

Data Controller Study 2025

Findings report

Economic analysis

June 2026

ico.

Information Commissioner's Office



Contents

1. Introduction	3
2. Data Controller Background.....	5
3. Data Processing Activities.....	7
4. Technology Adoption	11
5. Regulation and the ICO	13

1. Introduction

As the UK's independent regulator set up to uphold information rights, the Information Commissioner's Office (ICO) enduring objectives include safeguarding and empowering people, empowering responsible innovation and sustainable economic growth, promoting openness, transparency and accountability and developing the ICO's culture, capability and capacity. To achieve each of our objectives, it is essential that the ICO has a detailed understanding of how organisations within the UK economy collect, process and store [personal data](#).

The ICO commissioned an external research provider, IFF Research, to conduct the Data Controller Study to broaden our understanding of organisations' collection and use of personal data, inform our regulatory decisions with comprehensive insights and deliver our enduring objectives. This is the third year of the Data Controller Study and we now hold responses from over 6,800 organisations across the three years.

1.1. Research approach

The ICO commissioned IFF Research to conduct a mixed-method study comprising of a quantitative survey of more than 2,000 organisations and in-depth qualitative interviews of 20 data controllers each year.

Across the quantitative survey, a targeted sampling approach was used in order to achieve a representative sample of data controllers by organisation type (private, public, non-profit) and size (number of employees) and to capture respondents with responsibility for personal data processing within the organisation. In Year 3, quantitative survey fieldwork was conducted between November 2025 and January 2026 and a sample of 2,292 data controllers was achieved using Computer Assisted Telephone Interviewing (CATI) and online surveys.

The qualitative interviews were conducted following completion of the Data Controller Study quantitative survey, to provide the ICO with more in depth insights about areas of focus identified in the quantitative survey. In Year 1, the interviews focussed on the impacts of regulation, both as an enabler and a constraint. In Year 2, we used the qualitative interviews to provide additional insights on the use of technological processes to process personal data. In Year 3, we explored perceptions of data regulation by small businesses who were unaware of the ICO. Qualitative interviews in Year 3 were conducted between February and March 2026.

The quantitative survey data is presented in the interactive dashboard, and the findings are discussed in this narrative. The quantitative survey data is also available in an excel file. A summary of the qualitative interviews findings is provided in an individual document. The Technical Report provides information on

the quantitative and qualitative methodology, representative sampling approach, data collection and methodology limitations.

Considerations

The quantitative survey was developed to achieve a representative sample by sector (private, public and non-profit) and by size (number of employees). In Year 1 of the survey, we observed that the representative sample methodology resulted in small sample sizes for individual subgroups. We have mitigated that by setting a minimum of 50 interviews required for the individual subgroups, namely medium and large private sector, public sector and non profit sector subgroups. However, given the small subsample sizes, results for subgroups should be interpreted carefully and provided with the subgroup sample size.

2. Data Controller Background

Organisations that collect, process or store personal data are known as [data controllers](#). This section sets out summary demographic characteristics of the representative sample of UK data controllers that participated in the survey. Findings provide insights for organisations' size, type, annual turnover, types of services provided and location.

2.1. Organisation size

The representative sample included 73% sole traders (organisations with zero to one employees), 20% micro organisations (with two to nine employees), 6% small organisations (with ten to 49 employees), 1% medium organisations (with 50 to 250 employees), and 0.3% large organisations (with more than 250 employees).

2.2. Organisation type

The representative sample included 97% private sector businesses, 0.4% public sector organisations, including central and local government and 2% non-profit, society or charity organisations.

Public sector organisations consisted primarily of local government organisations such as councils, districts and boroughs (56%). 16% of public sector organisations reported being in the health sector (such as CCG, NHS Trust, GP surgery, etc) and 9% reported being in the education sector (such as FE institutions, schools and exam boards). Another 9% of organisations reported being other public authorities, for example arts councils, regulators and executive agencies, 2% reported being in the justice sector (policing, parole boards, tribunals, etc.), and 1% in central government departments respectively.

Within the sample of private sector organisations, there was a broad range of industry classifications represented. 15% of private-sector organisations reported Professional, Scientific and Technical Professions as their primary sector of operation. This was followed by 10% Construction, 9% Wholesale and Retail Trade, Repair of Vehicles and Motorcycles and 8% Arts, Entertainment and Recreation. There was also representation across other industry classifications, including Information and Communication (7%), Transportation and Storage (6%), Financial and Insurance Activities (6%), Education (6%), and Other Service Activities (7%).

