

| | |
|--------------------------------------------------------------------------|----------------------------------------------------|
| Title: Data Sharing Code | Impact Assessment (IA) |
| Lead department or agency: Information Commissioner's Office/DCMS | Date: 18/05/2021 |
| | Stage: Final |
| | Source of intervention: Legislative |
| | Type of measure: Statutory Code of Practice |
| Summary: intervention and options | |

What is the problem under consideration? Why is regulatory action or intervention necessary?

The Information Commissioner was required to prepare the Data Sharing Code (the code) under section 121 of the Data Protection Act 2018 (DPA 2018) to provide practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and such other guidance as she considers appropriate to promote good practice in the sharing of personal data.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

As the code and its remit was mandated by Parliament in s121 DPA 2018, it was not appropriate for the Commissioner to consider any alternative course of action. To the extent that the Commissioner had discretion about which issues to cover or how to interpret them within the code, these are described in the body of this assessment.

Will the code be reviewed?

The code will be kept under review in line with good regulatory practice, with s121(2) DPA 2018 allowing the Information Commissioner to make amendments or lay a replacement code.

Data sharing code of practice

[Impact assessment]

18 May 2021

Contents

| | | |
|------|-----------------------------------------------------------------|----|
| 1. | Executive summary | 3 |
| 2. | Background | 6 |
| 2.1. | Problem under consideration and rationale for intervention..... | 6 |
| 2.2. | Approach to the code | 11 |
| 2.3. | Scope of the code..... | 12 |
| 2.4. | Affected groups | 12 |
| 2.5. | Principles and approach | 14 |
| 2.6. | Regulatory constraints | 16 |
| 3. | Costs and benefits of the code | 17 |
| 3.1. | Direct costs and benefits of the code..... | 17 |
| 3.2. | Indirect costs and benefits of the code..... | 24 |
| 3.3. | Conclusions | 27 |
| 4. | Annex A: estimating familiarisation costs | 28 |

1. Executive summary

Data is one of modern society's greatest assets. Sharing personal data can lead to many economic and social benefits, including greater growth, technological innovation and the delivery of more efficient and targeted services. The new data sharing code aims to give businesses and organisations the confidence to share data in a fair, safe and transparent way. The code guides practitioners through the practical steps they need to take to share data while protecting people's privacy. It also seeks to dispel many of the misunderstandings about data sharing.

This impact assessment sets out the benefits and costs associated with the code, drawing on evidence including desk-based research, responses to the call for evidence and consultation on the code, and previous analysis of related issues.

Background

The data sharing code (the code) is a statutory code of practice prepared under section 121 (s121) of the Data Protection Act (DPA 2018). The code does not impose any requirements additional to those in the legislation. It will help controllers to comply with their legal obligations under the UK GDPR¹ and the DPA 2018. The high level objectives of the code are:

- The provision of practical guidance for organisations on the law and good practice in relation to data sharing.
- A better understanding by organisations of how to share data fairly and transparently.
- An improvement in the confidence of controllers to share data responsibly for the public good.
- An increased level of public trust about how their data is used.
- Economic and societal benefits from effective, compliant data sharing.

The rationale for the code is provided by the statutory duty to produce it under s121 DPA 2018. Looking beyond this, the potential to unlock benefits from data sharing, alignment with government policy objectives and the potential mitigation of market failures provide further evidence for the need for the code and a strong economic rationale.

Direct impacts

The direct incremental costs of the code are limited in that many of the requirements set out in the code are part of existing legislation that data controllers are already obliged to abide by.

¹ The GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside an amended version of the DPA 2018. See here for more information: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/>

The key direct impacts assessed are the costs and benefits to controllers of familiarising themselves with the code. The cost of familiarisation to data controllers in terms of the time taken to read through the relevant materials is indicatively estimated at £110 million. The benefits are achieved through helping controllers to comply more easily with existing legislation. These impacts are considered to be an indirect and inevitable consequence of DPA 2018 and the UK GDPR and are therefore not attributable to the code itself.

There is a range of good practice elements to the code covering:

- Data Protection Impact Assessments
- Data sharing agreements
- Data sharing in an urgent situation or emergency
- Sharing personal data in databases and lists

The assessment finds that there are only limited circumstances where there is the potential for an additional burden (perceived or otherwise) to be felt by controllers and that this is significantly outweighed by the benefits of greater regulatory certainty given by the good practice guidance.

Indirect impacts

The indirect impacts are those that come about through a change in behaviour or reallocation of resources following implementation of the code.² Although it is not possible to rule out indirect costs resulting from the code, it is difficult to identify any that are likely to bring about significant indirect incremental impacts and as such the assessment focuses on the potential indirect benefits.

The benefits of the code are inherent in the aim and rationale for it in attempting to overcome barriers to data sharing and providing easier routes to achieving compliance with existing legislation. While the code itself is not directly responsible for the benefits of data sharing and increased data use, it is clear that indirectly it could help to promote, facilitate and catalyse the benefits through behaviour change, improving controllers' confidence to share data, and in turn meeting the first mission of the draft National Data Strategy in unlocking the value of data across the economy.³

Indicative estimates of the benefits of data and increased data sharing are somewhere between £22.2 billion and £55.5 billion per annum.⁴ These benefits could be delivered through:

- product or service improvement;
- access to new markets;

² Further discussion on direct and indirect impacts can be found in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019)

³ DCMS, Draft National Data Strategy, December 2020

⁴ Based on the application of the methodology in: Ctrl-Shift, Data Mobility: The personal data portability growth opportunity for the UK economy (2018), to UK annual GDP from: ONS, Gross Domestic Product at Market Prices (2020)

- more efficient and effective public services and policy making; and
- innovation

With even a minor contribution to unlocking this overall value, the code has the potential to bring about significant benefits.

By promoting good practice and plugging gaps in information, the code will also ensure that benefits and positive spillover effects are maximised while reducing the potential for negative externalities. In addition, it will help to level the playing field by giving confidence to smaller organisations⁵, reducing the barriers to entry into digital markets and encouraging greater competition and innovation.

Conclusion

There is a clear rationale and policy alignment for the code both in terms of the statutory requirement but also in terms of contributing to wider government objectives on data and data sharing, as well as serving to address market failures.

Although quantification of all costs and benefits has not been possible and there are significant uncertainties as to the scale and scope of impacts, the analysis demonstrates that there are limited direct incremental impacts from the code. Where the code has the potential to generate incremental impacts, it is through its indirect impact on affected groups. The analysis demonstrates the potential for the code to drive significant benefits through increased confidence in data sharing which could in turn contribute towards unlocking substantial benefits to the economy and society.

