Department for Digital, Culture, Media & Sport

UK Business Data Survey 2021

Summary Report

May 2021

UK Business Data Survey 2021 Summary Report

The UK Business Data Survey is a telephone-based quantitative and qualitative study of UK businesses. It seeks to understand the role and importance of personal and non-personal data in UK businesses, domestic and international transfers of data, and the awareness of, and attitudes toward, data protection legislation and policy.

This is the first time this survey has been carried out. The quantitative survey took place from November 2020 to January 2021 and the qualitative interviews were undertaken in February 2021. The research was delayed from spring 2020 to minimise the impact of the COVID-19 lockdown on the quality of responses and the robustness of the results.

Lead analyst: Robert J Palmer

General enquiries:
enquiries@dcms.gov.uk

Media enquiries:
020 7211 2210

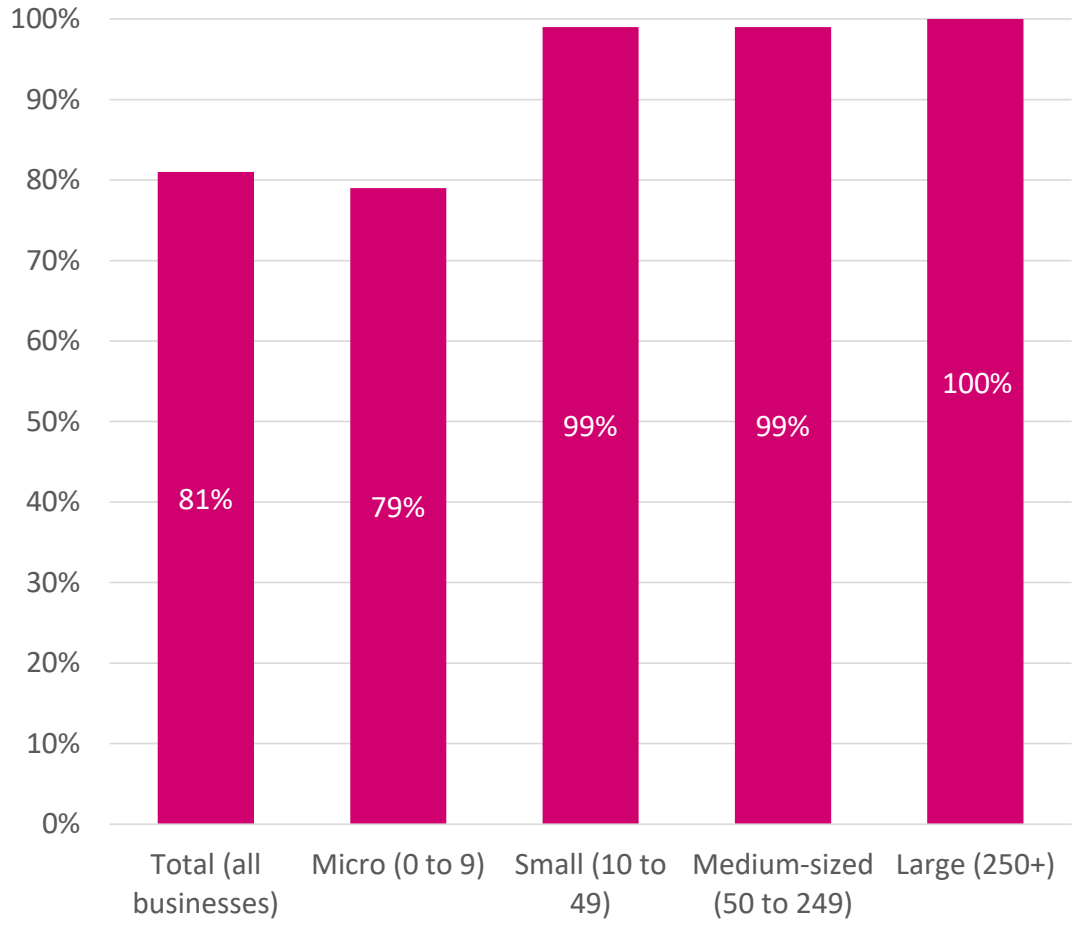
Contents

Summary

The collection, use and transfer of data has become increasingly important during the 21st Century, both to people and to industry. There is continued scope to improve our basic understanding of what data is used for, its value and the importance of being able to move data around, both domestically and internationally. This survey is intended to help the Government develop its evidence base in this regard and is its first iteration.

81% of all businesses surveyed said they handle digitised personal data, digitised non-personal data, or both, and use of data increases considerably as businesses become larger. This includes data collected from the businesses' employees (for example, for HR or payroll purposes) and data collected from elsewhere (such as customer data).

Figure 1: Percentage of businesses that said they handle any form of digitised data (businesses can collect data from both sources shown)