Non profit, society and charity organisations consisted of Health organisations (21%), 18% of Culture and Recreation organisations, 18% of Social Services and 13% of Education and Research organisations. Amongst others, there was representation from organisations across Religion (6%), Environment (4%), and Business and Professional Associations and Unions (4%).

2.3. Annual turnover

The estimated annual turnover for businesses was less than £100,000 for the majority of businesses (62%). 40% of organisations estimated annual turnover of less than £50,000 and 21% estimated annual turnover of between £50,000 and £100,000. 22% of organisations estimated an annual turnover between £100,000 and £500,000. 7% of organisations reported annual turnover of between £500,000 and £2 million, 3% of organisations reported annual turnover of more than £2 million and up to £10 million, and 1% reported turnover of more than £10 million.

2.4. Services provided to consumers

Several questions were designed to understand the types of products and services provided by organisations to consumers and the public and the interactions with consumers and the public.

Most organisations (58%) reported providing products or services, or products and services that were online or internet enabled. 13% of organisations reported providing online or internet enabled products, 26% of organisations reported providing online or internet enabled services and 19% reported providing both.

Of the organisations that reported providing online services, 30% reported providing an online marketplace for third party goods and services, 23% reported providing social media services, 19% reported providing online messaging or voice telephony services and 16% reported providing preventative or counselling services and news, education websites or subscription services respectively. Organisations also reported providing education technology (13%), electronic services controlling connected toys and other connected devices (11%) and music and video streaming (10%).

59% of organisations that offered online or internet enabled products or services reported generating revenues through direct payments or subscription fees from customers, 3% of organisations reported generating revenue from user's data (e.g. through advertising) and 20% of organisations reported generating revenue through both these methods. 15% of organisations offering online or internet enabled products or services reported that they did not generate revenue from these products or services.

2.5. Head office location

17% of organisations reported that their head offices were in the South East. This is followed by 14% of organisations reporting head offices in London, 12% in the South West, 10% in the East of England and 9% in the North West. Another 7% of organisations are based in the West Midlands, Scotland, and East Midlands respectively.

3. Data Processing Activities

This section provides an overview of the findings about the processing activities of data controllers. It sets out the types of personal data held by organisations, identifies the purposes for which organisations process personal data and indicates how data controllers share personal data with third-party organisations.

3.1. What data is held by data controllers

Volume of personal data processed

The majority (79%) of data controllers processed personal data for fewer than 1,000 data subjects in the last 12 months. In fact, 50% of respondents reported processing personal data for fewer than 100 individuals in the last 12 months. The volume of personal data processed increases with organisation size. When filtering for organisation size, most sole traders (56%) reported processing the personal data for less than 100 data subjects. In comparison, when considering large organisations with more than 250 employees, more than half (56%) reported processing personal data for more than 10,000 individuals.

Table 1: Volume of personal data processed by organisation size

Volume of personal data processed		By organisation size				
		Total	Sole traders	Micro	Small	Medium
Less than 100	50%	56%	39%	15%	4%	0%
100 to 999	29%	28%	33%	34%	23%	10%
1,000 to 9,999	12%	8%	17%	29%	25%	25%
More than 10,000	7%	5%	8%	17%	46%	56%
Don't know	3%	3%	3%	4%	2%	8%

Survey questions: What was the volume of personal data that you processed in the last 12 months? (in number of people’s personal data)

Sensitive data

Certain data is categorised as ‘special category’ data due to its sensitive nature. This includes factors such as ethnic background, political, religious or philosophical beliefs, trade union membership, genetic, biometric or health data, and sexual orientation.

In our survey, 27% of organisations reported processing sensitive data, up from 23% in Year 2 and 16% in Year 1 respectively. The majority (71%) of these

organisations reported processing 'special category' data. Another 40% of organisations that reported processing sensitive data reported processing personal data for children and young people under 18 and 25% of organisations processing sensitive data also reported processing criminal convictions & offences data.

Number of employees responsible for compliance

Overall, 69% of organisations reported 0-1 employee responsible for managing data protection compliance and 23% reported between two and nine employees. Less than 5% of respondents reported that ten or more full-time employees had at least some responsibility for managing data protection compliance.