In conclusion, the assessment finds that the code is likely to deliver significant incremental impacts that are beneficial.

⁵ <https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/whats-new/blogs/data-sharing-when-is-it-unlawful/>

2. Background

2.1. Problem under consideration and rationale for intervention

This section provides an overview of the context of the code, the potential value of increased data sharing and relevant market failures relating to digital markets and data sharing.

2.1.1. The data sharing code

The data sharing code (the code) is a statutory code of practice prepared under section 121 (s121) of the Data Protection Act (DPA 2018). It will soon be laid before Parliament.

It replaces the old statutory data sharing code laid under the Data Protection Act 1998. In addition, the code reflects changes in the type and amount of data stored by organisations, as well as advances in technology.

The Information Commissioner was required to prepare the code in order to provide practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation and such other guidance as she considers appropriate to promote good practice in the sharing of personal data. The code does not impose any requirements additional to those in the legislation. It will help controllers to comply with their legal obligations under the UK GDPR⁶ and the DPA 2018.

The code contains some optional good practice recommendations, which do not have the status of legal obligations but aim to help controllers adopt an effective approach to data sharing that both complies with the law and increases public trust.

High level objectives of the code

Bearing in mind the requirements set out above the key outcomes of the code are intended to be:

- The provision of practical guidance for organisations on the law and good practice in relation to data sharing.
- A better understanding by organisations of how to share data fairly and transparently.
- An improvement in the confidence of controllers to share data responsibly for the public good.

⁶ The GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside an amended version of the DPA 2018. See here for more information: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/>

- An increased level of public trust about how their data is used.
- Economic and societal benefits from effective, compliant data sharing.

Policy alignment

An important part of the context for the code and its objectives is its alignment with government policy. The most relevant and recent policy is the government's draft National Data Strategy, updated in December 2020, which looks at how the UK's existing strengths can be used to boost the better use of data across businesses, government, civil society and individuals. The strategy has five main missions which set out the priority areas for action for the strategy. The table below shows the missions that the code most closely aligns with:

| Draft national data strategy missions | Data sharing code alignment |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unlocking the value of data across the economy | The code's key aim is to enable businesses to share data more confidently and in the process is expected to unlock significant economic value as discussed in section 2.1.2. |
| Securing a pro-growth and trusted data regime | The code has been developed with a focus on reducing the burden to businesses and other organisations whilst promoting the benefits of increased and responsible data sharing. |
| Transforming government's use of data to drive efficiency and improve public services | Examples of the benefits of increased data use include the improvement of the effectiveness and efficiency of public services (see section 2.1.2) |
| Ensuring the security and resilience of the infrastructure on which data relies | The code provides controllers with advice and good practice recommendations to help ensure data sharing is done securely which includes investing in the infrastructure that supports this. |
| Championing the international flow of data | Although the code does not cover international data sharing, many of the same principles apply to enabling responsible data sharing internationally. |

As demonstrated, the code aligns well with recent relevant policy and has the potential to assist in progressing government objectives.

2.1.2. The value of data and data sharing

The value that increased data sharing and data use can bring to the economy is very significant. The draft National Data Strategy describes data as the driving force of the world's modern economies.⁷

Estimating the benefits of increased data use and sharing is difficult and the existing literature is limited.⁸ Indicative estimates place the potential increase in a country's annual GDP at somewhere between 1% and 2.5%,^{9, 10} which is equivalent to between £22.2 billion and £55.5 billion when applied to estimates of UK annual GDP as of 2019.¹¹ Although precise estimates are not practical to make, the evidence is clear that there are significant potential benefits from greater data sharing. Some examples of how these benefits could arise are provided below.

Product or service improvement

Data can provide useful insights through trends, patterns and associations that improve the products offered by an organisation. The ability to share data in order to aggregate data sets is imperative to gaining such insights and thus realising the economic benefit.¹²

Case study: Open banking

The code refers to open banking which enables businesses to offer improved services to customers using their personal data. For example, a fintech company can offer a service that helps customers to save by automatically transferring money from their current account to savings every month based on an analysis of their spending. This use of their personal data benefits the customer by increasing their savings and reducing inconvenience for them, and all takes place within a framework that protects the customer's privacy. It benefits the bank because it allows it to benchmark products against competitors and reach new customers more easily, and provides evidence for anti-fraud prevention checks and customer verification, which is also in the public interest and can lead to further product or service improvements.

The quality of data may also be considered a barrier to effective data sharing. This could relate to the accuracy of data, how complete it is, or even whether it

⁷ DCMS, Draft National Data Strategy (2020),

⁸ OECD, Measuring the Economic Value of Data and Data Flows (2020), page 9

⁹ OECD, Enhancing Access to and Sharing of Data (2019), page 11

¹⁰ Ctrl-Shift, Data Mobility: The personal data portability growth opportunity for the UK economy (2018)

¹¹ ONS, Gross Domestic Product at Market Prices (2020)

¹² HM Treasury, The Economic Value of Data: Discussion paper (2018) page 4

is interoperable or linkable across various systems. The data sharing code of practice gives practical guidance, such as undertaking a thorough DPIA and setting out what factors to consider when planning to share personal data. This ensures the data is accurate and complete at the point of collection, so that high quality data is used and the need to clean data prior to sharing is minimised.

Access to new markets

The OECD notes that sharing personal data between private organisations can often provide access to new customers and markets, allowing organisations to work together without the need for mergers and acquisitions.¹³

Case study: Air travel reward schemes

Airline companies often share personal data from their rewards schemes with credit card companies, so that if customers use a particular credit card for everyday purchases, they gain rewards such as free air travel or upgrades. This results in better performance for both companies, whilst they maintain their competitive advantages. It also creates benefits for customers, such as gaining rewards with one company for purchases they make with others.

More efficient and effective public services and policy making

The more high-quality data available, the better the public sector can design more focused and evidence-based policies.¹⁴ Further benefits can be seen in the efficient delivery of services, particularly public services, that more closely meet people's needs and improve their lives.

Case study: Health services

Sharing data in the healthcare sector between GPs regarding patient hospital activity and health conditions enables healthcare practitioners to identify those patients most at risk of hospital admission. In one county, healthcare practitioners were able to use this high-quality data to focus services on this high-risk group, resulting in a 30% reduction in hospital admissions. Not only does this provide a better service for patients but it highlights that data helps services to be provided in a more cost-effective manner.

