

Executive summary	2
Introduction	4
Data controller background	6
Data processing activities	8
Technology adoption	12
Regulation and the ICO	14
Overview of data controller qualitative interview findings	20

Executive summary

The Data Controller Study is a piece of research that aims to provide insight and support the Information Commissioner's Office (ICO) strategic, regulatory and research activities. The study includes both quantitative and qualitative data collection with organisations that collect, process and store personal data, with the aim to understand:

- the demographic characteristics and personal data processing activities of data controllers;
- the technology used by data controllers;
- innovation considerations of data controllers; and
- data controllers' views of both the work of the ICO and data protection in general.

The findings of the quantitative survey are presented in an interactive dashboard and accompanying narrative below, helping bring the findings to life. A summary of the qualitative findings provides an insight into data controllers' experiences with data protection regulation.

We have published the quantitative survey questionnaire, technical report and raw data for broader research and analytical purposes, in line with our enduring ICO25 objectives. We aspire for the data and findings to contribute to the development of collective data insights and support policy development and research that take into consideration data controllers' views and experiences, support public welfare and safeguard individuals' data protection rights.

We would be keen to discuss the use of data and findings across a range of sectors, such as public, regulatory and academic. If you wish to get in touch or have questions about the research, please email the team: [\[email protected\]](#).

Supporting documents

- [Data summary tables](#) - this Excel file provides a summary of all the survey questions in a table format.
- [Raw data file](#) - this Excel file is the raw data of the quantitative survey results.
- [Technical report](#) - the report sets out the methodology for the quantitative survey findings.
- [Qualitative infographic](#) - this infographic summarises the findings from the qualitative interviews.

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 2,280 organisations and qualitative interviews of 20 organisations.

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 (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 develop 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.

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 2,280 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 October and November 2023, using Computer Assisted Telephone Interviewing (CATI) and online surveys. The qualitative interviews were conducted between November 2023 and February 2024. 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 the following sections. 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. We note that due to the sample size for individual subgroups, results for subsample groups should be interpreted carefully and may not be representative of the full population. For example, filtering by private sector organisation with more than 250 employees or filtering by public sector organisations that reported being unaware of the ICO prior to taking part in the survey result in a weighted sample of less than 10 organisations respectively.

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.

Organisation size

The representative sample included 74% sole traders (organisations with zero to one employees), 19% micro organisations (with two to nine employees), 5% 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).

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 (45%). 13% of other types of public authorities consisted of arts councils, regulators and executive agencies. 12% of public sector organisations reported being in the health sector (such as CCG, NHS Trust, GP surgery, etc), 11% reported being in the education sector (such as FE institutions, schools and exam boards) and 5% reported being central government departments.

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 13% manufacturing and 13% wholesale and retail trade. There was also representation across other industry classifications, including 5% of organisations worked in construction and education (5%), human health and social work (5%), administrative and support services (5%), and others.

Annual turnover

The estimated annual turnover for businesses was less than £100,000 for the majority of businesses (58%). 34% of organisations estimated annual turnover of less than £50,000, 24% estimated annual turnover of between £50,000 and £100,000. 22% of organisations estimated an annual turnover between £100,000 and £500,000. 8% of organisations reported annual turnover of between £500,000 and £2 million, 4% of organisations reported annual turnover of more than £2 million and up to £10 million, and 1% reported turnover of more than £10 million.

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 (56%) reported providing neither products nor services that were online or internet enabled. The remaining organisations reported providing either online or internet enabled products (12%), services (17%), or both (14%).

Of the organisations that reported providing online services, 30% reported providing an online marketplace for third party goods and services, 27% reported providing online messaging or voice telephony services and 21% reported providing social media services. Organisations also reported providing news or education websites (19%), online gaming or streaming (14%) and music or video streaming (14%).

58% 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 20% 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.

Organisations also differed in the way that they interacted with their customers. 21% 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. Another 19% of organisations reported being an online only business, with no brick-and-mortar premises for customers to access. Most organisations (57%) engage with their customers in both ways.