Our study suggests that organisations may believe that all or a majority of employees are responsible for data compliance to at least some extent. This is because the number of reported employees with at least some responsibility for data protection compliance tends to be the same band as their reported organisation size. For example, 89% of sole traders reported 0-1 employees with at least some responsibility for data protection compliance and 76% of micro organisations reported between 2-9 employees responsible for data compliance. 44% of organisations with more than 250 employees reported that more than 250 full-time employees are at least partially responsible for managing data compliance.

We note that in the first year of the survey we identified discrepancies within this survey question. For example, we had noted that sole trader organisations reported that between two and nine employees are responsible for their data compliance. We have sought to improve response consistency by adding a question in the survey, cross-checking responses to this question with responses to organisation size and introducing a confirmation prompt where these numbers do not align. Whilst we are aware that some of these inconsistencies remain in the second and third year of the survey, we have maintained the organisations' original responses.

3.2. How data is used by organisations

Purpose of processing

Organisations process personal data for a variety of reasons. The most common purpose for processing personal data was product and service analytics (41% of organisations). This includes instances where an organisation processes personal data such as the recipient's name, delivery address and payment card details in order to enter a contract with the individual and sell their product or provide their service. Customer analytics can also help organisations identify and meet demand for their products and services.

Some controllers may be under a statutory obligation to process personal data. This can include, for example, tax reporting, social and welfare reporting and regulatory reporting. 32% of respondents reported regulatory or statutory requirements and 16% of respondents reported responding to requests from government authorities as key purposes for the processing of personal data.

Personal data can also help organisations tailor their marketing efforts and improve customer experiences, thereby increasing the effectiveness of their marketing strategies. 21% of respondents reported using personal data for direct marketing purposes.

Dependence of organisations on processing of personal data

The survey results highlight the importance of processing personal data for organisations to provide their goods or services. 53% of organisations reported that processing personal data is essential to the core functions of their business model and 51% reported that it is essential for supporting functions within the business. 13% of organisations reported that personal data processing is useful but not necessary for their business and 11% of organisations reported that processing personal data is not very important for any of the functions in the business.

Acquiring personal data

Organisations can acquire, receive, and collect personal data through a variety of means. Most organisations in the survey (89%) acquired personal data directly from customers or the public. 23% of organisations reported acquiring personal data through other businesses or organisations, in the course of providing products or services. 14% of organisations reported acquiring personal data through cookies or similar online tracking technologies, up from 10% in Year 1 and Year 2 respectively. 12% of organisations reported acquiring personal data from publicly available databases and 11% reported using data intermediaries, such as tech platforms or data brokers, to acquire and collect personal data. A small proportion of organisations also reported acquiring personal data through international sources (4%).

Storing personal data

76% of organisations reported holding personal data digitally. This was more pronounced for public sector organisations (where 91% of organisations reported that data is being held digitally) and increases with organisation size, with more than 87% of organisations with more than 10 employees reporting that data is being held digitally.

3.3. Data sharing

15% of organisations reported sharing personal data outside of their organisation. This was more pronounced for larger organisations, with 44% of large organisations with more than 250 employees reporting sharing personal data outside of their organisation.

Organisations sharing personal data outside of their organisations reported sharing the data with a variety of third parties, including other businesses or organisations (56%), public bodies such as government departments (51%), customers or stakeholders (33%), employees (32%) and other branches of their own business or corporate group or associated organisations (27%).

The most common recipients varied based on organisation characteristics. For example, 61% of organisations processing personal data for more than 50,000 data subjects and sharing data outside of their own organisation reported sharing this data with public bodies. Similarly, public sector organisations sharing personal data outside of their own organisation most commonly reported sharing this data with other public bodies (80%).

10% of organisations surveyed reported sharing sensitive personal data outside of their organisation. Sensitive data was shared most commonly with public bodies such as government departments (45%), customers or stakeholders (36%) and employees (36%).

Overall, 6% of organisations reported sharing UK residents' personal data internationally. Amongst this subset of organisations, the most common jurisdictions for data transfers were the EU and the United States with 79% and 51% of organisations sharing data internationally reporting these as a destination respectively.

4. Technology Adoption

This section sets out the technologies that data controllers use when processing personal data and examines adoption of different innovative technologies.

4.1. IT function management

The majority (69%) of organisations reported managing their IT functions in-house, with all IT functions performed by internal staff. 7% of organisations reported outsourcing all their IT functions to externally contracted service providers. 19% of organisations reported a hybrid between these models, with some IT functions performed in-house, while others are outsourced.