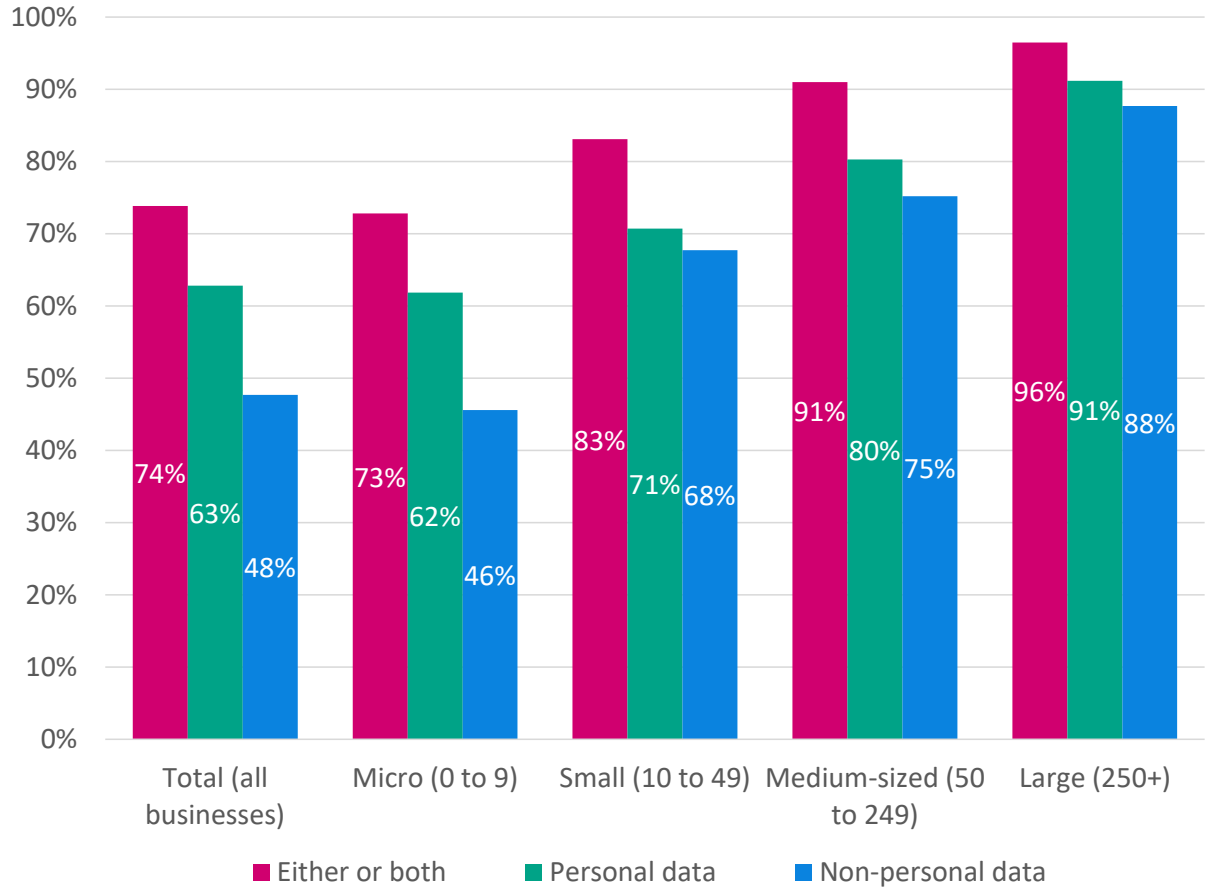
Base: 4,500 UK businesses

Almost all businesses with ten or more employees collect data. Note that micro businesses include sole traders, and that sole traders make up an estimated 76% of businesses[1].

[1] gov.uk/government/statistics/business-population-estimates-2020

Around three quarters of businesses said they collect data other than that collected from employees.

Figure 2: Percentage of businesses that handle data from sources other than their employees



Base: 4,500 UK businesses

Only 4% of large businesses (those with at least 250 employees) said they don't use data from sources other than their employees. However, data use is also widespread among smaller businesses with three quarters of micro-businesses (those with fewer than ten employees, including the self-employed) saying they handle either type of external data.

The following chapters provide some high-level results, both from the quantitative survey and longer, more in-depth qualitative interviews, with businesses across the UK. We plan to undertake further analysis and publish more detailed results, along with tables of data, in the autumn which we hope will prove useful in others' research.

Chapter 1: Introduction

Code of practice for statistics

The UK Business Data Survey is an official statistic and has been produced to the standards set out in the Code of Practice for Statistics.

Background

Publication date: 13th May 2021

Geographic coverage: United Kingdom

The Department for Digital, Culture, Media and Sport (DCMS) commissioned the UK Business Data Survey to help the Department understand the significance of data to industry, what it is used for and how it drives the economy. It also seeks to develop the evidence base around the international flow of data and difficulties encountered, as well the understanding amongst industry of the relevant regulatory framework.

This is the first time this survey was performed and it was carried out by IFF Research. It covers:

- how businesses handle data, the types of data they use and what it is used for
- businesses' awareness and understanding of, and difficulties encountered in, data protection regulations
- businesses' knowledge of and interaction with the Information Commissioner's Office, the UK's data protection authority
- international data transfers and the mechanisms via which these are carried out
- if a business does not use data, what makes them different from businesses that do

Methodology

DCMS commissioned IFF Research to carry out a questionnaire-based telephone survey of 4,500 UK businesses from 10th November 2020 to 29th January 2021. This was accompanied by 20 in-depth interviews in February 2021, to gain further qualitative insights from some of the organisations that answered the survey.

In both cases, the samples were selected to provide robust coverage by UK region, business size (number of employees) and sector. Weighting by these characteristics was applied to the data to ensure that the results reflect the UK business population.

Many questions were asked to a subsection of the overall sample. Where this is the case, it has been indicated in the supporting text.

A screening and question routing process was employed to minimise occasions when businesses initially said they do not collect or use data but in fact do. It was helpful to define what is meant by 'data' for the purposes of this research, and the definition given to respondents at the beginning of the interviews was as follows:

> *"Digitised information that your organisation may hold, for example things such as financial records and names and addresses of employees and customers. All businesses use data in some form, and we are interested in speaking with all businesses even if you only deal with a small amount of digitised data."*

The survey focussed on digitised data since, although non-digitised personal data (such as paper records) is covered by data protection legislation, it is thought that digitised data is by far the more prevalent form, and increasingly so. As such, it considered was better to concentrate the limited sample on businesses that use digital data.

Interpretation of findings

The survey results are estimates and subject to margins of error, which vary with the size of the sample and the percentage figure concerned. Percentage results, and subgroup differences by size and sector, have been highlighted only where statistically significant (at the 95% confidence level).

