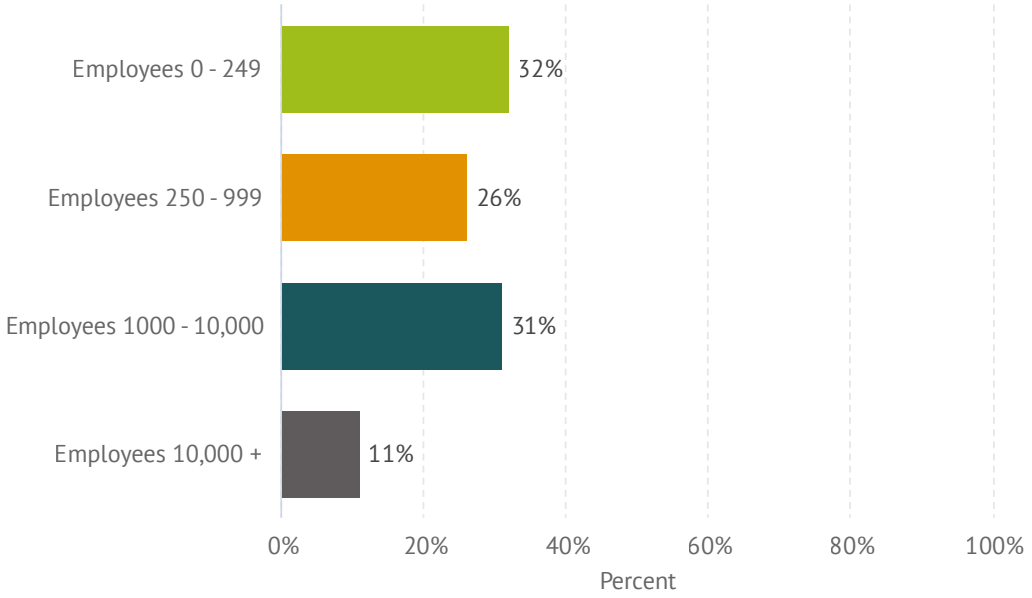
> *DSARs are a nightmare, along with Freedom Of Information Requests. It seems there is always an ulterior motive, and I don't think many people are actually interested in a copy of their personal data, they want to find something incriminating.*
> **Information Governance Manager, Public Sector**

> *Vexatious requests can be very onerous. Controllers need broader scope for rejection and to refine down the scope, plus criteria for when they can charge..... In my view the ICO should focus on helping controllers to manage complex and vexatious DSARs.*
> **DPO, Charity Sector**

6. About the survey respondents

6.1 Organisation size

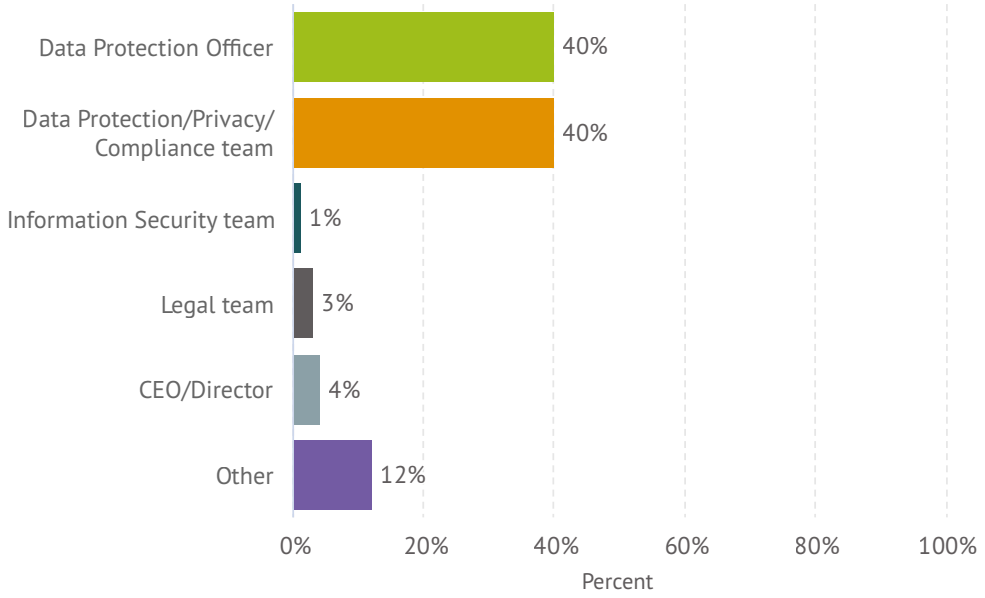
What is your organisation's size?



Our respondents were drawn from a wide range of organisations with a good balance from small businesses through to the 10,000 plus employee organisations.

6.2 Role in the organisation

What is your role in your organisation?