These results vary by the organisation's characteristics. For example, private sector organisations with more than 250 employees reported using a hybrid IT function more often (43%) and public sector organisations reported using a hybrid IT function more often (35%).

4.2. Technology used by data controllers

Technology adopted by data controllers

Many organisations are implementing technologies to assist in the processing and protection of personal data. Cloud storage and specialised hardware or software for managing Data Protection Compliance were the most commonly reported technologies used by data controllers, with 46% and 28% of respondents reporting their use, respectively. Organisations also reported using encryption (25%), physical data servers (22%) and cloud processing facilities (15%). 18% of organisations reported not using any digital technologies, for example due to all data being held physically.

Many technologies have seen an increase in uptake across the three years of the Data Controller Study. For example, the use of cloud storage increased from 36% in Year 1 to 43% in Year 2 and 46% in Year 3. Similarly, the use of artificial intelligence decision making systems has increased from 6% in Year 1 to 8% in Year 2 and 14% in Year 3.

Technology considered but not adopted by data controllers

Out of the technologies that had not been adopted, the most commonly considered technology was cloud storage, with 29% of organisations having considered adopting cloud storage but ultimately decided not to. 22% of organisations had considered the adoption of cloud processing facilities and software / hardware for managing data protection compliance respectively, but ultimately decided not to.

Artificial intelligence decision making systems and biometric recognition technology were considered but ultimately not adopted by 13% and 11% of organisations respectively.

The percentage of organisations that considered the adoption of technologies not in use is higher for organisations that process data for more than 50,000 data subjects. For example, 65% of organisations that did not adopt artificial intelligence systems had considered the adoption of the technology and 63% of organisations had considered the adoption of software or hardware for data protection compliance but ultimately decided against it.

A variety of factors contributed to organisations considering but not adopting certain technologies. The most commonly reported factor was the high cost of the technology (54%). This was followed by ultimately seeing no need for the technology (42%) and a lack of expertise or staff training required (39%). Organisations also highlighted the role that data protection law plays in the adoption of technologies; 28% of organisations that considered but chose not to adopt technologies highlighted the effort required to understand compliance requirements and 20% reported legislative requirements as a factor for ultimately not using the technology.

5. Regulation and the ICO

Data protection law is designed to help organisations to securely manage and safeguard personal data. The introduction of this legislation can also result in organisations having to change certain business processes and incur compliance or monitoring costs. This section explores interactions between organisations and data protection law and the ICO. The section also provides insights into organisations' nuanced view of regulation as both an enabler and a constraint in different circumstances.

5.1. Awareness of data protection law and the ICO

Familiarity with data protection law

The majority of organisations reported feeling very (23%) or fairly (55%) familiar with data protection law. 17% of organisations reported not being very familiar and 4% reported not being at all familiar with data protection law. The proportion of organisations reporting familiarity with data protection law has increased from Year 1, where 16% and 48% reported being very or fairly familiar, respectively.

Familiarity varied amongst respondents in different types of organisations. For example, familiarity increased with organisation size, with 61% and 37% of respondents in large private sector organisations (with 250+ employees) reporting they were very or fairly familiar with data protection law respectively. Respondents in public sector organisations were also more likely to report familiarity with data protection law, with 93% reporting they were fairly or very familiar.

Findings from the qualitative interviews:

In Year 3, 20 qualitative follow-up interviews were conducted to understand more about private sector micro organisations that were unaware of the ICO prior to completing the Data Controller Study.

Levels of awareness of data protection legislation were relatively basic, with many organisations able to discuss data protection principles, but unable to recognise specific laws. Organisations reported a 'common sense' approach rather than having heard or learnt about data protection in a formal context. Organisations reported that being unaware of the requirements was a key challenge in understanding their overall compliance with the law.

The full findings are available in the qualitative findings report.

Awareness of the role of the ICO

62% of organisations reported being aware of the ICO and its work before completing the survey. This remains broadly in line with findings from Year 1 (59%) and Year 2 (63%).

Larger organisations were more likely to report awareness of the ICO in comparison to smaller organisations (90% of large organisations with more than 250 employees were aware of the ICO in comparison to 60% of sole traders).