¹³ OECD, *Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies* (2019) pages 45-46

¹⁴ Verhulst, S., (2019), "Sharing Private Data for Public Good", Project Syndicate

Innovation

Data sharing can lead to significant future innovations. Although the nature of innovation makes it difficult to identify exactly what these will be, past evidence demonstrates that increased data sharing can and has enabled significant innovations that have in turn led to benefits to society.

Case study: Digital identities

The use of digital identities has come about due to the ability of service providers and individuals to share their identity online. This means data subjects only need to provide proof of identity once which can then enable them to access and manage their use of multiple services. More secure data sharing is now enabling government departments to further the use of digital identities and invest in their use for a wider variety of services, reducing the time and potential security threats involved with multiple identity checks through the UK Digital Identity and Attributes Trust Framework. The framework is still in its early stages but it is hoped it will enable innovation from providers and give people the confidence to use digital identities.

2.1.3. Market failure rationale

From an economic point of view, data and digital markets have the potential to raise a range of market failure issues.¹⁵ Market failures are instances where the market alone is not resulting in an efficient outcome for the economy and society more widely, providing a rationale for intervention. This can be exacerbated when multiple market failures are present in combination.

Key market failures in relation to data and digital markets¹⁶ can be summarised as follows:

- **Data as a public good:** data that is shared is non-rivalrous (multiple parties can use it simultaneously without diminishing its usefulness) and in some instances non-excludable (not possible to exclude individuals from using it) meaning that individuals and organisations may not be adequately incentivised to invest in and embark on data sharing as they are not able to reap the full rewards of doing so. This means intervention may be required to improve these incentives.
- **Externalities:** data sharing can lead to significant positive and negative externalities (some of which are discussed in 2.1.2) which are impacts that

¹⁵ HM Treasury, The Economic Value of Data: Discussion paper (2018)

¹⁶ For more discussion on the market failures associated with data and data sharing see: Competition Markets Authority, Online Platforms and Digital Advertising Markets Study (2020) Appendix T; and HM Treasury, The Economic Value of Data: Discussion paper (2018)

are felt by individuals and organisations who are not directly involved in the transaction. This can mean that intervention is required to promote and encourage positive externalities whilst reducing the potential for negative externalities to occur where they are not already accounted for.

- **Information failure:** controllers often don't fully understand the implications of data sharing or what is necessary to comply with legislation, leading to inappropriate data sharing or an aversion to data sharing. Data subjects are also not fully aware of how and why data is being shared, leading to a lack of trust and willingness to agree to data sharing now and in the future. This can lead to information failures that disincentivise data sharing and require intervention to address.
- **Economies of scale and scope:** increased data sharing can lead to more data being collected and/or different data sources being combined. This can bring additional insights which can lead to additional benefits in terms of innovation and service provision. It can also incentivise controllers to hoard data and/or restrict its sharing to gain a competitive advantage and distort markets. Intervention may therefore be required to promote the benefits of economies of scale and scope whilst sustaining competition.
- **Coordination failures:** to fully realise the benefits of data sharing, a number of factors need to align between the parties and the data itself (eg timing, trust, operability, communication). Intervention is sometimes required to ensure coordination.
- **Distributional impacts:** as data sharing affects, to some extent, all of society, there is the potential for impacts to occur that affect particular groups more than others.

2.1.4. Summary of rationale for intervention

The rationale for the code is in the statutory duty to produce it (s121 DPA 2018). However, beyond this the potential to unlock some of the benefits of data sharing, alignment with government policy objectives and the market failures identified, provide further evidence for the need for the code and a strong economic rationale.

2.2. Approach to the code

The development of the code was supported by a substantial body of evidence including extensive consultation. A call for views commenced in August 2018 to inform the initial drafting of the code, for which 101 responses were received.¹⁷ This was then followed by a public consultation on the draft code, concluding in September 2019 for which there were 152 responses.¹⁸ This included

¹⁷ <https://ico.org.uk/media/about-the-ico/consultations/2615362/data-sharing-code-call-for-views-summary-of-responses.pdf>

¹⁸ <https://ico.org.uk/media/about-the-ico/consultations/dsc/2618904/data-sharing-code-summary-of-consultation-responses.pdf>

stakeholders from industry, academia, the public sector and the community and voluntary sector as well as individuals. Alongside this, in-person consultations were held with representatives from government departments, arm's length bodies and devolved administrations between 2018 and 2020 which included representatives from 13 organisations.

The consultation responses picked up on a wide variety of themes from the code including data ethics, security, and technology. The responses provided were integral to the initial drafting and re-drafting of the code. Care was taken to ensure that perceived burdens to controllers were removed or minimised with the final version reflecting a wide range of helpful inputs. Adaptations included removing guidance that was perceived as onerous to ensure the code does not place significant time or cost burdens on controllers, as well as publishing additional SME summary guidance to reduce the burden on smaller organisations.

2.3. Scope of the code

The code focuses on the sharing of personal data between controllers, ie where separate or joint controllers determine the purposes and means of the processing of personal data, as defined in UK GDPR Article 4(7). The code does not cover sharing with processors, which are defined in UK GDPR Article 4(8).

There is no formal definition of data sharing within the legislation, although the scope of the code is defined by s121 DPA 2018 as "the disclosure of personal data by transmission, dissemination or otherwise making it available". The code describes that this includes:

- providing personal data to a third party, by whatever means;
- receiving personal data as a joint participant in a data sharing arrangement; the two-way transmission of personal data; and
- providing a third party with access to personal data on or via your IT systems.

For the purposes of the code, data sharing does not include providing data access to employees or contractors, nor providing data to processors such as third-party IT processors.

2.4. Affected groups

The affected groups for the data sharing code are wide and varied. It is directly relevant to many controllers and indirectly relevant to most data subjects. The burden of compliance for data sharing is on controllers, rather than data subjects, and as such the direct impacts of the code are considered primarily for controllers with the indirect impacts considered for all parties.

Data subjects whose data is shared

It is reasonable to assume that the number of data subjects directly affected by data sharing includes the whole of the UK population.¹⁹ According to the latest estimates from the ONS, this stood at around 66.8 million in 2019. It is not possible to say, even indicatively, what proportion is more or less likely to be impacted (positively and negatively) by data sharing or the data sharing code. However, where certain impacts are more or less likely to affect different groups of data subjects, qualitative commentary is provided.