Head office location

25% of organisations reported that their head offices were located in the South East. This is followed by 11% of organisations reporting head offices in the South West, North West and London, respectively. Another 7% of organisations are based in the West Midlands, Scotland, and Yorkshire and the Humber respectively.

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.

What data is held by data controllers

Volume of personal data processed

The majority (81%) of data controllers processed personal data for fewer than 1,000 data subjects in the last 12 months. In fact, 48% 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 (57%) reported processing the personal data for less than 100 data subjects. In comparison, when considering large organisations with more than 250 employees, more than two thirds (68%) reported processing personal data for more than 10,000 individuals.

Table 1: Volume of personal data processed by organisation size

Survey questions: B1. Approximately how many people does your organisation employ? D2. Approximately how many people does your organisation employ?

Volume of personal data processed	Total	Sole traders	Micro	Small	Medium	Large
Less than 100	48%	57%	24%	13%	4%	1%
100 to 999	33%	31%	40%	27%	13%	6%
1,000 to 9,999	11%	8%	17%	23%	19%	16%
More than 10,000	7%	2%	15%	35%	64%	68%
Don't know	2%	2%	3%	2%	0%	10%

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, 16% of organisations reported processing sensitive data. The majority (75%) of these organisations reported processing 'special category' data. Another 50% of organisations that reported

processing sensitive data reported processing personal data for children and young people under 18 and 27% 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 19% 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.

83% 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, 48% of organisations with more than 250 employees reported that more than 250 full-time employees are at least partially responsible for managing data compliance. Similarly, 55% of organisations with 50 to 250 employees reported that 50 to 250 employees were responsible for their data protection compliance.

However, we note that we have identified discrepancies within this survey question. For example, we note that sole trader organisations reported that between two and nine employees are responsible for their data compliance. Whilst we are aware of these inconsistencies, we have maintained the organisations' original responses. We will look to improve response consistency and identify whether there is justification for indicating a higher number of employees responsible for data protection compliance than the organisation's number of employees in the next iteration of the survey, by cross-checking responses to this question with responses to organisation size or introducing confirmation prompt and requesting explanations where these numbers do not align.

How data is used by organisations

Purpose of processing

Organisations process personal data for a variety of reasons. 37% 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. 30% of respondents reported regulatory or statutory requirements and 21% 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.

Data controllers in action: why data controllers process data

Views from a non-profit theatre and arts venue

The theatre and arts venue collects personal data through their box office sales, collecting audience information such as name, address and email. Box office data is held for a year before being deleted, but customers can consent to the continued storage of their personal data if they opt-in to a mailing list.

The data controller at the venue spends 50-60% of their time on data issues related to keeping the data up to date and deleting old records.

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. 52% of organisations reported that processing personal data is essential to the core functions of their business model and 49% 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 (86%) or supporting (86%) 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 (93%) acquired personal data directly from customers or the public. 24% of organisations reported acquiring personal data through other businesses or organisations, in the course of providing products or services and 13% of organisations reported acquiring personal data from publicly available databases. 10% of organisations reported acquiring personal data through cookies or similar online tracking technologies and 10% 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 (5%) and from public bodies such as government departments, HRMC, NHS etc (1%).

Storing personal data

75% of organisations reported holding personal data digitally. This increases with organisation size, with

more than 90% of organisations with more than 50 employees reporting that data is being held digitally.

Data sharing

15% of organisations reported sharing personal data outside of their organisation. This was more pronounced for organisation processing higher volumes of personal data, with 29% 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 (50%), employees (34%) and customers or stakeholders (28%).

The most common recipients varied based on organisation characteristics. For example, 94% 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 employees. Similarly, public sector organisations sharing personal data outside of their own organisation most commonly reported sharing this data with other public bodies (77%).

8% of organisations surveyed reported sharing sensitive personal data outside of their organisation. Sensitive data was shared most commonly with employees (49%), public bodies such as government departments (44%) and other businesses or organisations (40%).

Overall, 7% 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 56% and 23% of organisations sharing data internationally reporting these as a destination respectively.