Table 2: Proportion of respondents reporting awareness of the ICO, by organisation size

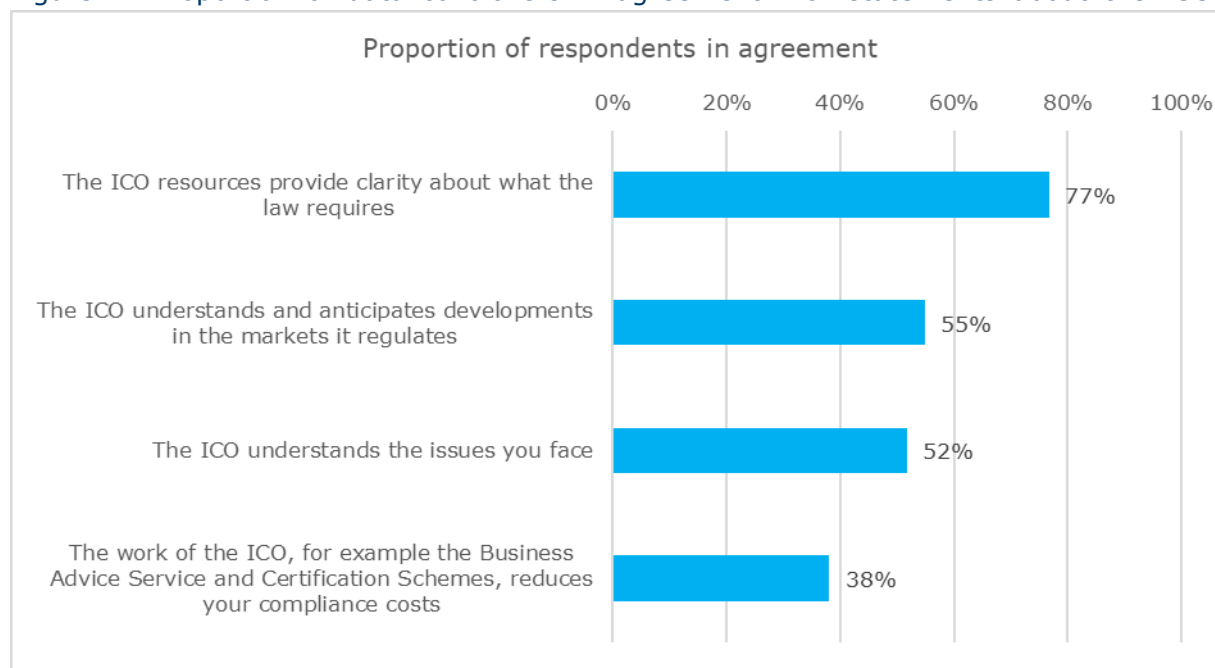
Awareness of the ICO	Total	By organisation size				
		Sole traders	Micro	Small	Medium	Large
Yes	62%	60%	64%	73%	84%	90%

Survey question: To what extent would you agree with the following statements? "Before completing this survey, I was aware of the ICO and its work."

Awareness of the ICO was also more pronounced for organisations that reported processing higher volumes of personal data. For example, 55% of organisations that processed personal data for less than 100 data subjects reported being aware of the ICO. In comparison, 92% of organisations that processed personal data for more than 100,000 data subjects reported being aware of the ICO prior to the survey.

Amongst organisations that were aware of the ICO, the views around the ICO's support were largely positive. 77% of organisations aware of the ICO prior to completing the survey agreed that the ICO resources provide clarity about what the law requires and 52% agreed that the ICO understands the issues that their organisations face. 55% of organisations that were aware of the ICO agreed that the ICO understands and anticipates developments in the markets it regulates and 38% agreed that the work of the ICO reduces compliance costs.

Figure 1: Proportion of data controllers in agreement with statements about the ICO



Survey questions: To what extent do you agree with the following statements? "Agreement" is the combination of responses "strongly agree" or "agree".

The findings also highlight that the ICO provides valuable resources to many organisations. 63% of organisations that were aware of the ICO reported using ICO materials or services to comply with data protection regulations in the last 12 months. The most common materials and resources used were ICO guidance to improve understanding with UK GDPR, PECR, FOIA, EIR, and NIS (38%) and to improve understanding of compliance activities such as ROPA, DPIA (25%).

These proportions are lower when filtering for only sole traders, where 41% of the organisations aware of the ICO reported not using any of the ICO materials or services.

Whilst it is good to see that many organisations that are aware of the ICO use one or more of the resources provided, the survey findings suggest that smaller organisations in particular do not make full use of the variety of [events](#) and [advice and services](#) that are available.