Controllers who are sharing data

These are the controllers that provide data to another controller. It is not possible to state precisely which organisations the code is relevant to. As such, we have made the simplifying assumption that to some extent the code is relevant to all controllers, which includes most organisations as well as some individuals such as sole proprietors. Although data does not exist to accurately describe all controllers, we have collected data on some key groups to provide an indicative quantitative estimate. The key groups and sources are:

| Organisation type | Coverage | Source |
|-------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Businesses | Registered and unregistered businesses and sole proprietors in the UK | ONS, Business Population Estimates, Oct 2020 |
| Public bodies | All Central and Local Government Organisations in the UK | ONS, Business Population Estimates, Oct 2020 |
| Charities ²⁰ | All those registered with the charity regulators in the UK | Charity Commission, Register of Charities for England and Wales, Feb 2021 Charity Commission for Northern Ireland, Register of Charities, Feb 2021 Scottish Charity Regulator, Scottish Charity Register, Feb 2021 |

Although this does not provide coverage of all potential relevant controllers (eg, unregistered community groups), it does help to provide a reasonable and

¹⁹ Although data sharing covers individuals outside of the domestic population, the Impact Assessment is limited to the UK. The same limitation is applied to controllers and other affected groups

²⁰ Note: there is potential for double counting of charities that are registered with charity regulators and also set up as limited companies, however, we don't expect this to have a significant impact on the assessment given the very small proportion of organisations this represents.

proportionate indication of the scale. The indicative estimate of the total number of organisations in this affected group is 6.2 million.

Controllers with whom data is shared

These are controllers that receive data from another controller. It is likely that in many cases this affected group is not distinct from controllers who are sharing data and at some point in time many controllers will fall into each affected group. As such, the indicative quantification of this group is identical to the above at 6.2 million. However, it is important to note the distinction as the way they are impacted by data sharing may differ, particularly the ways in which benefits are accrued through the additional insights that they may be able to gain and subsequently bring about additional value as described in section 2.1.2.

The Information Commissioner

The data protection regulator, with primary responsibility for regulating the UK GDPR, and the DPA 2018. This includes investigating potential infringements of the underpinning legislation and using relevant enforcement powers as appropriate. The Commissioner will be affected as her office will need to provide advice, promote good practice and assess conformance with the code.

Justice system

The justice system will be affected as, in accordance with s127(3) of the DPA 2018, a court or tribunal must take into the provisions of the code in any proceedings before it to the extent that it appears relevant to the questions it is required to determine.

Wider society and third parties not engaged in or impacted directly by data sharing

There are a wide range of benefits that could accrue to organisations and individuals that are not directly involved in data sharing. Examples of these include but are not limited to individuals that receive improved services (eg medical treatments) that result from insights gained by data sharing; supply chain companies that supply or provide services to controllers that engage in data sharing and gain increased revenue as a result of the increased activity of controllers. It is not possible to quantify this affected group but it is likely to include all data subjects and controllers as well as others.

2.5. Principles and approach

The assessment is focussed on the incremental impacts of the code, both direct and indirect.²¹ Impacts are assessed using cost benefit analysis, which aims to identify the full range of impacts of the code; however, it is important to bear in mind that it is not practical to undertake a forensic analysis of all the

²¹ Further discussion on the direct and indirect impacts can be found in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019)

implications of the code. The approach used in this assessment is based on that of the impact assessment for the Age Appropriate Design Code.²²

The evidence base primarily constitutes desk-based research, responses to the call for evidence and consultation on the code, and previous analysis of related issues.

As the code was mandated by Parliament in s121 DPA 2018, the Commissioner did not have an option to consider alternative action or regulatory intervention. For this reason, this assessment does not consider alternative options to drafting a statutory Code of Practice. It is simply an evaluation of the introduction of the code against the counterfactual explained below.

2.5.1. Counterfactual

The 'counterfactual' in an impact assessment is the baseline against which the incremental impacts of the introduction of a policy can be estimated. Absent the introduction of the code, the existing legislation including UK GDPR and DPA 2018 would continue to apply and form the counterfactual for the purposes of this assessment.

In line with impact assessment guidance²³, the assessment assumes compliance both with existing legislation in the counterfactual and with guidance within the code in the absence of specific evidence of levels of non-compliance. This is a simplifying assumption and does not suggest that there is total compliance with existing legislation. It should also be noted that if a lack of compliance were to be identified, it is expected that the code would help to enable controllers to more easily comply with existing legislation and remove barriers such as a lack of awareness or understanding of legislation, therefore improving compliance.

Establishing the counterfactual in this way allows us to then identify what impacts are incremental to the code. As stated in the code and noted above, the code does not impose any requirements additional to existing legislation and as such direct incremental impacts of the code are limited. This is discussed further in section 3.

2.5.2. Analytical approach

The assessment is split into distinct elements, assessing the direct and indirect impacts of the code separately. The approach taken for direct impacts is to assess the key elements of the code that may be likely to generate impacts for any of the affected groups. These are addressed in turn and assessed for their likelihood to create incremental impacts.

²² ICO, Age Appropriate Design: a code of practice for online services – Impact assessment (2020)
²³ BEIS, Business Impact Target: appraisal of guidance (2017)

The assessment of indirect impacts is taken as a whole, since the way in which the key elements of the code bring about indirect impacts is not sufficiently distinct to justify separate analysis.

The impacts of the code fall into three broad categories:

- Incremental impacts of the code: these are impacts that the Commissioner considers can be directly attributed to the code.
- Impacts of the scope and requirements of s121 DPA 2018: the Commissioner considers that any requirements within the code that arise as a direct consequence of the wording and requirements of s121 DPA 2018 are not incremental impacts of the code.
- Impacts of existing explicit requirements of the UK GDPR and the DPA 2018: these are considered neutral in terms of the code as controllers are expected to already be compliant with these requirements.

In reality, it is not always possible to categorise impacts distinctly and they may be considered to straddle several of the above to differing extents.

2.5.3. Quantification

Quantified analysis of the impacts is particularly challenging for the data sharing code, given its wide ranging scope and the difficulties in attributing impacts to it.

For example, in terms of the potential for costs falling on controllers within scope, the code leaves room for interpretation, with costs varying even between organisations of the same type.

In addition, calculating the incremental costs of the code on controllers is complex, as the nature of these costs will vary considerably depending on the sophistication and maturity of the controller's existing data protection systems and processes, the nature of the services they provide, the data sharing associated with those services and the level of risk to data subjects. Consultation responses from controllers did not go into the detail necessary to inform quantification of costs, even anecdotally.

Equally, on the benefits side, the nature of many of the benefits, such as increased confidence for controllers or increased trust on the part of data subjects, is challenging to quantify.

Consequently the analysis focuses primarily on non-monetised impacts. However, where possible, high level qualitative analysis is provided to give an indication of scale in some instances.