How to interpret the qualitative data

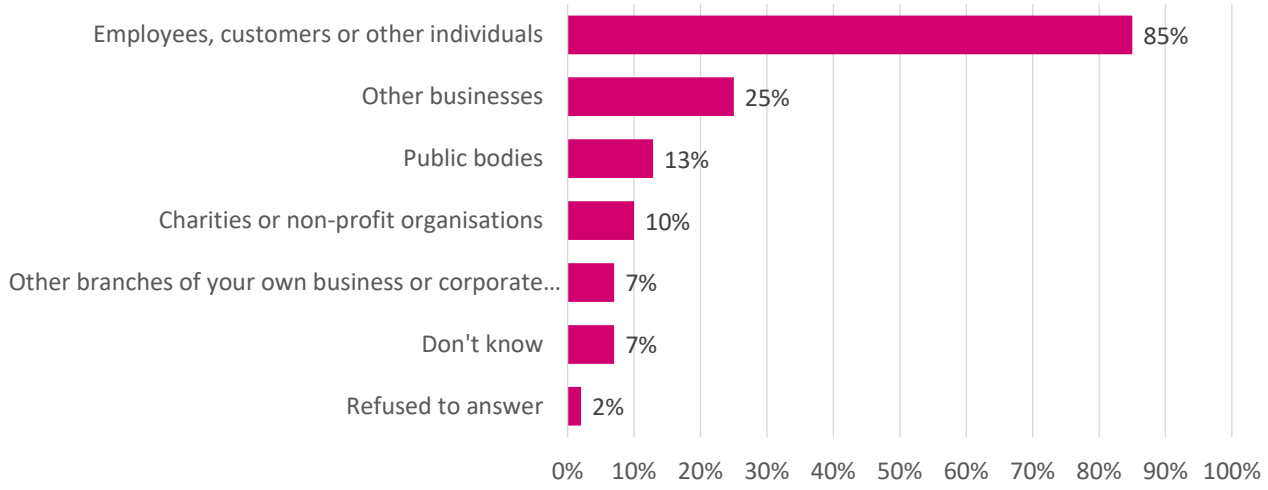
The qualitative survey findings offer more nuanced insights into how and why businesses hold attitudes or adopt behaviours with regards to data. The findings reported here represent common themes emerging across multiple interviews. Where examples or insights from one organisation, or a small number of organisations are pulled out, this is to illustrate findings that emerged more broadly across interviews. However, as with any qualitative findings, these examples are not intended to be statistically representative, and cannot be generalised across the population.

Chapter 2: How businesses handle data

Of businesses that said they use any form of digitised data, 93% said they acquire personal data from individuals through them volunteering information (for example if a new customer registers with them).

As shown in *Figure 3*, of businesses that said they collect *personal* data, either from employees or elsewhere, by far the most common source of personal data is employees, customers or other individuals, with 85% saying they collect personal data from these sources, although a quarter of businesses obtain personal data from other businesses.

Figure 3: Sources of personal data as a percentage of UK businesses who use digital data



Base: 3,630 UK businesses that collect personal data

This was further backed by the in-depth, qualitative interviews where major forms of acquiring personal data is through customers volunteering information, such as customer data through incoming enquiries and orders, employee data as part of prospective employment, among others. For some sectors, revenue would not be possible without personal data at all. As one of the interviewees highlighted:

"If we don't talk to our customers, we are not going to sell them anything."

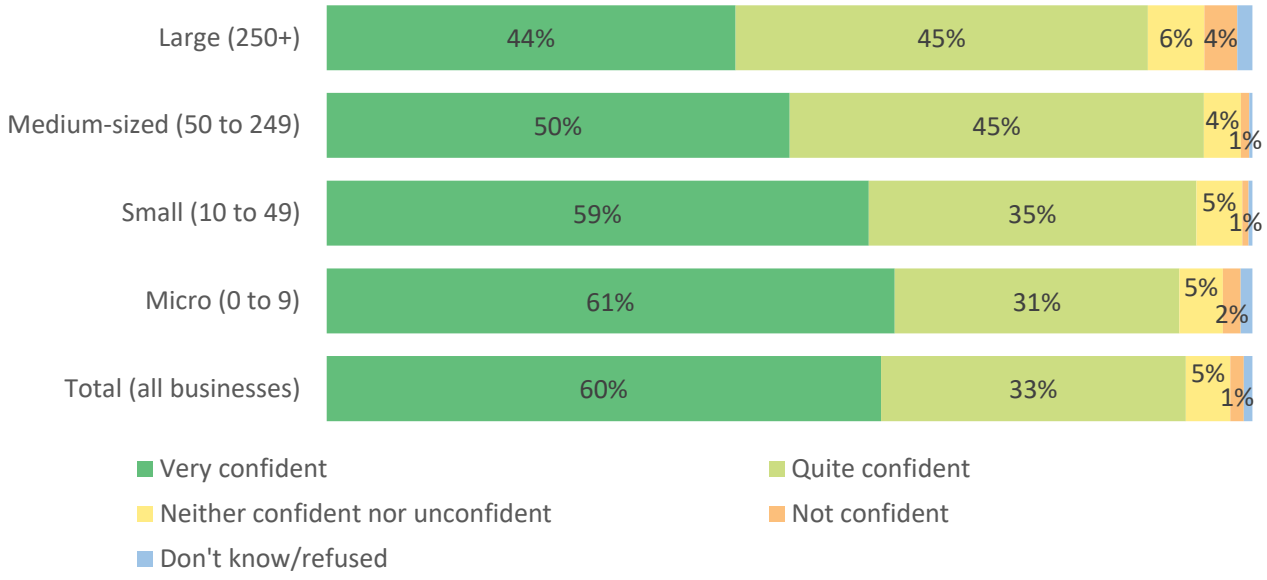
Non-personal data such as sales or stock-level data is also very common, with around half of these businesses saying they generate this type of data. In-depth interviews also added the need for businesses acquiring or generating non-personal data such as sales data to map trends, and carry out financial projections and budgeting. Non-personal data is also used to launch promotions, load/discount prices or understand which products they need to stock more or less of based on sales levels.

DCMS wanted to understand whether or not data-use in business has become easier or more prevalent amongst businesses. Around half the businesses that use digitised data said that data had become more readily available in the last ten years. We asked these particular businesses about the advantages this gave them and around half said that it had enabled them to innovate

and perform new functions. An even larger proportion, around 60%, said that it had led to efficiency improvements.

Around two thirds of UK businesses that collect personal data said they have a privacy management framework or data protection strategy in place. Of the subgroup of those that have employees, the vast majority (93%) felt that their employees were proficient in handling personal data. One business mentioned in an in-depth, qualitative interview that its Data Protection Officer (DPO) has good rules in place to ensure compliance regarding data transfers, and ensure that the right contracts are in place to mitigate the risks.