Technology adoption

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

IT function management

The majority (72%) of organisations reported managing their IT functions in-house, with all IT functions performed by internal staff. 6% 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, organisations with more than 250 employees reported using a hybrid IT function more often (49%). Similarly, 28% of organisations processing personal data for more than 10 million data subjects reported managing their IT functions entirely in-house.

Technology used 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 36% and 27% of respondents reporting their use, respectively. Organisations also reported using physical data servers (24%), encryption (22%) and cloud processing facilities (14%). 20% of organisations reported not using any digital technologies, for example due to all data being held physically.

Data controllers in action: technology used by data controllers

Views from an auction house

The auction house holds personal data including names, addresses, contact information and banking arrangements to update client on the progress of their orders, arrange sales and execute wills.

The data is stored both on paper and in digital copies. Paper copies are stored in A4 files which are locked in a storage cabinet in a back office accessible only to staff. Digital records are saved in the cloud and are only accessible on computers with a licensed software. Information stored in this software is structured with different levels of access and clearance.

Technology considered but not used by data controllers

15% of organisations had considered adopting cloud storage but ultimately decided not to. 13% and 12%

respectively of organisations that considered adopting encryption and software / hardware for managing data protection compliance ultimately decided not to.

These percentages are much higher for organisations with more than 250 employees or organisations processing personal data for more than 2 million data subjects. For example, more than half of respondents in organisations with more than 250 employees that do not use cloud storage, software or hardware for data protection compliance and physical data servers reported having previously considered adopting the technologies. 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 physical data servers had previously considered adopting these technologies.

A variety of factors contributed to organisations considering but not adopting certain technologies. With 58%, the most common factor for organisations considering but not adopting a technology was that organisations ultimately saw no need. Other reported factors included lack of expertise or staff training required (49%), high cost of the technology (44%) and lack of time for the implementation (37%). Organisations also highlighted the role that data protection law plays in the adoption of technologies; 42% of organisations that considered but chose not to adopt technologies highlighted the effort required to understand compliance requirements and 23% reported legislative requirements as a factor for ultimately not using the technology.

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. It provides insights into organisations' nuanced view of regulation as both an enabler and constraint in different circumstances.

Awareness of data protection law and the ICO

Familiarity with data protection law

The majority of organisations reported feeling very (16%) or fairly (48%) familiar with data protection law. 24% of organisations reported not being very familiar and 12% reported not being at all familiar with data protection law.

Familiarity increased with organisation size, with 40% and 53% of large organisations (with 250+ employees) reporting they were very or fairly familiar with data protection law respectively.

Public sector organisations were also more likely to report familiarity with data protection law, with 77% reporting they were fairly or very familiar.

Awareness of the role of the ICO

59% 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 (84% of large organisations with more than 250 employees in comparison to 55% of sole traders that were aware of the ICO).

Table 3: Proportion of respondents reporting awareness of the ICO, by organisation size

Survey questions: B1. Approximately how many people does your organisation employ? 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	Total	Sole traders	Micro	Small	Medium	Large
Yes	59%	55%	69%	81%	92%	84%

Awareness of the ICO was also more pronounced for organisations that reported processing higher volumes of personal data. For example, 49% of organisations that processed personal data for less than 100 data subjects reported being aware of the ICO. In comparison, 94% 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. 72% of organisations aware of the ICO prior to completing the survey agreed that the ICO resources provide clarity about what the law requires and 49% agreed that the ICO understands the issues that their organisations face. 49% of organisations that were aware of the ICO agreed that the ICO understands and anticipates developments in the markets it regulates and 31% agreed that the work of the ICO reduces compliance costs.

Table 4: 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”.

Statement	Proportion of respondents in agreement
The ICO resources provide clarity about what the law requires	72%
The ICO understands the issues you face	49%
The ICO understands and anticipates developments in the markets it regulates	49%
The work of the ICO, for example the Business Advice Service and Certification Schemes, reduces your compliance costs	31%

The findings also highlight that the ICO’s support and advice services provide a valuable resource to many organisations. 58% 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 ICO guidance to improve understanding with UK GDPR, PECR, FOIA, EIR, and NIS (33%) and to improve understanding of compliance activities such as ROPA, DPIA (20%).

