Data Protection and Digital Information (no. 2) bill

Open Data Institute response

May 2023

About the ODI

The Open Data Institute (ODI) is an independent, non-partisan, not-for-profit organisation founded by Sir Nigel Shadbolt and Sir Tim Berners-Lee in 2012. We have a mixed funding model and have received funding from multiple commercial organisations, philanthropic organisations, governments and intergovernmental organisations to carry out our work since 2012.

The ODI wants data to work for everyone: for people, organisations and communities to use data to make better decisions and be protected from any harmful impacts. We work with companies and governments to build an open, trustworthy data ecosystem. Our work includes:

- **consultancy:** working with organisations in the public, private and third sectors, building capacity, supporting innovation and providing advice
- **research and development:** identifying good practices, building the evidence base and creating tools, products and guidance to support change
- **policy and advocacy:** supporting policymakers to create an environment that supports an open, trustworthy data ecosystem

Our 5 year strategy sets out what we think are the elements of an open and trustworthy data ecosystem for a world where data works for everyone. Our approach allows us to adjust our implementation and engagement as the world around us, and the organisations we work with, change. Our activities will be set out on an annual basis, mapped to the six principles that guide everything we do:

1. We believe that a **strong data infrastructure** is the foundation for building an open, trustworthy data ecosystem on a global scale and that this can help address our most pressing challenges.
2. Strong data infrastructure includes data across the spectrum, from open to shared to closed. But the best possible foundation is **open data, supported and sustained as data infrastructure**. Only with this foundation will people, businesses and governments be able to realise the potential of data infrastructure across society and the economy.
3. For data to work for everyone, it needs to work across borders – geographic, organisational, economic, cultural and political. For this to happen ethically and sustainably, there needs to be trust – **trust in data and trust in those who share it**.
4. There is greater need than ever for trusted, **independent organisations to help people across all sectors, economies and societies to benefit** from better data infrastructure.

5. For data to work for everyone, those collecting and using it need to be highly alert to inequalities, biases and power asymmetries. All organisations working in data must take proactive steps to ensure that they **contribute fully and consciously to creating a diverse, equitable and inclusive data ecosystem**.
6. The world needs a new cohort of **data leaders – individuals who have data knowledge and skills** and are equipped to understand the value, limitations and opportunities offered by data, data practices and data sharing.

Consultation response

This is the ODI's response to the Data Protection and Digital Information (No 2) Bill committee's consultation on the Bill.

We at the ODI have spent more than a decade working to build an open, trustworthy data ecosystem. We want a world where data works for everyone, and where the UK builds on its well-deserved reputation as a centre of global excellence for data assurance, data practices, and data governance.

Any legislative change around data protection should pay due care to enabling, and ensuring, safe and trusted data-flows between the UK and other countries. This trusted flow of data would help to secure the economic benefits of data flows - such as increased productivity, increased trade, and increased levels of research - with trust and safety.

We believe that the Data Protection and Digital Information (No. 2) Bill goes some way to achieving a more open and trustworthy ecosystem, but that it should take into account a number of considerations that go beyond legislation, and require a commitment to building public trust, enhancing the data ecosystem, culture and practices around data use, and considering the potential future uses of data. We have set out our thoughts on these three areas below:

- **Public trust**. Public trust in the wider data ecosystem is vital if we are to unlock the economic value of data, as ODI research has shown.[1] The sensitivity or value of the same type of data might vary in different contexts, and depending on how the data is used, and who it is used by. While trust varies within data ecosystems, depending on how data is used, and by whom, weak or diminished trust in part, or all, of the ecosystem can lead to lower levels of data sharing - which impacts the ability of actors in the data ecosystem to utilise data for the public good. Any new legislation and regulation around data protection should not only ensure it maintains levels of public trust, but that it builds trust. Research from Frontier Economics for the ODI has found that the economic value of data and data flows is underpinned not only by trust in the data itself, but by trust in the data system as a whole.[2] Therefore, building and maintaining that trust is vital in order to achieve the true economic potential of data and data flows.