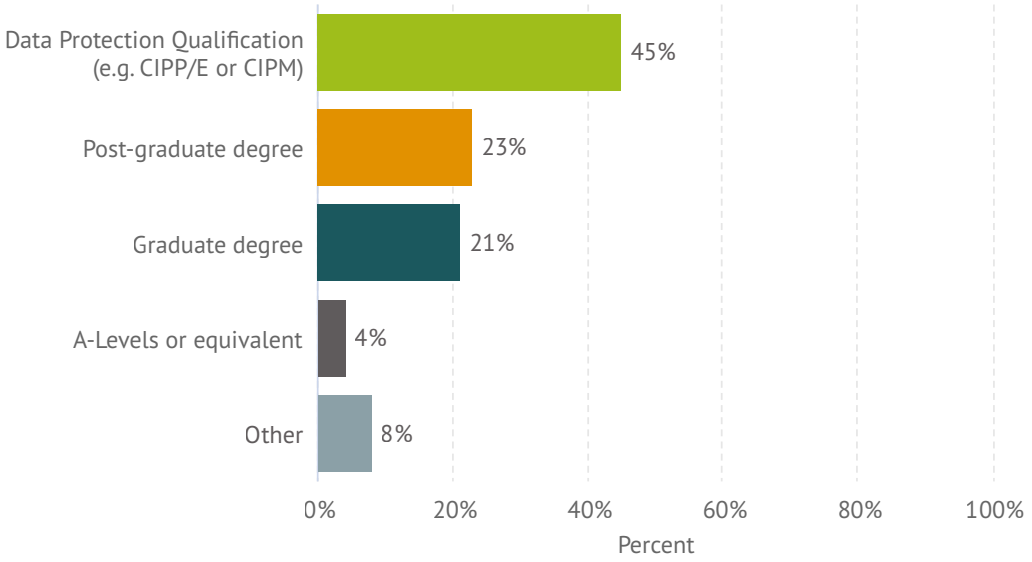


Our specialist audience is largely made up of DPOs (Data Protection Officers) and Privacy/ Compliance Managers.

The majority of respondents in the "other" category were information security roles with the occasional finance, marketing or HR executives in the mix. On this basis we can assume the vast majority of respondents have first-hand experience of dealing with data protection and privacy matters.

6.3 Level of qualification

What is your level of qualification?



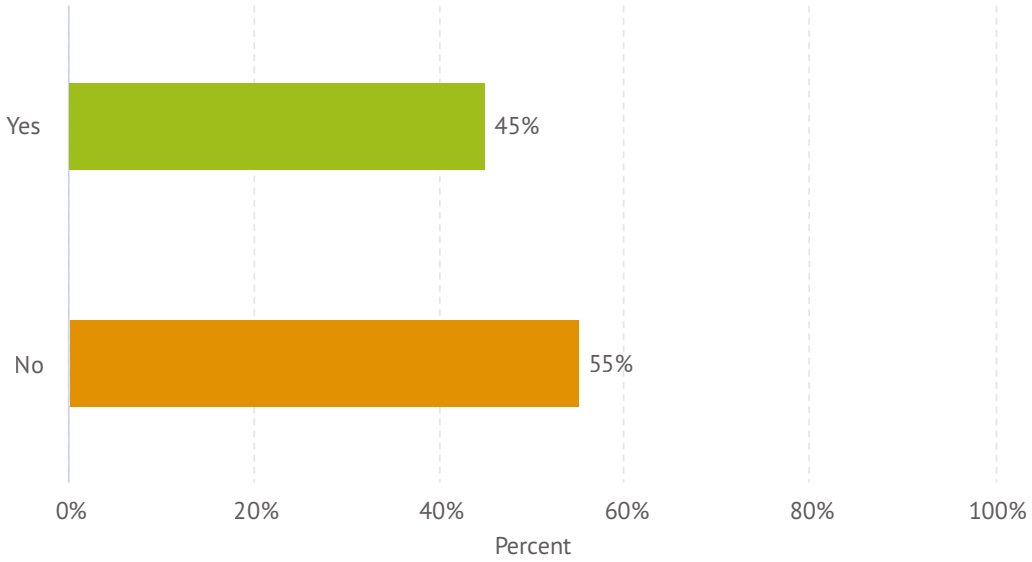
It's not too surprising the most popular response was a data protection qualification, but it's also clear many people approach data protection with a wide variety of qualifications, and this does not stop them doing their job effectively.

To an extent this presents a problem for privacy professionals in that they do not acquire a standard qualification in the way you might see with lawyers or finance executives. This can sometimes serve to devalue the role.

Having said this, qualifications such as the PC.dp, CIPP/E and CIPM, to name a few, are available and relatively accessible for individuals – particularly if their organisation chooses to sponsor them.