These proportions are lower when filtering for only sole traders, where 51% 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 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. 32% 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. 35% of respondents

provided a neutral response (reporting “neither agree nor disagree”) and 26% of organisations disagreed that data protection law had been an enabler.

These results vary by an organisation’s characteristics. For example, 87% of medium and large 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 68% and 54% 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. About a third of respondents agreed that data protection law has revealed data security and compliance gaps that they are addressing (33%). 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 45% 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 33% 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. 30% of organisations agreed that data protection law has helped identify, use and store personal data more efficiently and at a lower cost and 26% of organisations agreed that data protection law has helped identify new uses of personal data to improve or expand existing products or services.

Data controllers in action: data protection law as a motivator for change

Views from a vehicle leasing brokerage firm

The organisation collects client personal data, including date of birth, address and medical conditions to provide their vehicle leasing service.

For their organisation, new data protection laws acted as motivation to implement new data protection compliance activities that they were planning to introduce sooner, rather than later. As a result, improved controls, including password-protected security backups and e-signature services, were implemented more quickly, with positive effects.

“We have always been used to dealing with personal data and how important it is to protect people,” the interviewee noted, “[data protection regulation] probably forced us to make changes earlier than we would have done.”

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 (52%), cyber security concerns (49%) 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. 49% of respondents reported challenges in ensuring personal data is not out of date and 48% 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 (38%) and a lack of clarity about regulatory requirements (35%) as key challenges. An additional 33% 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 73% of organisations reported that data protection law had placed little to no constraints on their core activities, 24% 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 86% and 71% 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. 71% 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 high compliance costs as the most common constraint (44%). Uncertainty is also cited as a cause of constraint to organisation's core activities, with 42% of respondents reporting a lack of clarity about data protection law requirements and 40% citing uncertainty about adopting innovative products or services with unclear compliance assurance as key constraints.

Data controllers in action: data protection law as a barrier

Views from a Category C adult prison

Within the prison system, personal data is often shared with third-parties for legal representation or rehabilitation purposes. A representative from a UK prison reported that data protection regulation had introduced delays around information sharing.

For example, the interviewee noted that the regulation was making it more challenging to share information with solicitors. “We have to go back to [the solicitors] and get them to send a form into the prisoner and then the prisoner has to get back to us [...]. It makes some of our work long winded.”

Similarly, data protection laws have made it more challenging to share personal data with rehabilitation and support facilities without obtaining consent: “We want to share information and we want it to be as easily accessible as possible.[...] When we get those barriers, it slows it down.”

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, 35% of organisations reported facing costs as a result of complying with the UK GDPR. These costs presented themselves in the form of one-off direct costs (reported by 20% of organisations) and one-off indirect costs (11%), ongoing direct costs (19%) and ongoing indirect costs (14%).

Common costs include software, reported by 44% of those respondents that incurred costs, existing employee undertaking regulatory compliance training (31%), existing employee undertaking regulatory compliance work (29%) and hardware (26%).

Of those respondents that reported having incurred costs of complying with the UK GDPR in the last 12 months, 64% of respondents reported compliance costs of less than £10,000. The cost of compliance is seen to increase in tandem with organisation size. The majority of sole traders (84%) reported a total cost of compliance of less than £10,000 over the last 12 months.

Data controllers in action: costs incurred by data controllers

Views from a business providing shipping containers storage solutions

GDPR was one of the core factors behind the business becoming a paperless organisation. As part of this move to a paperless system, tablets were purchased, totalling £9,000.

In addition, this business spent approximately £8,000 on encryption software and introduced 2 factor authentication on all login events to better protect the personal data stored.

Despite the initial cost, the organisation felt there would be savings in the future, such as using less paper, and printing.

“I would say in three years it will pay for itself.”

Data protection law as an enabler and a constraint

Our study also revealed that more than 15% of organisations see data protection law as both a constraint

and enabler at the same time. In fact, 64% 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.