- **Culture and practices**. The ODI believes that whilst legal rights and obligations are a hugely important part of a country's ecosystem on data protection, they are not the only part. The culture and practices around data such as the presence of trustworthy and sustainable data infrastructure[3] and institutions; a focus on increasing data literacy

[1] How trust is a key to the value of Data - The ODI
[2] The economic impact of trust in data ecosystems – Frontier Economics for the ODI [report] – The ODI
[3] Data infrastructure – The ODI

within organisations and citizens more widely[4]; the presence of a mature, capable, and high-quality data assurance sector[5]; and high levels of citizen engagement with the data system[6] are all hugely important in ensuring the UK remains a world leader in data, data protection, and data rights. The ODI urges the Government, and relevant regulators, to remain focused and aware on shaping culture and practices effectively.

- **Potential future uses of data**. As we have seen over the past few decades, data use and applications develop rapidly, and sometimes, in unexpected ways. It is hard to predict how use cases for data might change in the future or how it might be applied: this is a core characteristic of data, and partly the reason why data has a high option value.[7] It is vitally important that the UK's data protection laws and regulations are able to allow for future uses of data and innovation around the application of data, as well as the potential harms associated with them. Many of the risks within the data ecosystem that are today considered "actual" or "material" were merely "academic or immaterial" only a few years ago.

The areas outlined above are hugely important to a well functioning data ecosystem, and to the wellbeing of citizens - we believe they are also the areas that the UK should be investing in for itself.

Our consultation response now turns to addressing some of our concerns with the Data Protection and Digital Information (No. 2) bill, and where we think there are areas for improvement.

Adequacy with the EU

Leaving the EU means the Government can diverge from existing EU law, and remove some of the claimed complexities and costs associated with it.

However, there is a risk that too great a divergence would put the UK's 'data adequacy' at risk. The Government's own impact assessment show that losing adequacy could result in "£190m and £460m in one-off Standard Contractual Clauses (SCC) costs", lead to "an annual cost of between £210m and £420m in lost export revenue" and present significant difficulty to businesses in adhering to two different data protection systems. We would also refer readers to the UCL European Institute and New Economics Foundation report on the cost of data

[4] Data literacy: what is it and how do we address it at the ODI? – The ODI
[5] Assurance, trust, confidence – what does it all mean for data? – The ODI
[6] Our manifesto – The ODI
[7] The Value of Data – The ODI

inadequacy which posits a much higher cost to businesses.[8] We believe that any change in data protection systems will be particularly challenging for SMEs with small staff numbers who will have to adapt to a new set of data protection requirements, that will involve training and upskilling staff to remain compliant. In addition, for businesses based in the UK that want to trade with Europe and its citizens, they will be required to abide by both systems. Given GDPR is the higher standard, it is possible that businesses will continue to abide by GDPR, rather than balancing two separate regimes.

A number of UK based data institutions collect, maintain and share data for research purposes. Currently, researchers are able to use existing provisions effectively, and they are clear in their concerns that changes to legislation that risk EU data adequacy pose a risk to the research that can be carried out.

The ODI believes that the UK's competitive advantage lies in the free flow of trusted data and our research into the Value of Data sets out further evidence for the economic gains provided by access to data across and between economies.[9]

For the sake of a well functioning data ecosystem, and for the UK to maintain its position as a global leader in data, it is vital that we enable a data protection framework that provides reassurance to other countries about how their citizens' data will be treated in the UK, while also pressing other countries to be clear on their own data protection frameworks for data belonging to UK citizens and businesses. Given the level of adoption of GDPR worldwide, it is highly likely that ongoing, and continuing alignment with European data protection regulations will remain important.

We believe that achieving data adequacy with the EU must be considered a priority.