Figure 4: Percentage of businesses that expressed confidence in their employees' proficiency in handling personal data



Base: 1,909 UK businesses that collect personal data and employ staff

It is possible that this is an overestimate if businesses are reluctant to admit a lack of confidence in their employees' abilities. The level of confidence is slightly lower for large businesses than for small or micro ones. As suggested by the in-depth, qualitative interviews, it may be that the level of confidence expressed is a function not only of the proficiency of the employees but also the complexity of the business's data and related processes.

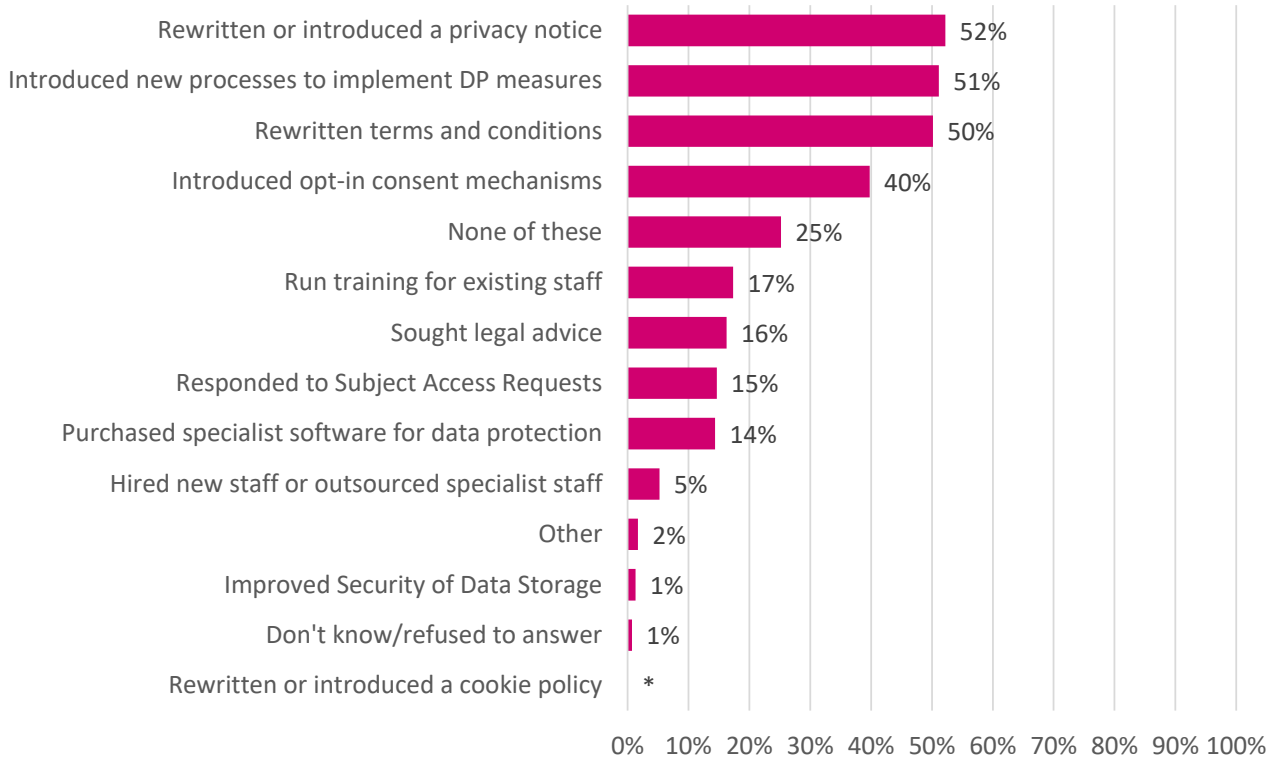
In those interviews, a number of the businesses were 'quite confident' in their employees' abilities in handling personal data. An interview with a privacy and compliance officer of a large business highlighted the complexity of large businesses, noting that they are also aware that their business as a whole "does not really understand the legal rules".

Chapter 3: Data protection regulation

The General Data Protection Regulation (GDPR) was introduced into UK law in 2018, in the form of the Data Protection Act (DPA) 2018. DCMS wanted to learn about businesses' response to this new legislation.

The survey finds that businesses that collect personal data (either from their employees or elsewhere) have performed a number of actions as a result of GDPR and DPA 2018 to, for example, ensure compliance with the legislation.

Figure 5: Percentage of businesses that performed a particular action in response to GDPR and DPA 2018