2.6. Regulatory constraints

The Commissioner has drafted the code within the following regulatory constraints:

- her remit, powers and duties as set out in the UK GDPR and the DPA 2018; and
- the obligations placed upon her by s121 of the DPA 2018.

3. Costs and benefits of the code

The analysis in this section sets the potential costs of the code against the benefits to understand whether there are likely to be significant impacts on affected groups (both positive and negative) and judge the code's overall impact on society. The analysis draws on a mixture of quantitative and qualitative evidence but as noted above is limited by the evidence available.

The analysis of effects is split into two distinct categories:²⁴

- **Direct:** these are first round impacts that are generally immediate and unavoidable with relatively few steps in the logic chain between the introduction of the measure and the impact taking place.
- **Indirect:** these are second round impacts that occur after the shift to a new equilibrium and are often the result of changes in behaviour or reallocations of resources following the immediate impact of the introduction of the measure.

Direct impacts are given the same weight as indirect impacts in our analysis. The only distinction is that the indirect impacts are taken as a whole rather than with reference to specific elements of the code as the ways in which indirect impacts are brought about are not sufficiently distinct to justify individual analysis.

3.1. Direct costs and benefits of the code

We identify and analyse direct impacts of the code in the form of familiarisation with the code itself and the good practice examples and recommendations below. However it is important to note at the outset that direct incremental costs of the code are limited in that many of the requirements set out in the code are part of existing legislation that data controllers are already obliged to abide by.

3.1.1. Familiarisation

Controllers are expected to familiarise themselves with the code, although the extent of familiarisation will differ by controller.

Costs

There is a direct cost to controllers in terms of time and activity spent on familiarisation with the code. Although all controllers are expected to comply with the code in its entirety, it may not be necessary for all controllers to

²⁴ Further discussion on direct and indirect impacts can be found in: Regulatory Policy Committee, RPC case histories – direct and indirect impacts (2019)

familiarise themselves with the whole code. In order to model this, controllers have been split into groups according to an indicative level of exposure to data sharing. The levels then align with an expected level of familiarisation with the code and an associated cost. A summary of the estimated familiarisation costs is provided below with further analysis provided in Annex A.

| Data sharing exposure | Organisations (millions) | Estimated cost per organisation | Total cost (millions) |
|-----------------------|--------------------------|---------------------------------|-----------------------|
| High | 0.4 | £162 | £71 |
| Medium | 0.9 | £10 | £9 |
| Low | 4.9 | £6 | £30 |
| Total | 6.2 | £18 | £110 |

The total costs are estimated at £110 million; however this should be viewed as a conservative upper-end estimate because not all organisations will familiarise themselves with the code and there is evidence that a significant proportion of organisations do not engage with guidance at all.²⁵

Benefits

The direct benefit to controllers of familiarisation with the code is in helping them to comply with existing legislation. There are also other benefits such as increased confidence to engage in data sharing which are discussed under indirect costs and benefits (section 3.2).

Categorisation of impact

The impacts associated with familiarisation are a result of the production of the code itself which in turn is a direct result of the requirements of s121 DPA 2018. As the code provides good practice as well as practical guidance, it could be said that s121 of DPA 2018 enables some judgement about the scope and length of the code. However, as s121 is explicit in requiring the Commissioner to provide practical guidance on legislation as well as good practice guidance such that the Commissioner considers appropriate, this provides a broad scope for the code. Although there is some discretion implied in s121 of DPA 2018, it does not necessarily follow that discretion implies incrementality. A similar assessment was also made for the impacts of familiarisation of the age-appropriate design code.²⁶

While the assessment acknowledges that the issue of attribution here is complex, it is assumed that even where elements of the code could be deemed incremental, these are limited and likely to be balanced by the benefits to

²⁵ See BEIS, BIT Appraisal of guidance: assessments of regulator-issues guidance (2017) sections 2.3 and 2.4

²⁶ ICO, Age Appropriate Design: a code of practice for online services – Impact assessment (2020) see section 3.1

controllers in terms of regulatory certainty and greater ease in complying with legislation, particularly when taken in aggregate.

The impacts of familiarisation associated with the code are therefore considered to be a direct and inevitable consequence and therefore an impact of s121 of the DPA 2018.

3.1.2. Good practice examples and recommendations

The following analysis takes elements of the code which have been identified as good practice for controllers to follow and assesses the potential for each of these to bring about incremental costs to controllers.

Data Protection Impact Assessments (DPIAs)

The code encourages the use of data protection impact assessments. For example:

“In particular, you will find it helpful to use the data protection impact assessment (DPIA) process along with the code when considering sharing data. Some or all of the DPIA questions are likely to help you when you are assessing whether it is appropriate to share data, and whether it would be in compliance with the law.”²⁷

Of the DPIAs that were received by the ICO for review in the last year, around one third were specifically identified as relating to data sharing processing. Although this is not necessarily representative of DPIAs more generally, it demonstrates that data sharing is an important consideration for DPIAs.

Costs

The code does not add any situations where a DPIA is mandatory over and above the requirements of existing legislation. While the recommendation means it would be helpful to controllers when evidencing compliance, it is not a necessity. However, it is accepted that some controllers may see this guidance as an indication that they should consider undertaking DPIA processes.

We would expect larger organisations and those with higher exposure to data sharing to already employ the services of a Data Protection Officer (DPO) - and in some circumstances it is a legal requirement to do so - who is already familiar with DPIAs and we would expect that DPIAs are already standard practice for these organisations. As such, in these circumstances, any incremental costs associated with the code would be minimal.

For smaller organisations, there could be situations where the code has highlighted an area where DPIAs are required that had not been identified before. This will be due to a legal requirement. In these circumstances, businesses could face additional costs (as well as benefits) from developing a

²⁷ ICO, Data Sharing Code of Practice (2020) page 16

DPIA. Although not possible to quantify, it is expected that these circumstances would be relatively limited.

The costs of completing a DPIA are uncertain, the extent to which work is required is specific to the context of each organisation, the services they offer, their risk appetites and existing DPIA provision. As a result, we have been unable to estimate these costs.

Benefits

There are a number of benefits that could come about through the development of DPIAs. In addition to the increased confidence that is discussed under section 3.2, controllers may also benefit from reduced costs in implementing DPIA procedures given the greater clarity around how to do them. They are also useful to controllers in demonstrating accountability and compliance. This would also be useful to the ICO. For example, in the case of an investigation if the controller had a readily available and good quality DPIA addressing all the relevant points in the code, the case could be closed much more quickly.