Data controllers in action: data protection law as a constraint for one core activity and an enabler for others

Views from a Parish Council

Councils may need to collect personal data for a variety of reasons, including for the management of allotments, taking bookings for Parish halls and verifying identities at Council meetings.

A representative of a UK Parish Council explained how the introduction of the UK GDPR has resulted in both negative and positive consequences to their operations.

On one hand, the Council representative explained that following new data protection guidelines, they were restricted in their social media promotion practices as they were no longer able to use photos with young people: "One of the unintended consequences I suppose was around photography and young people's images, where we used to take pictures randomly and use them on social media. Now as a general policy we don't take photographs simply because it's not always possible to get everybody's permissions." They have tried to mitigate this issue, but the paperwork was too onerous and have therefore been more limited in the social media promotions they can publish.

On the other hand, the Council noted greater engagement in consultation meetings once data minimisation principles were implemented. The Council previously collected personal details to gather feedback on Council activity and policy but adopted a new anonymised feedback system following the introduction of the UK GDPR. "In the past we would have asked for names and addresses but now, because we are aware of data protection much more, we don't do that," noted the interviewee, "It wasn't necessary to get people's information."

The results were unexpected but positive. Since the Council started to explicitly state that the consultation meetings would be anonymous, they noticed greater engagement, and that participants were freer with their opinions. "The consultations have a much better outcome because it's anonymous whereas previously it was attributed to them."

Overall, the Parish Council representative found that data protection regulation have been positive: "We thought it was going to be really onerous and it's actually turning out to be beneficial which is certainly something we were not expecting".

Overview of data controller qualitative interview findings

In addition to the quantitative Data Controllers Study survey, IFF conducted 20 follow-up interviews with data controllers in order to provide more context and to delve into some of the findings of the survey. The interviews were held between 29 November 2023 and 2 February 2024.

The main themes of the responses are summarised in a [short visual infographic](#) and in full below. We have also noted variations in responses across the participants, reflecting the diversity amongst organisations' views and experiences. The participants were drawn from the participants of the quantitative survey. The Technical Report provides supplementary information about the methodology followed for the qualitative interviews. A broad range of organisations participated including commercial and retail businesses and industrial service providers, legal and accountancy service providers, public and local government organisations and social and non-profit organisations. Although the small sample means that we should be careful when generalising the results, the summary of the main themes of the responses provides valuable additional insight when considering the quantitative survey findings.

Types of processing

As the organisations covered a range of activities and sizes, it is important to note that the scale of data processing, and the data subjects this relates to, vary across the interviews. Some of the respondents dealt with all of the data processing themselves, others employed third party services, such as accounting software, which aided in the management and security of data within the organisation, while others utilised a hybrid approach.

Organisations interviewed also differed in their approach to the use of data within their organisation. Some used data to support the operations of their activities, including commercial exploitation, while others used data to support service delivery, and others used data they held in only very limited cases, such as in the case of a local library.



Views from a Community Library

"The resources we will have used will come from the legal department at the county council but have also spoken many times with Citizens Advice and ACAS, but never the ICO."

All of the organisations interviewed held personal data and some had established approaches for data protection, before the introduction of GDPR. In some cases, this changed a lot following the introduction of the legislation, with organisations mentioning they were not as able to access or share personal data as they were before introduction of the legislation, while in others it represented only minor changes to existing methods for protecting data held by the organisations and was seen as beneficial for creating structures and establishing processes.



Views from a local sight loss charity

“I could imagine for other people that didn’t already have this in place it would have been difficult, but because we did – it sounded scary when it was announced but then had a look and realised we were already doing it all; now we record that we are doing it rather than naturally doing it.”

Views on data protection legislation

The quantitative survey findings indicated that while 32% of data controllers found data protection law to be an enabler to their core activities and 24% perceived data protection law as a constraint at least to some extent, 16% of data controllers suggested that data protection legislation had acted as both an enabler and a constraint on their core activities. The qualitative interviews provide insight into these views, discuss the positive and negative impacts of the legislation, and delve into some data controllers’ views that concurrently discuss both aspects of data protection legislation for their activities.

