Information Commissioner's Office

Data Controller Study 2025

Findings report

Economic analysis

June 2025

ico.
Information Commissioner's Office

Contents

1. Introduction

The Information Commissioner's Office (ICO) has carried out the Data Controller Study, in order to broaden our understanding of organisations' collection and use of personal data, inform our regulatory decisions with comprehensive insights and deliver our enduring objectives.

The Study involves a quantitative survey of a representative sample of 2,320 organisations and qualitative interviews of 20 organisations.

1.1. Motivation

In our increasingly digital society, sharing personal data, such as name, address, or card details, is often a pre-requisite to accessing services. From utility companies to airlines, healthcare organisations to non-profit organisations, sharing personal data has become vital for interactions across our society, including communication, social welfare, retail and entertainment. If we are to confidently use the products and services provided by organisations, we need to trust that our information rights will be respected.

But who are these organisations? Why do they collect personal data and how much information do they hold? How does data protection regulation such UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) inform the use of personal data across organisations?

As the UK's independent regulator set up to uphold information rights, the ICO's 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.

This will be used to help the ICO build a comprehensive picture to understand organisations' experiences in collecting and processing personal data, which will in turn inform decision making, policy development and regulatory support going forward.

1.2. Research approach

The ICO commissioned IFF Research to conduct both quantitative and qualitative data collection with organisations that collect, process and store personal data. The mixed-method study comprises of a quantitative survey of 2,320 data controllers and in-depth qualitative interviews of 20 data controllers. 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.

The quantitative survey fieldwork was conducted between November 2024 and January 2025, using Computer Assisted Telephone Interviewing (CATI) and online surveys. The qualitative interviews were conducted between February and March 2025. The Technical Report provides information on the quantitative and qualitative methodology, representative sampling approach, data collection and methodology limitations.

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.

Considerations

The quantitative survey was developed to achieve a representative sample by sector (private, public and non-profit) and by size (number of employees). The methodology is set out in the accompanying Technical Report. In Year 1 of the survey, we observed that the representative sample methodology resulted in small sample size for individual subgroups. We have mitigated that by setting a minimum of 50 interviews required for the individual subgroups, these were for medium and large private sector, public sector and non profit sector subgroups. The results for subsample groups 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 a representative sample of data controllers that participated in the survey. Findings provide insights for organisations' size, type, annual turnover, types of services provided to consumers and location.

2.1. Organisation size

The representative sample included 72% 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 3% non-profit, society or charity organisations.

Public sector organisations consisted primarily of local government organisations such as councils, districts and boroughs (63%). 18% of public sector organisations reported being in the health sector (such as CCG, NHS Trust, GP surgery, etc). 10% of other types of public authorities consisted of 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% reported being in the education sector (such as FE institutions, schools and exam boards) and in central government departments respectively.

Within the sample of private sector organisations, there was a broad range of industry classifications represented. 23% of private-sector organisations reported Professional, Scientific and Technical Professions as their primary sector of operation. This was followed by 9% Other Service Activities, 9% Wholesale and Retail Trade, Repair of Vehicles and Motorcycles and 9% Arts, Entertainment and Recreation. There was also representation across other industry classifications, including 7% of organisations worked in construction and education (6%), administrative and support services (6%), and others.

Non profit, society and charity organisations consisted of Social Services organisations (24%), 19% of Culture and Recreation organisations and 15% of Health organisations. This was followed by 12% Religion organisations and 12% Education and Research organisations. There was representation from Development and Housing (6%), Business and Professional Associations, Unions (4%), Environment (2%) and Philanthropic Intermediaries (1%).

2.3. Annual turnover

The estimated annual turnover for businesses was less than £100,000 for the majority of businesses (67%). 44% of organisations estimated annual turnover of less than £50,000, 23% estimated annual turnover of between £50,000 and £100,000. 16% 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, 2% 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. 12% of organisations reported providing online or internet enabled products, 29% of organisations reported providing online or internet enabled services and 17% reported providing both.

Of the organisations that reported providing online services, 23% reported providing an online marketplace for third party goods and services, 20% reported proving social media services, 16% reported providing online messaging or voice telephony services and 16% reported providing news, education websites and subscription services. Organisations also reported providing education technology (11%), electronic services controlling connected toys and other connected devices (7%) and online gaming and streaming (7%).

65% of organisations that offered online or internet enabled products or services reported generating revenues through direct payments or subscription fees from customers, 4% of organisations reported generating revenue from user's data (e.g. through advertising) and 12% of organisations reported generating revenue through both these methods. 17% of organisations offering online or internet enabled products or services reported that they did not generate revenue from these products or services.