Categorisation of impact

The assessment considers the impact of good practice recommendations on DPIAs to be uncertain but limited and largely resulting from existing legislation with the potential to create only minor incremental impacts over and above existing legislation. The direct impacts are assessed as neutral in terms of the code.

Data sharing agreements

As with DPIAs, data sharing agreements are encouraged within the code but are not mandatory. The code states:

“Drafting and adhering to a data sharing agreement should help you to comply with the law, but it does not provide immunity from breaching the law or from the consequences of doing so. However, the ICO will take into account the existence of any relevant data sharing agreement when assessing any complaint we receive about your data sharing.”²⁸

Costs

The good practice recommendation for data sharing agreements goes further than that for DPIAs in stating explicitly that data sharing agreements could be taken into account when assessing complaints. However, as with DPIAs, the code does not make any mandatory requirements over and above that of existing legislation and does not state that the lack of a data sharing agreement would negatively impact a controller or processor when the ICO assesses a complaint.

²⁸ ICO, Data Sharing Code of Practice (2020), page 25

It is likely that larger organisations and those with higher exposure to data sharing already have processes in place related to data sharing agreements or similar and as such the code would place no additional burden on controllers.

For smaller organisations, existing legislation means that they may already be engaging in data sharing agreement processes or something similar when using third party services, particularly when they are engaging in data sharing with larger organisations. For example, large cloud service providers and online advertising platforms may include data sharing agreements in their contractual terms when providing services. As such, there will only be limited circumstances in which organisations are not already engaged in data sharing agreement processes or similar.

As with DPIAs, it is not possible to quantify the costs of producing data sharing agreements as they will vary greatly in relation to the specific context of the organisation but also the nature and scale of the data sharing itself.

Benefits

For organisations already using data sharing agreements, the primary incremental impact is likely to be the greater regulatory certainty and clarity around the production of data sharing agreements.

Organisations that now feel it necessary to produce data sharing agreements are likely to benefit from the increased regulatory certainty. They may also find it easier to defend against legal challenges as data sharing agreements allow controllers to demonstrate accountability and compliance. As with DPIAs, it would also be useful to the ICO. For example, in the case of an investigation if the controller had a readily available and good quality data sharing agreement addressing all the relevant points in the code to demonstrate its accountability, ultimately enabling the ICO to close the case more quickly.

Categorisation of impact

The direct impacts of good practice recommendations on data sharing agreements within the code are uncertain but limited and largely resulting from existing legislation with the potential to create only minor incremental impacts over and above existing legislation. The direct impacts are assessed as neutral in terms of the code.

Data Sharing in an urgent situation or an emergency

The data sharing code seeks to ensure controllers are clear on how to share data in an emergency situation and how to plan ahead and put processes in place for when it is necessary.

"Where possible, if you are likely to be involved in responding to emergency or critical situations, you should consider the types of data you are likely to need to share in advance. As part of this it would be useful to consider any

pre-existing DPIA, and also refer to your business continuity and disaster recovery plans. As part of your planning, you should bear in mind that criminals might use a major incident or crisis as an opportunity to try to obtain personal data unlawfully. Therefore, the security measures outlined earlier in this code still remain relevant and necessary in times of urgent sharing.”²⁹

Costs

The code is clear that it provides points that are useful to consider but does not impose any burdens additional to existing legislation.

Many controllers will already have disaster recovery arrangements that are broad enough in scope to cover data sharing and others will not see urgent or emergency situations as relevant to their organisation so the scope for direct incremental impacts here is limited.

Given the wide ranging and unpredictable nature of the likely urgent situations and emergencies that controllers may need to plan for, it is not possible to quantify the scale or cost.

Benefits

In the limited situations where the code is seen to provide reasons for controllers to put in place additional processes, it is likely to be balanced by the significant benefits in doing so through mitigation of risks and negative impacts arising from urgent situations or emergencies.

The code notes that in a number of situations it would be more harmful not to share data than to share it. In these situations, sharing data and having the tools to plan ahead and do it confidently can help with:

- preventing serious physical harm to a person;
- preventing loss to human life;
- protection of public health;
- safeguarding vulnerable adults or children;
- responding to an emergency; or
- an immediate need to protect national security.

The benefits to mitigating some of the emergencies or urgent needs noted above could be substantial and although the benefits that can be attributed to the code are likely to be limited and indirect, the code could bring about significant benefits overall.

Categorisation of impact

²⁹ ICO, Data Sharing Code of Practice (2020), page 63

There are likely to be only limited circumstances where the code results in the implementation of additional processes and in these circumstances the costs are likely to be significantly outweighed by the potential benefits noted above. As it is not possible to estimate this with the required degree of certainty, it is conservatively assumed that the costs and benefits are balanced.

For the purposes of the assessment, the code is not considered to significantly impact on controllers in terms of data sharing in an urgent situation or an emergency over and above existing legislation. The direct impacts are assessed as neutral in terms of the code.

Sharing personal data in databases and lists

The code sets out good practice for controllers engaged in the acquisition or transfer of databases. The code states:

"You will find it beneficial to follow the good practice set out in this code. The due diligence carried out by both the sharing and recipient controllers is crucial to compliance."³⁰

Costs

The code makes a number of good practice recommendations such as implementing processes for enquiries and checks when receiving databases to ensure compliance and using written contracts between organisations receiving and supplying the databases. However, none of these recommendations are mandatory and as such they do not impose any requirements additional to existing legislation.

Where controllers do need to implement the good practice recommendations, it is likely that in the majority of cases they already have processes in place through contracts and other acquisition arrangements, as well as external professional advisers to mitigate the risk of receiving or providing poor quality products and services and to protect themselves from litigation.

The cost of arrangements related to sharing personal data in databases and lists is related to the perceived risks, the contexts of the organisations involved and the nature of the database or list itself and as such, it is not possible to quantify.

Benefits

As with the other good practice guidance, this is likely to bring about greater regulatory certainty to controllers and potentially reduce the costs of seeking external professional advice.

Categorisation of impact

This aspect of the code is not considered to present any incremental impacts over and above existing legislation. The limited costs to controllers are assumed

³⁰ ICO, Data Sharing Code of Practice (2020), page 57

to be balanced by the potential benefits. The direct impacts are assessed as neutral in terms of the code.

Dealing with complaints and requests

The code outlines how controllers should deal with complaints and requests. It states:

"Individual data subjects may have queries or complaints about the sharing of their personal data, particularly if they think the data is wrong or that the sharing is having an adverse effect on them.