Of those data controllers interviewed, eighteen were either positive or neutral about the overall impact of regulation on their operations, with the majority of this group discussing positive impacts. Those data controllers reporting the impact of legislation as overall positive, identified a range of benefits, including the streamlining of existing practices, clarity on what could be done and improving the confidence of customers and public services users, relating to their data. Respondents also mentioned unanticipated benefits, such as improved public consultations due to introduction of anonymity in a parish council’s consultation process and reduced printing costs due to providing advertising material only to customers that had joined a theatre’s mailing list. Costs, which included training, software and hardware, were not viewed as outweighing these benefits, and in many cases were seen as an ongoing cost of operating, rather than being specifically related to legislation such as GDPR



Views from a plant nursery

“And that benefits our business...a big chunk of our business is online, either directly or indirectly...And if individuals don't feel that they are well protected then I am sure they would find alternative ways to shop.”

Agreement that the impact had been positive was not universal; two data controllers felt that the impact had been negative overall. A small retailer expressed a view that broadly all regulation introduced by the Government increased costs and made their business harder to run and was therefore unable to identify the value that regulation could provide for organisations. A respondent providing insights from a public organisation, a prison, suggested that the requirements of gaining permission for accessing and sharing data was making it harder for them to efficiently achieve their objective of rehabilitating prisoners. These views provide an important comprehensive insight in data controllers’ experiences engaging with regulation put in place.

The costs of compliance

When discussing the introduction of legislative requirements, such as the introduction of data protection law, it would not be unusual to observe monitoring and compliance costs for organisations. The quantitative findings have indicated that 35% of organisations have faced costs in order to comply with UK GDPR in the past 12 months. Data controllers interviewed in the qualitative study identified costs for software and subscriptions, costs of creating a new role to manage data protection policies, costs for data storage and increased liability insurance premiums. The costs generated were not characterised as being significant to the operation of the organisations and in many cases expenditure, such as training, software or revising policies was characterised as part of the ongoing costs of operations. One respondent identified costs as being an issue, though this was not supported by a clear statement of those costs. Overall respondents acknowledge costs in complying with the legislation, however, they broadly seem to perceive them as costs relevant to carrying out their activities.

“

Views from a law firm

“At the time [of the introduction of GDPR] we didn't realise the impact from an ongoing resource point of view. Both direct and indirect, but more indirect. It is difficult to quantify and predict the costs.”

“

Views from a business buying, selling and renting shipping containers

“We have a much better understanding of what we can and cannot do, we've had to change our focus slightly so actually it is not affected us.”

“Nobody understood what it was, but GDPR makes it a lot clearer, both to understand and to follow.”

The ICO's guidance to data controllers

Of those data controllers asked, many had made direct visits to the ICO website and consulted guidance on areas of interest. Views on the clarity and specificity of that information differed - although several noted that the material was clearly presented, others felt it was too technical.



Views from a solicitor, dealing with commercial and private legal issues

“Occasionally, we go to visit the website of the ICO to make sure that there is nothing new, and sometimes on our continuing development courses, we have sections on data protection.”

The findings also highlight that the ICO was one of a range of sources used for obtaining information about data protection legislation. Some relied on parent organisations, others on consultations with related organisations, such as trade bodies, while others relied on providers of accounting software, or other providers of guidance, such as the Citizens Advice Bureau.



Views from an agricultural engineering company

“The main resource again is through our software because they update us as to what the new legislation is.”



Views from a vehicle leasing company

“We normally get guidance and consulting support from the finance company that we deal with.”

Summary

The qualitative interviews are an interesting addition to the evidence from the quantitative part of the Data Controllers Study. They demonstrate that organisations that engage with data protection legislation have developed informed views about the impact of data protection and provide a nuanced insight in data collection, processing and storage, and the costs of compliance. Additionally, the responses demonstrate that the ICO’s guidance and information is not often consumed directly by data controllers, and is often being used in combination with guidance from other sources.