Organisations also differed in the way that they interacted with their customers. 30% of organisations reported being an online only business, with no bricks and mortar premises for customers to access. 13% of organisations reported engaging with their customers only through brick-and-mortar means, with no engagement with digital economy, for example, email or card payments. Most organisations (53%) engage with their customers in both ways.

2.5. Head office location

17% of organisations reported that their head offices were in the South East. This is followed by 16% of organisations reporting head offices in London, 10% in the South West, 9% 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 (83%) of data controllers processed personal data for fewer than 1,000 data subjects in the last 12 months. In fact, 55% 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 (65%) 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 (54%) 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	**Total**	**By organisation size**				
		Sole traders	Micro	Small	Medium	Large
Less than 100	55%	65%	33%	17%	7%	1%
100 to 999	28%	27%	30%	28%	15%	9%
1,000 to 9,999	10%	6%	20%	25%	26%	17%
More than 10,000	5%	1%	11%	22%	42%	54%
Don't know	3%	1%	6%	7%	11%	19%

Survey questions: D2. 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, 23% of organisations reported processing sensitive data. The majority (65%) of these organisations reported processing 'special category' data.

Another 30% of organisations that reported processing sensitive data reported processing personal data for children and young people under 18 and 23% of organisations processing sensitive data also reported processing criminal convictions & offences data.

Number of employees responsible for compliance

Most organisations reported having a few full-time employees responsible for managing data protection compliance in the organisation over the past 12 months. Overall, 76% of organisations reported 0-1 employee responsible for managing data protection compliance and 18% 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.

84% of organisations reported between zero and one part-time employee with responsibility for managing data protection compliance. Less than 2% reported having ten or more part-time employees with such a responsibility.

These results vary by organisation size, and the findings indicate that organisation size seems to be in the same band as the number of employees with at least some responsibility for data protection compliance, suggesting that organisations may believe that all employees are responsible for data compliance to at least some extent. For example, 53% of private sector organisations with more than 250 employees reported that more than 250 full-time employees are at least partially responsible for managing data compliance. Similarly, 52% of private sector organisations with 50 to 249 employees reported that between 50 and 249 full-time employees were responsible for their data protection 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 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. 36% of organisations reported product and service analytics as the most observed purpose for processing personal data. For example, if an organisation sells goods online, it can process personal data such as the recipient's name, delivery address and payment

card details in order to enter a contract with the individual and provide their core 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. 27% of respondents reported regulatory or statutory requirements and 13% 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. 22% 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. 51% of organisations reported that processing personal data is essential to the core functions of their business model and 45% 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.

Of organisations processing personal data for more than 10 million data subjects, organisations noted that the processing of personal data was essential to either their core (100%) or supporting (57%) functions within their 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. 21% of organisations reported acquiring personal data through other businesses or organisations, in the course of providing products or services. 10% of organisations reported acquiring personal data through cookies or similar online tracking technologies and 10% of organisations reported acquiring personal data from publicly available databases. 8% 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 (3%).

Storing personal data

77% of organisations reported holding personal data digitally. This increases with organisation size, with more than 80% of private sector organisations with more

than 10 employees reporting that data is being held digitally and more than 90% of public sector and non profit sector organisations with more than 10 employees reporting that data is being held digitally.

3.3. Data sharing

14% of organisations reported sharing personal data outside of their organisation. This was more pronounced for organisation processing higher volumes of personal data, with 45% of organisations processing data for more than 2 million data subjects 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 (58%), public bodies such as government departments (47%), customers or stakeholders (24%) and other branches of their own business or corporate group or associated organisations (21%).

The most common recipients varied based on organisation characteristics. For example, 86% of organisations processing personal data for more than 2 million data subjects and sharing data outside of their own organisation reported sharing this data with data intermediaries. Similarly, public sector organisations sharing personal data outside of their own organisation most commonly reported sharing this data with other public bodies (90%).

7% 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 (42%), other businesses or organisations (34%) and employees (33%).

Overall, 4% 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 73% and 41% 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 (72%) 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. 17% 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 (33%) and public sector organisations also reported using a hybrid IT function more often (38%). Similarly, 91% of organisations processing personal data for more than 10 million data subjects reported managing their IT functions entirely in-house.

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 43% and 23% of respondents reporting their use, respectively. Organisations also reported using encryption (23%), physical data servers (22%) and cloud processing facilities (12%). 17% of organisations reported not using any digital technologies, for example due to all data being held physically.

Findings from the qualitative interviews:

20 qualitative follow-up interviews were conducted to understand more about organisations' use of certain technologies of interest: anonymisation, pseudonymisation, artificial intelligence, automated decision making and biometric recognition technology.

Throughout the completion of the qualitative interviews, we found that the understanding of these technologies is relatively low. Often organisations reported the use of technologies in the survey, but upon further inspection, their use of the technology either did not align with our definitions or the organisation did not use the technology for the purposes of processing personal data.