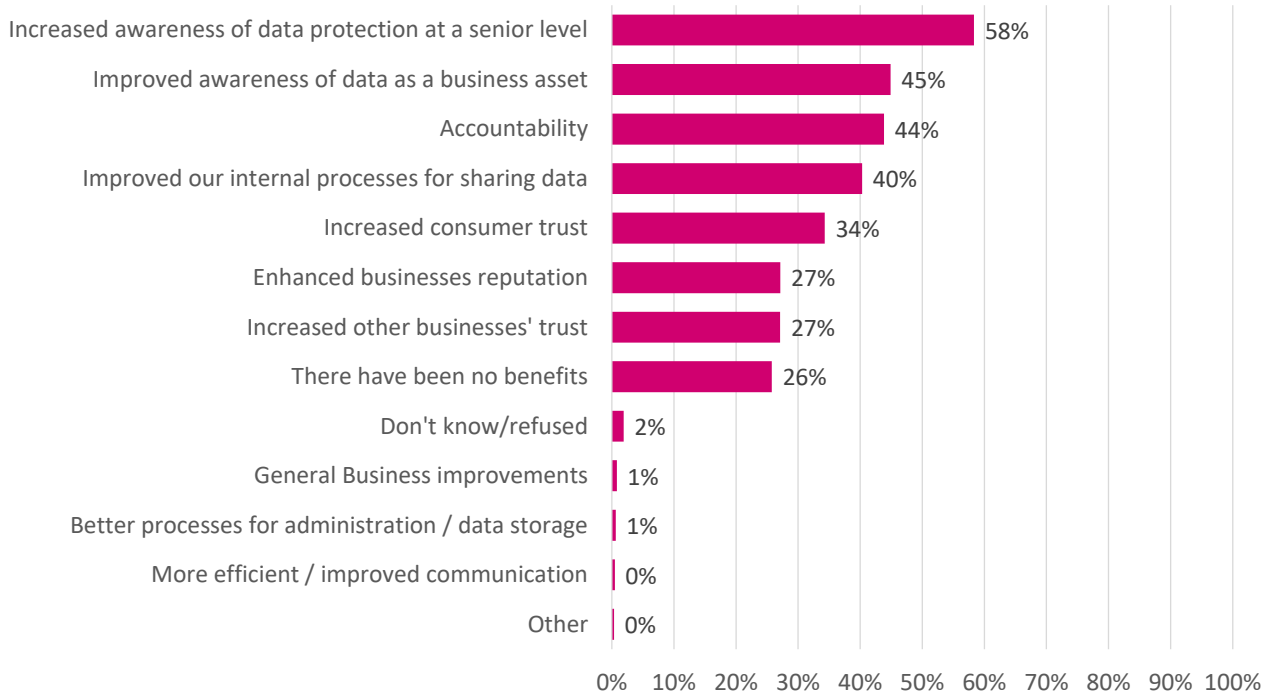


Base: 3,630 UK businesses that collect personal data
**Figure suppressed to avoid disclosure.*

As shown above, the most commonly-stated actions are privacy notices, new processes, terms and conditions, and opt-in mechanisms, which mainly appear to be the more public-facing ones. A little over half the businesses said that they had implemented new processes in order to comply with the rules. A quarter of the businesses said they performed none of these actions, although it is not known why.

A substantial proportion of respondents felt that there had been benefits to their business from the implementation of GDPR and DPA 2018, with only around a quarter saying that there had been no benefits (see *Figure 6*).

Figure 6: Percentage of business that mentioned what, if any, advantages GDPR and DPA 2018 had brought to their business



Base: 3,630 UK businesses that collect personal data

In-depth interviews brought to light other benefits such as more respectful treatment of consumer data, keeping their databases up to date by removing any old data, making regulations clearer and gaining business by building customers' trust and confidence in them.

However, in those interviews, one respondent at a small business mentioned the amount of time they had to spend to train themselves on the subject and put documentation together:

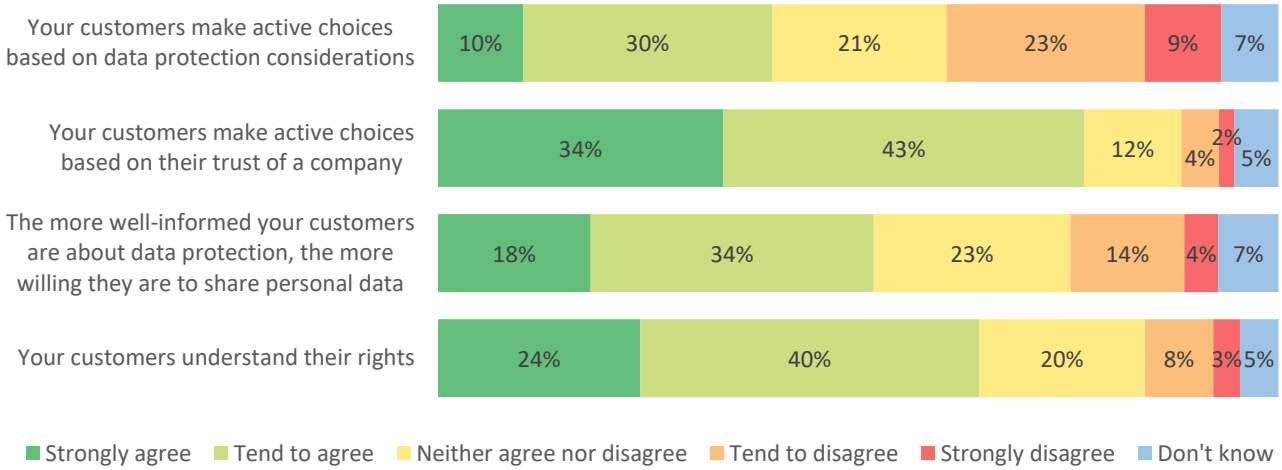
"I had to spend a lot of time reading it and putting documentation in place to confirm that what we were doing was correct."

And a large (250 or more employees) business highlighted the time spent responding to subject access requests:

"We receive over 100k requests per year."

Thinking about businesses' customers, the respondents were asked about the extent to which they agreed with the following statements relating to their customers, GDPR and DPA 2018.

Figure 7: Percentage of businesses that agreed or disagreed with statements about their customers



Base: 3,136 that collect personal data other than from their employees

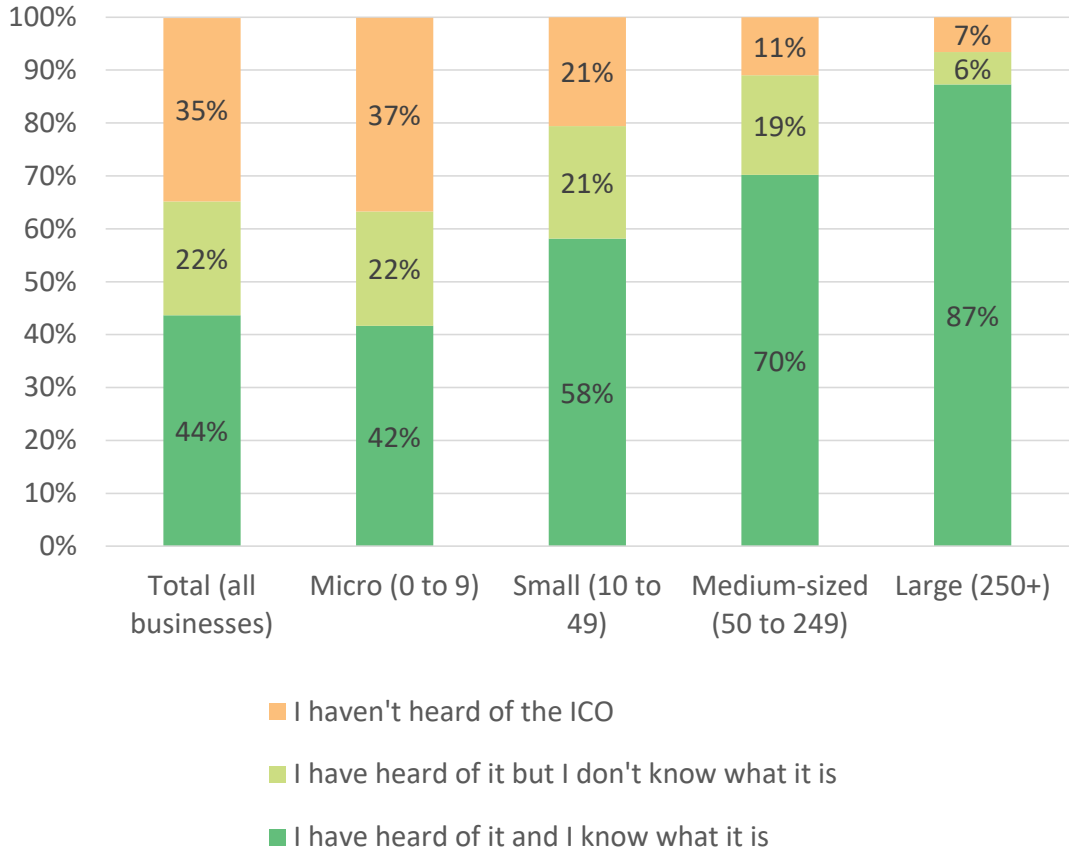
The results in *Figure 7* suggest that businesses consider the trust their customers put in them to be important, with 77% of businesses saying that this influences the choices their customers make. Of the four statements above, the one agreed with least was in regard to customers making choices based on data protection considerations.