The way you handle these queries and complaints makes a difference both to the individuals and to your organisation. It is not always a case of simply providing a response. The comments you receive might be an invaluable resource for you when you are reviewing your data sharing arrangement."³¹

Costs

It also sets out a number of good practice points including providing a single point of contact for complaints or enquirers. As with the other good practice recommendations, this does not impose any additional mandatory requirements that go over and above existing legislation.

Benefits

Although recommendations such as providing a single point of contact may require additional work to put in place, they can also reduce the burden on businesses by enabling co-ordination of requests and complaints.

Categorisation of impact

For the purposes of the assessment, the code is not considered to significantly impact on controllers in terms of dealing with complaints and requests. The direct impacts are assessed as neutral in terms of the code.

3.2. Indirect costs and benefits of the code

3.2.1. Costs

Although it is not possible to rule out indirect costs from the code, it is difficult to identify any that are likely to bring about significant indirect incremental impacts.

Potential examples include unintended market distortions where incumbent businesses are given greater market power; or displacement effects where activities in one sector are displaced by increased activities in another. However, these are not covered in detail as there is not enough evidence, within the

³¹ ICO, Data Sharing Code of Practice (2020), page 46

consultation responses received and more generally, to suggest that they would in fact occur.

3.2.2. Benefits

The benefits of the code are inherent in the aim and rationale for it in attempting to overcome barriers to data sharing and providing easier routes to achieving compliance with existing legislation. While the code itself is not directly responsible for the benefits of data sharing and increased data use, it is clear that indirectly it could help to promote, facilitate and catalyse the benefits through behaviour change, improving controllers' confidence to share data, and in turn meeting the first mission of the draft National Data Strategy in unlocking the value of data across the economy.

Indicative estimates of the benefits of data and increased data sharing put the overall value across the economy at somewhere between £22.2 and £55.5 billion (see section 2.1.2). This is a wide range and shouldn't be viewed as a precise quantified estimate but does provide some indication of the significant scale of benefits that the code could help to unlock, even if it only makes a minor contribution to the overall value.

More specific examples of benefits of data sharing are discussed in section 2.1.2. In summary this covers:

- product or service improvement;
- access to new markets;
- more efficient and effective public services and policy making; and
- innovation

The benefits described are not intended to be exhaustive, given the wide-ranging nature of data and data sharing, but provide a good justification for the encouragement of increased data sharing.

The key contribution that the code makes to these benefits is in enabling increased trust and confidence in data sharing, both by controllers in sharing the data and also by data subjects. As noted in the Treasury's paper on the economic value of data, some businesses perceive data as a liability, particularly where personal data is concerned.³² There can be a perception that sharing data will lead to a 'loss of control' over the data that is shared, which could in turn lead to a personal data breach. This misconception severely curtails access to and usage of personal data and can be a significant opportunity cost. The code therefore addresses how to ensure data is safely and securely shared in order that any liability or risk is minimised and accounted for. Further, guidance on data sharing agreements and frameworks is provided in the code so that controllers are clear on how they can use any personal data shared with them. A

³² HM Treasury, The Economic Value of Data: Discussion paper (2018) page 5

recent ODI paper on the economic impact of trust in data ecosystems³³ suggests that trust-building interventions like the code can significantly boost the economic benefits of data sharing.

A lack of experience, expertise and mechanisms through which to strike agreements with other controllers are some of the key barriers to data sharing.³⁴ In addition, some perceived barriers to data sharing arise from misconceptions, which the code aims to dispel. Whilst data protection legislation is often viewed as a barrier to effective and efficient data sharing, it is actually an enabler. The code helps provide guidance on how data can be shared in a safe, ethical and compliant manner.

As with the benefits described above, the ways the code helps to remove barriers – both perceived and real – to data sharing are not intended to be exhaustive, but provide helpful examples of where the code helps to promote data sharing.

In terms of meeting the key elements of the rationale and combatting the market failures discussed in section 2.1.3, the code is expected to make significant contributions to mitigating these market failures. By promoting good practice and plugging gaps in information, the code will ensure that benefits and positive externalities are maximised while reducing the potential for negative externalities. It will also help to level the playing field by giving confidence to smaller organisations³⁵, reducing the barriers to entry into digital markets and encouraging greater competition and innovation.

Finally, as demonstrated in section 2.1.1, the code aligns well with government policy objectives relating to data and digital markets, particularly those within the draft National Data Strategy and is expected to contribute to meeting these objectives which will in turn help to bring about the benefits associated with the policy.

3.2.3. Categorisation of impact

Although there is limited potential for the code to bring about direct incremental impacts, the wide scope of the code means that there are a number of ways in which it can drive and unlock indirect incremental impacts. The value of data and hence the potential value of data sharing is so large that even if the indirect impacts of the code unlock only a small proportion of this, the effect could nevertheless be significant. Even when viewed conservatively, it is clear that the indirect benefits noted would significantly outweigh any other incremental costs.

³³ ODI, Economic Impact of Trust, February 2021

³⁴ Bennett Institute, The Value of Data Policy Implications Report (2020) page 7

³⁵ <https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/whats-new/blogs/data-sharing-when-is-it-unlawful/>

As such the impacts described above are considered beneficial and incremental to the code; however, it is not possible to quantify as there is a very high degree of uncertainty as to the extent that impacts are attributable to the code.

3.3. Conclusions

The analysis and discussion within this impact assessment demonstrates a clear rationale and policy alignment for the code both in terms of the statutory requirement but also in terms of contributing to wider government objectives on data and data sharing, as well as serving to address market failures.

Although quantification of all costs and benefits has not been possible and there are significant uncertainties as to the scale and scope of impacts, the analysis demonstrates that there are limited direct incremental impacts from the code. Where the code has the potential to generate incremental impacts, this is through its indirect impact on affected groups. The cost benefit analysis demonstrates the potential for the code to drive significant benefits through increased confidence in data sharing which could in turn contribute towards unlocking substantial benefits to the economy and society.

In conclusion, the assessment finds that the code is likely to deliver significant incremental impacts that are beneficial.

4. Annex A: estimating familiarisation costs

The following annex sets out the approach taken to estimating familiarisation costs for the code.

As noted in section 3.1.1, to estimate the familiarisation costs we have attempted to identify the organisations that the code is relevant to and then separated them based on their likely exposure to data sharing. This is then used to estimate the likely cost to each organisation of familiarising themselves with the code.

Organisations

The organisations covered in the analysis of familiarisation costs are businesses, public sector organisations and charities.

The latest release of the ONS Business Population Estimates states that there are almost 6 million businesses across the UK. The assessment uses the make-up of these by size and sector to inform exposure to data sharing.