The full findings are available in the qualitative findings report.

Technology considered but not adopted by data controllers

30% of organisations had considered adopting cloud storage but ultimately decided not to. 22% and 20% respectively of organisations that considered adopting software / hardware for managing data protection compliance and cloud processing facilities ultimately decided not to.

These percentages are much higher for private sector organisations with more than 250 employees or organisations processing personal data for more than 2 million data subjects. For example, private sector organisations with more than 250 employees that do not use cloud storage, software or hardware for data protection compliance and cloud processing facilities reported having previously considered using cloud storage (66%), software or hardware for data protection compliance (55%) and cloud processing facilities (50%). Similarly, more than 80% of organisations that process data for more 2 million data subjects that did not adopt cloud storage, software or hardware for data protection compliance and cloud processing facilities had previously considered adopting cloud storage (85%), software or hardware for data protection compliance (93%) and cloud processing facilities (68%).

A variety of factors contributed to organisations considering but not adopting certain technologies. With 48%, the most common factor for organisations considering but not adopting a technology was that organisations ultimately saw no need. Other reported factors included high cost of the technology (45%), lack of expertise or staff training required (38%) and lack of time for the implementation (25%). Organisations also highlighted the role that data protection law plays in the adoption of technologies; 25% of organisations that considered but chose not to adopt technologies highlighted the effort required to understand compliance requirements and 17% reported legislative requirements as a factor for ultimately not using the technology.

Findings from the qualitative interviews:

Most organisations not using anonymisation, pseudonymisation or biometric recognition technology reported that they did not see a need for them and were therefore unlikely to adopt such technology in the future.

Regarding artificial intelligence and automated decision making, several organisations reported that their organisations are too small and do not process enough personal data to meaningfully benefit from such technology. Whilst many organisations could see the benefits that this technology could provide to their organisations in the future, they were wary of the sensitivity of the data they hold and would therefore not expect to adopt such technology in the future. Others reported that their use of AI would increase with great certainty. In fact, five of

the 20 organisations interviewed described the rise of AI as “inevitable”.

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. In the Data Controller Study 2024 quantitative survey questionnaire, we have introduced a question about data controllers' knowledge of the requirement to register with the ICO under data protection legislation, we provide respondents' views in this section. 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 (18%) or fairly (60%) 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.

Familiarity varied amongst respondents in different types of organisations. For example, familiarity increased with organisation size, with 39% and 43% 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 95% reporting they were fairly or very familiar.

Awareness of the role of the ICO

63% of organisations reported being aware of the ICO and its work before completing the survey. Larger organisations were more likely to report awareness of the ICO in comparison to smaller organisations (74% of large organisations with more than 250 employees in comparison to 62% of sole traders that were aware of the ICO).

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

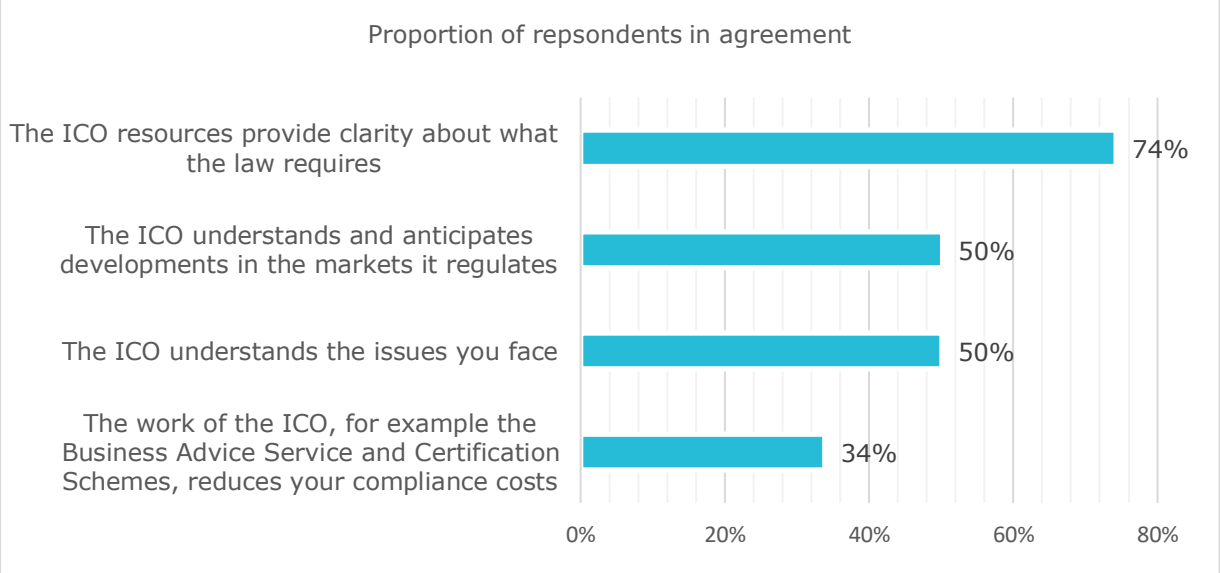
Awareness of the ICO	Total	By organisation size				
		Sole traders	Micro	Small	Medium	Large
Yes	63%	62%	64%	68%	78%	74%