Chapter 4: Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights in the public interest. Find out more here: ico.org.uk/about-the-ico

As shown in *Figure 8*, around two thirds (65%)[2] of businesses said they have heard of the ICO, although around a third of those who had heard of the ICO said they did not know what it is. Awareness of the ICO increases considerably with business size, with 87% of large businesses (those with at least 250 employees) saying they had heard of the ICO, compared with 58% of small businesses. Only a small minority (6%) of large businesses said they had heard of the ICO without knowing what it is, compared with 21% of small businesses.

Figure 8: Percentage of businesses that have heard of the ICO or not



Base: 3,945 UK business that collect digitised personal and non-personal digitised data (either from employees or elsewhere)

By far, the ICO-provided service used most often by businesses that have heard of the ICO is its online guidance and Data Protection Hub[3], with 41% of these businesses reporting having used

[2] The figures in the 'Total' bar in the chart don't sum to this due to rounding.
[3] ico.org.uk/global/data-protection-and-coronavirus-information-hub

this service. This service helps individuals and organisations navigate data protection. 70% of businesses that used this service said that they found it to be useful.

Chapter 5: International data transfers

It is important for the Government to understand the nature of the flow of data into and out of the UK, why this is necessary for businesses, and what difficulties businesses face in undertaking the international transfer of data.

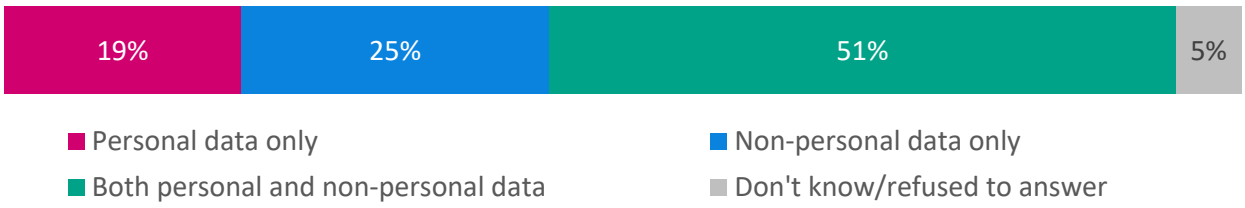
As was shown in *Figure 1* on page 4, 81% of businesses said they use digital data, and this section applies to these businesses only. Only a relatively small minority of those businesses (12%) exchange (send or receive) personal or non-personal data between the UK and organisations or people outside the UK.

This also means that this and the following sections relate to a much smaller sample of businesses than the previous sections. The sample size is nonetheless large enough to provide robust overall results without breaking them down into smaller cohorts such as by size.

10% (12% of 81%) of all UK businesses send or receive digitised data, either personal or non-personal, to/from organisations or people outside the UK.

As data protection legislation is intended to protect individuals from the misuse of data about them, and therefore only applies to personal data, it is important to have an idea of the split between personal versus non-personal data that businesses share internationally. The sample size for this cohort is too small to break *Figure 9* down by business size.

Figure 9: Percentage split between businesses that share personal data only, non-personal data only or both, internationally



Base: 624[4] UK businesses that send or receive data outside the UK

Personal and non-personal data can often be difficult to separate, and so further analysis of the survey data will be required to look into the types of data used by businesses that responded with personal data only or non-personal data only, versus those that use both.

The main reasons given for *not* sharing data internationally were businesses had no business need to do so (92%) or that their business does not operate internationally (78%). Some businesses, around 20%, had concerns about the legal risks and uncertainty of international data transfers, this being of greater concern to large businesses, at around 30%, which also had less of an issue with the resources required.

In-depth, qualitative interviews also highlighted difficulties for businesses in interpreting the laws of a destination country, and the risks involved with transferring data. One large business added that obtaining legal advice from a lawyer about a destination country can present a large cost burden.