Findings from the qualitative interviews:

Sole traders and micro organisations tended to believe that their practices were not impacted by regulators day to day. Whilst organisations reported a broad understanding that regulators existed to keep people safe and uphold laws, they expected regulators would only get involved with their organisations if there were complaints about non-compliance.

Many organisations did not think that ICO resources or support were relevant to them due to the low volume of data collection and processing. Following being told

about the resources ICO offers, organisations viewed the data protection checklist and e-learning videos as the most likely useful services.

The full findings are available in the qualitative findings report.

Data protection registration

The data protection registration requirement applies to all data controllers, with some exemptions applicable for certain types of data controllers and personal data processing activities. 44% of organisations were aware of the data protection registration requirement and were registered with the ICO. 25% of organisations were unaware of the data protection registration requirement. 13% of organisations were aware of the data protection registration requirements but believed their organisation was exempt from registering and 7% of organisations were aware of the data protection registration requirement but reported that their organisation was not registered. 4% of organisations reported being exempt from the data protection registration requirement but that their organisation had chosen to register with the ICO anyway.

Awareness of the requirement to register increases with organisation size, with more than 85% of medium and large organisations reporting awareness of the ICO registration requirement. Similarly, 81% of public sector organisations reported being aware of the ICO registration requirement compared to 61% of non-profit, society and charity organisations.

5.2. Data protection law as an enabler

Positive impacts of data protection legislation

The survey results provide insights into how data protection law can act as an enabler for organisations. 41% of respondents agreed that data protection laws have been an enabler that has positively influenced the undertaking of core activities within the organisation in the last 12 months. 31% of respondents provided a neutral response (reporting “neither agree nor disagree”) and 22% of organisations disagreed that data protection law had been an enabler. Positive sentiment is on an upward trajectory, from 32% in Year 1 and 38% in Year 2.

These results vary by an organisation’s characteristics. For example, 82% of medium and large private sector organisations (those with more than 50 employees) agreed that data protection laws had been an enabler for their core activities. Public sector organisations and non-profit or charity organisations were also more likely to report that data protection laws have been an enabler, with 64% and 58% agreeing respectively.

The survey also looked to identify the manners in which data protection law could provide positive influences for organisations’ core activities. 40% of respondents

agreed that data protection law has revealed data security and compliance gaps that they are addressing and 56% of organisations reported that data protection law can provide clarity on the types of innovation or technology that are compliant with personal data protection. 40% of organisations also reported that data protection law has helped identify new processes to assist with innovating responsibly.

Respondents also provided insights into how regulation can impact innovation and efficiency. 39% of organisations agreed that data protection law has helped identify, use and store personal data more efficiently and at a lower cost and 34% of organisations agreed that data protection law has helped identify new uses of personal data to improve or expand existing products or services.

5.3. Data protection law as a constraint

Challenges of processing personal data

Processing personal data introduces a broad range of challenges for organisations.

One of the key challenges faced by data controllers is ensuring the integrity and safety of personal data. Organisations reported ensuring personal data is not out of date (54%), not easily retrievable or usable by people outside of the organisation (53%) and accurate (52%) as some of the most notable challenges in processing personal data. Organisations also highlighted cyber security concerns (51%) and unauthorised access (42%) as challenges for processing personal data.

Data controllers also highlighted challenges around understanding regulatory requirements. More than a third of respondents reported a lack of expertise in understanding the legal requirements of data processing (38%) and a lack of clarity about regulatory requirements (36%) as key challenges. Similarly, 34% of respondents reported lack of expertise in processing personal data whilst considering external risks. These findings may, in-part, indicate knowledge gaps and highlight the potential for additional training and support opportunities for organisations.

Constraining factors of data protection law

Whilst 63% of organisations reported that data protection law had placed little to no constraints on their core activities, 34% of organisations reported that data protection had placed constraints to at least some extent. This is an increase from 24% in Year 1.

This effect was more pronounced for medium and large organisations, with 61% reporting that data protection laws had placed constraints on their core activities to at least some extent across both these subpopulations. This could, in part, relate to the increased volume of personal data that medium and large

organisations process. 80% of organisations processing personal data for more than 50,000 data subjects reported that data protection law had placed constraints on their core business to at least to some extent in the last 12 months.