Survey question: F1: 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, 60% of organisations that processed personal data for less than 100 data subjects reported being aware of the ICO. In comparison, 90% 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. 74% of organisations aware of the ICO prior to completing the survey agreed that the ICO resources provide clarity about what the law requires and 50% agreed that the ICO understands the issues that their organisations face. 50% of organisations that were aware of the ICO agreed that the ICO understands and anticipates developments in the markets it regulates and 34% agreed that the work of the ICO reduces compliance costs.

Table 3: Proportion of data controllers in agreement with statements about the ICO



Survey questions: F2: 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's support and advice services provide a valuable resource to many organisations. 59% 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 (35%) and to improve understanding of compliance activities such as ROPA, DPIA (21%).

These proportions are lower when filtering for only sole traders, where 47% of the organisations aware of the ICO reported not using any of the ICO materials or services.

Whilst it is good to see that 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.

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. 14% of organisations were aware of the data protection registration requirements but were exempt from registering and 7% of organisations were aware of the data protection registration requirement but their organisation was not registered. 3 % of organisations were exempt from the data protection registration requirement but their organisation had chosen to register with the ICO.

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. 38% 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 24% of organisations disagreed that data protection law had been an enabler.

These results vary by an organisation's characteristics. For example, 74% 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 57% and 51% agreeing respectively.

The survey also looked to identify the manners in which data protection law could provide positive influences for organisations' core activities. Compliance with data protection law helps safeguard personal data, reducing the likelihood of harms owing to data breaches. 35% of respondents agreed that data protection law has revealed data security and compliance gaps that they are addressing. This in turn highlights the broader positive impact that data protection law has had on keeping personal data more secure.

Data protection law is designed to provide guidance around personal data collection, processing and storing practices to ensure upkeep of personal data

rights. This is supported by findings in the survey, where 52% of organisations reported that data protection law can provide clarity on the types of innovation or technology that are compliant with personal data protection and 36% of organisations reported that data protection law has helped identify new processes to assist with innovating responsibly.

In addition, respondents provided insights into how regulation can impact innovation and efficiency. 34% of organisations agreed that data protection law has helped identify, use and store personal data more efficiently and at a lower cost and 30% 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 retrievable or usable by people outside of the organisation (51%), cyber security concerns (47%) and unauthorised access (41%) as some of the most notable challenges in processing personal data.

Data controllers also highlighted challenges around ensuring the accuracy of personal data being collected and processed in line with the UK GDPR principles. 53% of respondents reported challenges in ensuring personal data is not out of date and 49% of respondents reported challenges in ensuring personal data is accurate.

Finally, 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 (35%) and a lack of clarity about regulatory requirements (33%) as key challenges. An additional 31% 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

Overall, whilst 65% of organisations reported that data protection law had placed little to no constraints on their core activities, 31% of organisations reported that data protection had placed constraints to at least some extent.

This effect was more pronounced for medium and large organisations, with 70% and 59% respectively reporting that data protection laws had placed constraints

on their core activities to at least some extent. This could, in part, relate to the increased volume of personal data that medium and large organisations process. 93% of organisations processing personal data for more than 10 million data subjects reported that data protection law had at least to some extent placed constraints on their core business activities in the last 12 months.

Organisations that reported constraints to their core activities reported uncertainty about adopting an innovative product of service with unclear compliance assurance as the most common constraint (26%). Lack of clarity is also cited as a cause of constraint to organisation's core activities, with 26% of respondents reporting a lack of clarity about data protection law requirements and 23% citing high costs involved in data protection compliance as key constraints.

Cost of compliance

The cost of maintaining compliance 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, 20% 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 40% of organisations), ongoing costs (47%) and both one off and ongoing costs (14%).

Common costs include the ICO data protection registration fee (62%), software (39%), existing employee undertaking regulatory compliance work (22%) and existing employee undertaking regulatory compliance training (21%).

Of those respondents that reported having incurred costs of complying with the UK GDPR in the last 12 months, 63% 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 (80%) reported a total cost of compliance of less than £1,000 over the last 12 months.

5.4. Data protection law as an enabler and a constraint

Our study also revealed that 18% of organisations see data protection law as both a constraint and enabler at the same time. In fact, 60% 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. The case study below exemplifies how data controllers provide a nuanced view about data protection law being both an enabler and a constraint for organisations.