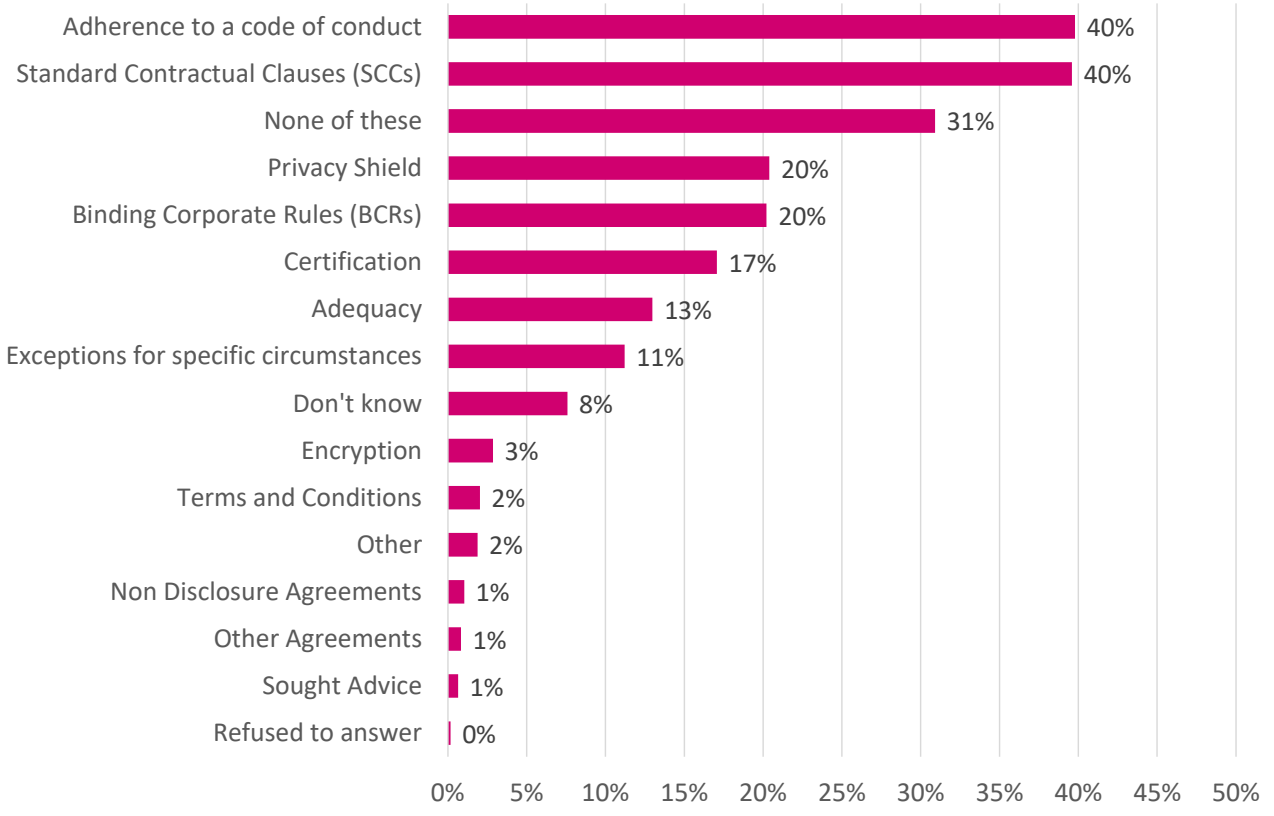
[4] Although this is more than 10% of the sample, the result that 10% of businesses exchange data internationally is derived from weighted data in order to properly represent the UK business population.

Chapter 6: International transfer mechanisms

In *Chapter 5*, businesses that collect and use digitised data were asked whether or not they exchange data (either personal or non-personal data) between the UK and other countries. As mentioned in that chapter, 12% said they did. These businesses were then asked further questions about the legal mechanisms they employ to undertake these transfers.

There are a number of legal safeguards businesses use to lawfully transfer data outside the UK. Some of these, such as Standard Contractual Clauses (SCCs) only apply to personal data, though many can apply to any type of data, such as encryption.

Figure 10: Percentage of businesses that exchange data internationally and that use a particular legal safeguard

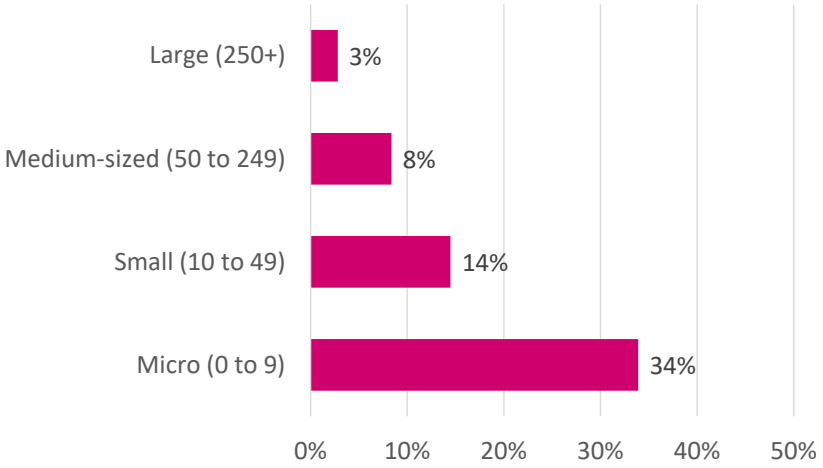


Base: 624 UK businesses that send or receive data outside the UK

As shown in *Figure 10*, the most commonly-used are SCCs and codes of conduct. Please see the *Glossary* at the end of this document for definitions of these safeguards.

In general, it would appear that use of these mechanisms increases with business size. The chart below shows the proportion of businesses that exchange data between the UK and other countries but do *not* use any of these transfer mechanisms, that is, those that selected 'none of these' in *Figure 10* above.

Figure 11: Percentage of business that exchange data internationally but which do not *use any form of legal safeguard*



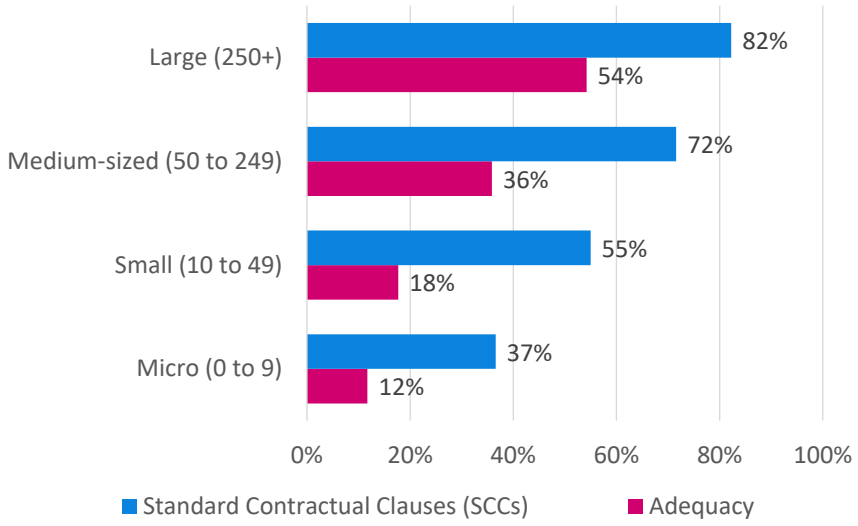
Base: 624 UK businesses that send or receive data outside the UK

Adequacy (see the *Glossary* on page 19 for a definition) is an important mechanism as it enables the free-flow of personal data without needing additional measures such as SCCs and Binding Corporate Rules. Regarding transfers between the UK and countries outside the EEA, this is only applicable to the small number of countries that have been given adequacy status by the European Commission[5] and, by extension, the UK. For EU-UK personal data transfers, the UK has maintained an extension to adequacy status until June 2021. Therefore, EU data protection legislation (GDPR) continued to apply to the UK when the survey fieldwork was completed in January 2021.