Organisations that reported constraints to their core activities reported lack of clarity about data protection law requirements as the most common constraint (37%). This was followed by uncertainty about adopting an innovative product of service with unclear compliance assurance (33%) and high costs involved in data protection compliance (31%) as key constraints.

5.4. Data protection law as an enabler and a constraint

Our study also revealed that 22% of organisations see data protection law as both a constraint and enabler at the same time. In fact, 66% of organisations that reported data protection law had constrained their activities to at least some extent also reported agreement that data protection law was an enabler.

5.5. Cost of compliance

The cost of complying with UK GDPR varies based on the size of the organisation, the amount of personal data being processed and the purpose for which the personal data is being processed.

In our survey, 21% of organisations reported facing costs as a result of complying with the UK GDPR. These costs presented themselves in the form of one-off costs (reported by 36% of organisations), ongoing costs (43%) and both one off and ongoing costs (20%).

Common costs include the ICO data protection registration fee (62%), software (47%), existing employee undertaking regulatory compliance training (29%) and hardware (27%).

Of those respondents that reported having incurred costs of complying with the UK GDPR in the last 12 months, 46% of respondents reported compliance costs of less than £1,000. The cost of compliance is seen to increase in tandem with organisation size. The majority of sole traders (54%) reported a total cost of compliance of less than £1,000 compared to 78% of large organisations reporting compliance costs of more than £10,000 over the last 12 months.

In Year 3, a new question about the value of individual cost categories was added to the survey. Participants were asked how much each of the cost categories they reported cost in the past 12 months. The results are presented in Table 3.

The most commonly reported cost category included the ICO data protection registration fee, with an average of £65 reported amongst those organisations that reported the cost. 10% of organisations also reported facing software costs. On average, organisations reporting a non-zero cost for this expenditure reported

costs of £1,225. Costs relating to existing employees undertaking compliance work and compliance training were reported at a median average of £1,900 and £1,000, respectively.

Table 3: Costs reported by cost category

Cost category	Organisations reporting cost category (%)	Organisations reporting non-zero cost (%)	Min	Median	Max
Existing employee undertaking regulatory compliance work	5%	3%	£ 3	£ 1,900	£ 3,000,000
Existing employee undertaking regulatory compliance training	6%	4%	£ 2	£ 1,000	£ 100,000
Data Protection Officer	4%	2%	£ 2	£ 5,000	£ 120,000
Software	10%	7%	£ 1	£ 1,225	£ 200,000
Hardware	6%	3%	£ 1	£ 2,150	£ 500,000
Privacy Enhancing Technology	5%	3%	£ 1	£ 2,000	£ 900,000
Consulting	5%	3%	£ 10	£ 2,500	£ 80,000
ICO data protection registration fees	13%	10%	£ 2	£ 65	£ 60,000
Responding to Subject Access Request (SARs)	4%	2%	£ 2	£ 3,000	£ 400,000
Other	0%	0%	£ 50	£ 500	£ 300,000

Survey question: Of this total cost, in the past 12 months how much did each of the following cost your organisation?¹

5.6. Implications of the Data Use and Access Act

In Year 3 of the Data Controller Study, new questions around the Data Use and Access (DUA) Act were introduced to understand the proportion of organisations aware and impacted by the new legislation.

¹ Note: Question was asked to respondents who had reported each cost category. Respondents were able to leave the answer box free, which would be recorded as a zero result. The min, max and median are therefore calculated using non-zero responses only.

Overall, 32% of organisations reported being aware of changes to data protection law that have been introduced as a result of the DUA Act. 57% of organisations reported being unaware.

Awareness was affected by organisation type, with a larger proportion of public sector organisations (53%) and a lower proportion of non-profit, society and charity organisations (27%) being aware of the changes. Larger organisations were also more likely to report awareness of changes (78% of organisations with 250+ employees in comparison to 30% of sole traders).

Amongst those organisations that were aware of changes to data protection as a result of the DUA Act, 28% of organisations reported that their organisations would be affected by these changes. 64% reported that their organisations would not be affected and 7% reported not knowing. Similar trends are noticed in terms of organisation type and size. A higher proportion of public sector organisations (46%) and large organisations (51%) reported being affected by the changes.

Respondents that reported their organisations would be affected by the changes of the DUA Act, were asked additional questions on new costs associated with such changes. Overall, 83% of these organisations reported foreseeing new costs. 26% of organisations anticipated both one-off and ongoing costs. 34% foresaw one-off costs only and 23% anticipated ongoing costs only.