6.4 Regulated vs unregulated sectors (e.g. Financial Services, Broadcasting)

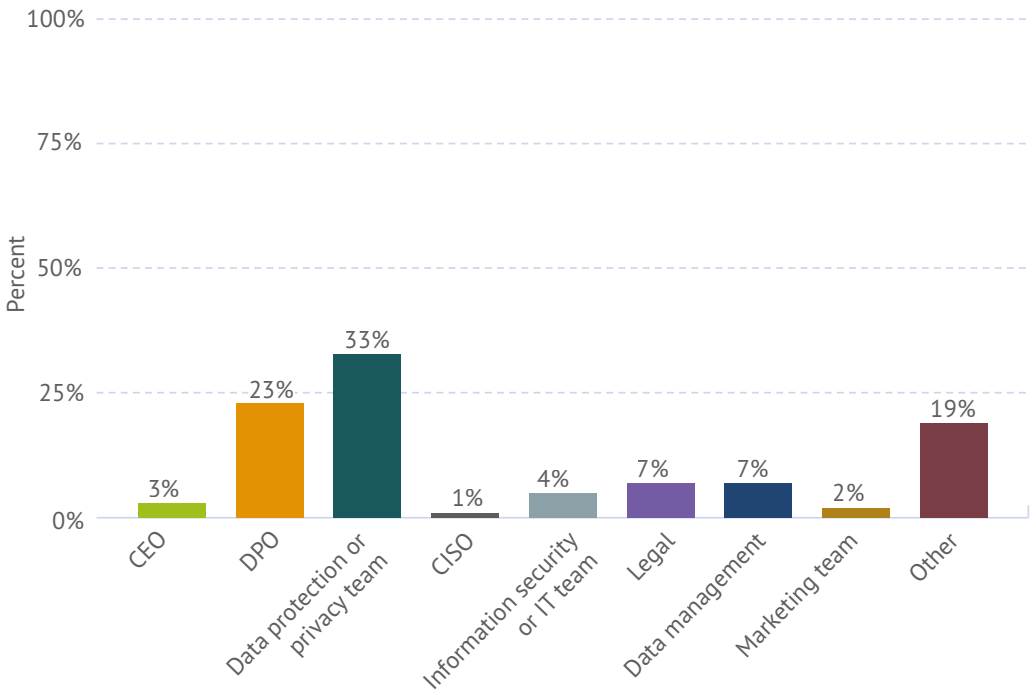
Do you work in a regulated sector (e.g. Financial services, Broadcasting)



We had assumed businesses in a regulated sector would have a greater focus on data protection. To an extent this is true. We carried out a cross-tabulation of size of team vs whether respondents worked in a regulated sector. We found there appears to be a greater incidence of 'no resource' in unregulated sectors.

Methodology

We launched our survey online between 1st and 29th November 2021. All responses were treated anonymously, and the respondent group were visitors to the DPN website through links in email newsletters as well as promotion on social media. Our registered audience is predominantly data protection and privacy professionals in UK.



The chart above is based upon a 2020 DPN Survey

We received a total of 301 completed surveys and have analysed their responses against a variety of topics; from the size of the organisation they work in, to how they handle activities such as DSARs, data breaches and the use of technology. Alongside the survey we conducted a series of in-depth interviews.

We plan to run the Privacy Pulse Survey every year to gain insight into trends surrounding resourcing, the challenges faced and the adoption of technology to support data protection and privacy.

About DPN

The Data Protection Network (DPN) publishes expert analysis, insight and resources. Our content is written and developed by a team of data protection specialists, members of our Advisory Group and other respected contributors.

In 2017 the DPN published the first definitive industry guidance on legitimate interests and in 2020 we published detailed data retention guidance.

The DPN is run by DPN Associates Ltd, a data protection consultancy which provides no-nonsense privacy advice to businesses across a range of sectors.

Based on extensive real-world experience, our team continues to stay at the forefront of data protection. To learn more about us visit: *dpnetwork.org.uk*

exterro

About Exterro

Exterro empowers the world's largest organisations, law firms and Government agencies to proactively and defensibly manage their Legal Governance, Risk and Compliance (Legal GRC) requirements.

Exterro's Legal GRC software is the only comprehensive platform that automates the complex interconnections of data privacy, legal operations, digital forensics, and cybersecurity compliance.

Thousands of legal teams, IT leaders and investigators around the world trust our integrated Legal GRC platform to manage their risks and drive successful outcomes at a lower cost. For more information, visit *www.exterro.com*.

Exterro Privacy Software

Quickly and easily identify, map, manage and protect your organisation's data to establish robust global privacy compliance processes.

Exterro provides the most effective and defensible way to accurately develop and maintain a comprehensive data inventory. Combined with the ability to efficiently leverage data and records retention rules that address legal and business requirements while reducing risks and costs, you'll be in safe hands with the world's most trusted software solutions for meeting domestic and international regulatory obligations.

www.dpnetwork.org.uk

DATA PROTECTION NETWORK