The use of adequacy (used by 13% of businesses that exchange data internationally) as a transfer mechanism increases by business size, with 54% of large businesses relying on adequacy compared to only 18% of small businesses.

[5] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.

Figure 12: Percentage of businesses that exchange data internationally that use SCCs and adequacy, by business size



Base: 624 UK businesses that send or receive data outside the UK

Some small businesses that participated in the in-depth, qualitative interviews suggested a need for some guidance from the ICO to help ensure other businesses' compliance, such as government accreditation.

66% of businesses that have implemented SCCs agreed that they facilitate adherence to safe handling of personal data in practice. A higher proportion, around 72%, thought that adequacy facilitated the safe handling of personal data.

Businesses were also asked how easy or difficult, in general, they find using any of these safeguards. 60% of all businesses that used a safeguard said they found it fairly easy or very easy, with 12% saying they found it fairly or very difficult. There is very little difference between businesses of different sizes. A potential explanation is that whilst the necessary expertise is more available to larger businesses, this is balanced out by the increased complexity of larger businesses' data-sharing and data-processing activities.

By and large, the difficulty was attributed to either the requirements being too complicated or bureaucratic, or to a general lack of understanding or difficulty understanding what the safeguards really mean.

Glossary

Adequacy

Data adequacy is a status granted by the European Commission to countries outside the European Economic Area (EEA) which provide a level of personal data protection comparable to that provided in European law. When a country has been awarded the status, information can pass freely between it and the EEA without further safeguards being required. Data adequacy can also be awarded to specified sectors of an economy or international organisations[6].

Binding Corporate Rules (BCRs)

Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group[7].

Code of Conduct (CoC)

Under the UK GDPR, trade associations and other representative bodies may draw up codes of conduct that identify and address data protection issues that are important to their members, such as fair and transparent processing, pseudonymisation or the exercise of people's rights. They are a good way of developing sector-specific guidelines to help with compliance with the UK GDPR. There is a real benefit to developing a code of conduct as it can help to build public trust and confidence in your sector's ability to comply with data protection laws[8].

Encryption

Encryption is the conversion of data from a readable format into an encoded format that can only be read or processed after it has been decrypted. Encryption is the basic building block of data security and is the simplest and most important way to ensure a computer system's information cannot be stolen and read by someone who wants to use it for nefarious purposes. For example, it is utilised by both individual users and large corporations to ensure the security of user information that is sent between a browser and a server on the internet. That information could include everything from payment data to personal information. Firms of all sizes typically use encryption to protect sensitive data on their servers and databases[9].

Non-Disclosure Agreements

Non-disclosure agreements are an important legal framework used to protect sensitive and confidential information from being made available by the recipient of that information. Companies and start-ups use these documents to ensure that their good ideas will not be stolen by people they are negotiating with. These agreements may be referred to alternatively as confidentiality agreements (CA), confidentiality statements, or confidentiality clauses, within a larger legal document.[10]

Privacy Shield

Privacy Shield is an agreement between the EU and US allowing for the transfer of personal data from the EU to US. Privacy Shield is designed to create a program whereby participating companies are deemed to have adequate protection, and therefore facilitate the transfer of information. In short, Privacy Shield allows US companies, or EU companies working with US companies, to meet this requirement of the GDPR[11]. In

[6] Institute for Government (instituteforgovernment.org.uk)
[7] European Commission Official Website (ec.europa.eu)
[8] ICO Website (ico.org.uk)
[9] Kaspersky website (kaspersky.co.uk)
[10] Investopedia
[11] Privacy Trust (privacytrust.com)

2020 the Court of Justice of the European Union in the Schrems II ruling invalidated Privacy Shield for US-EEA personal data transfers.[12]

Standard Contractual Clauses (SCCs)

Standard Contractual Clauses (SCCs) are standard sets of contractual terms and conditions which the sender and the receiver of personal data both sign up to, aimed at protecting personal data leaving the European Economic Area (EEA) through contractual obligations in compliance with the GDPR's requirements in territories which are not considered to offer adequate protection to the rights and freedoms of data subjects. SCCs are particularly important in the sphere of data protection, as these contribute towards a harmonised approach that concerns cross border processing or processing that affects the free flow of personal data or natural persons within the EEA itself, allowing for the consistent implementation of the GDPR's specific provisions[13].

Terms and Conditions

Terms and Conditions is the document governing the contractual relationship between the provider of a service and its user.

[12] CJEU Press Release, July 2020 (curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf)
[13] Lexology (lexology.com)

Further Information

The Department for Digital, Culture, Media and Sport would like to thank IFF Research for its work in developing the survey and carrying out the fieldwork.

For general enquiries contact:

Department for Digital, Culture, Media and Sport
100 Parliament Street
London
SW1A 2BQ
Telephone: 020 7211 6000
enquiries@dcms.gov.uk

This report has been published in accordance with the Official Statistics Code of Practice:
code.statisticsauthority.gov.uk

We can also provide documents to meet the specific requirements for people with disabilities. Please email enquiries@dcms.gov.uk

Department for Digital, Culture, Media & Sport

Any enquiries regarding this document should be sent to us at enquiries@dcms.gov.uk

This document is also available from our website at www.gov.uk/dcms

Department for
Digital, Culture, Media & Sport
4th Floor, 100 Parliament Street
London SW1A 2BQ
www.gov.uk/dcms