All businesses with no employees are assumed to have a low exposure to data sharing. Although this may not be true of all sole proprietors, it is seen as a reasonable mid-point with some having very low level involvement with data sharing and others higher. These businesses make up the vast majority of organisations representing over 75% of all businesses. For businesses with employees, exposure is estimated based on the sector, informed by the likely activities of these businesses and their average size. The assignment is made based on high level assumptions but provides a useful indication and a proportionate approach to assigning data sharing exposure likelihood. These are justified as follows:

| Sector | Data sharing exposure | Brief justification |
|-----------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Agriculture, Forestry and Fishing | Low | Low average business size and not much customer data |
| Mining, Quarrying, and Utilities | Medium | Mixed with utility providers expected to have lots of customer data but mining and quarrying businesses will not |
| Manufacturing | Medium | Low potential for large amounts of customer data but larger sized businesses with lots of employee and contractor data |
| Construction | Medium | Low potential for large amounts of customer data but larger sized |

| | | |
|-----------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | businesses with lots of employee and contractor data |
| Wholesale and Retail Trade; (including auto-repair) | Medium | Mixed in terms of potential for lots of customer data in larger retail organisations but with medium risk and less so in wholesale than retail |
| Transportation and Storage | Low | Relatively low risk and mid to low levels of data |
| Accommodation and Food Service Activities | Medium | Mixed in terms of potential for high levels of customer data for some accommodation businesses but with medium risk and less so for smaller food and drink establishments |
| Information and Communication | High | High volumes of data and data sharing activity |
| Financial and Insurance Activities | High | High volumes of high-risk data and data sharing activity |
| Real Estate Activities | High | High volumes of high-risk data and data sharing activity |
| Professional, Scientific and Technical Activities | High | Sector includes lawyers, researchers and others with high-risk data and potential for sharing |
| Administrative and Support Service Activities | Medium | Mixed depending on which other sectors the services are linked to |
| Education | High | Potential for high levels of high-risk data including children's data |
| Human Health and Social Work Activities | High | Potential for high levels of high-risk data including medical and children's data |
| Arts, Entertainment and Recreation | Medium | Mixed as sector includes gambling, libraries and others that may have some personal data but also low risk activity like artists and musicians |
| Other Service Activities | Low | includes membership organisations but also a lot of low-level and low risk service activity such as repair shops, dry cleaners, hairdressers and others |

For charities, the register of charities from each of the charity regulators across the UK provides information on the number of charities by income band. In the absence of other information, we have used the simplifying assumption that

charities with larger incomes are likely to have higher exposure to data sharing. The breakdown is as follows:

| Annual income band | Data sharing exposure |
|---------------------------|------------------------------|
| £0 to £0.5m | Low |
| £0.5m to £10m | Medium |
| £10m and over | High |

For public sector organisations, given they would be more likely to be involved in the processing of personal data and, in particular, high risk personal data, due to the activities they carry out, we assumed a minimum of medium exposure with those with over 50 employees assumed to have high data sharing exposure:

| Employees | Data sharing exposure |
|------------------|------------------------------|
| 0 to 49 | Medium |
| 50 and over | High |

Familiarisation costs

As part of developing the code the Commissioner sought to ensure maximum clarity and readability while still providing the necessary information. On top of this a number of additional guidance documents and web pages were developed to make the code more accessible to its wide and varied audience, in particular, guidance focused on sole proprietors and small organisations. Drawing on impact assessment guidance³⁶, an estimate of the average time taken to read each document is provided below:

| Element of guidance | Word count | Fleisch reading ease score | Assumed words per minute | Estimated reading time (Hours: Minutes) |
|----------------------------------|-------------------|-----------------------------------|---------------------------------|------------------------------------------------|
| Data sharing: a code of practice | 27,371 | 39.5 | 75 | 6:05 |
| Data sharing code: the basics | 836 | 59.4 | 100 | 0:08 |
| SME hub data sharing pages | 1,048 | 49.4 | 75 | 0:14 |

For the purposes of the assessment, we have made some broad assumptions about the documents that a typical organisation in each data sharing exposure

³⁶ BEIS, BIT Appraisal of Guidance: Assessments for Regulator-Issued Guidance (2017)

group would be expected to read. It should be noted that this does not suggest that organisations that fall into these groups should only read the guidance noted here; some will need to read more and others less; it is just intended to provide an indicative average for the assessment of familiarisation costs.

| Data sharing exposure group | Typical documents | Total estimated reading time (Hours: Minutes) |
|------------------------------------|----------------------------------|------------------------------------------------------|
| High | Data Sharing: a code of practice | 6:05 |
| Medium | Data Sharing Code: the basics | 0:22 |
| | SME Hub Data Sharing Pages | |
| Low | SME Hub Data Sharing Pages | 0:14 |

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings (ASHE).³⁷ Assuming that the relevant 'occupational group' is 'Managers, Directors and Senior Officials', the 2019 median hourly earnings (excluding overtime) for this group is £21.90. This hourly cost is uprated for non-wage costs using the latest figures from Eurostat and in line with Regulatory Policy Committee guidance,³⁸ resulting in an uplift of 22% and an hourly cost of £26.71. Using this hourly cost and making the simplifying assumption of one individual being responsible for familiarisation for each organisation³⁹, the table below shows the estimated total familiarisation costs:

| Data sharing exposure | Organisations (millions) | Estimated cost per organisation | Total cost (millions) |
|------------------------------|---------------------------------|----------------------------------------|------------------------------|
| High | 0.4 | £162 | £71 |
| Medium | 0.9 | £10 | £9 |
| Low | 4.9 | £6 | £30 |
| Total | 6.2 | £18 | £110 |

³⁷ See https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly_labour_costs and <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2020>

³⁸ See guidance in https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs_August_2019.pdf

³⁹ In reality there may be one individual responsible for understanding the code for multiple organisations or multiple individuals in one organisation but in the absence of data to make a precise estimate, the simplifying assumptions is deemed appropriate

The breakdown across organisation type is as follows and demonstrate that the vast majority of familiarisation costs is expected to come from businesses:

| Data sharing exposure | Organisations (millions) | Estimated cost per organisation | Total cost (millions) |
|------------------------------|---------------------------------|----------------------------------------|------------------------------|
| Businesses | 5.98 | £18 | £107.8 |
| Charities | 0.20 | £8 | £1.6 |
| Public Sector Bodies | 0.01 | £76 | £1.0 |
| Total | 6.19 | £18 | £110.3 |