Automated Decision Making (ADM) and algorithms

Fairness has a specific and evolving meaning in the context of the use of machine learning and AI, and there is growing interest in the question of how unfair outcomes from the use of AI systems can be prevented, particularly when it impacts those without the means to overturn or challenge these unfair outcomes, or when it embeds and amplifies existing biases.

As laid out in the ODI's work on Inclusive Data,[10] there are unfairly distributed harms produced by AI systems that can have a far greater impact on those from less privileged socio-economic backgrounds, or in circumstances where intersectionality of race, gender, socio-economic background and disability exist.

---

[8] UCL European Institute & New Economics Foundation (2020), 'The Cost of Data Inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision'
[9] The Value of Data – The ODI
[10] Inclusive Data Perspectives from a Roundtable Discussion - The ODI

A significant challenge with determining fairness in ADMs and algorithms, is that discriminatory harms are often difficult for individuals to detect. The inner workings of AI systems and algorithms are mostly opaque, preventing users or civil society from having the opportunity to scrutinise them. Even when they are made available for review, people lack the technical knowledge to assess the fairness or unfairness of the system, and in many cases, systemic "unfairness" is only noticeable on an aggregate, or a population level. The Public Law Project's extensive work demonstrates how algorithms are being used by the government on a range of sensitive policy issues, from policing to benefits, and their work enables these algorithms to be investigated and assessed. It is likely that the algorithms identified by PLP are only a small part of the algorithmic decision making in Government.

Algorithms and employee monitoring are being used to monitor employees and to make judgements and decisions about their recruitment and employment – often with little to no regulation or human oversight. This has led to the Trades Union Congress (TUC) drawing attention to the challenge of "management by algorithm" and "robo-firings". In addition, work by the Public Law Project has shown how algorithms are being used by the Government on a range of sensitive policy and public service areas, including for example, in policing, determining an individual's benefits status, and about immigration matters.

As the ODI has pointed out previously, algorithms depend on the quality of the data entered – if the data is biased, the ADM will be biased too. We have seen several examples where ADMs have led to biased outcomes, sometimes with long-lasting ramifications. We know that machine learning and ADMs not only incorporate biases but amplify and enhance them.

Under current law, ADMs must have an element of human oversight where it relates to a significant decision. However, clause 11 of the Bill would relax the requirements for human oversight and put a burden on the negatively impacted consumer or employee to bring a complaint. It would also mean that employees and individuals could be held to a standard that they cannot negotiate or influence – a concerning asymmetry of power that could be rebalanced through legislation, and by increasing data literacy for people to understand how to provide effective oversight..

The Government's own work recognises the importance of transparency around the use of algorithms. The Central Digital and Data Office (CDDO) and the Centre for Data Ethics and Innovation (CDEI) are helping public sector organisations to provide clear information about the algorithms they utilise. The Bill seems somewhat incongruous. It could go further in mandating transparency and responsible algorithm use by employers, public sector bodies, and tech platforms in particular. While mandatory reporting was in the Government's consultation, and the majority of respondents agreed with the proposal, it has disappointingly been left out of the Bill.

Proactive monitoring and regulatory action from appropriate regulatory bodies should also consider how AI systems can help address or overcome existing socioeconomic inequalities. While it is important to focus on preventing the possible harmful impacts of AI systems, algorithms, and ADMs, these systems have significant potential that can be leveraged for social good, as we outlined in work[11] on the Commission on Race and Ethnic Disparities (also known as "the Sewell Report).

The use of AI, algorithms, and ADMs will vary from sector to sector, and therefore the risks associated with their use will also vary - both in magnitude, and impact. The use cases for AI in recruitment and management, health research, and in transport all present different risks and therefore require different levels of protections for those impacted by their use.

We strongly believe that people should have the right to object to ADM processes that affect their lives significantly, especially where these processes have no element of human oversight, and no ability for objection or appeal.

Transparency and an organisation's willingness to explain the AI algorithms it uses builds trust. It also enables those shaping and developing the algorithm or ADM to monitor how decisions are made, and to address failings, biases or problems in the system. The ability to oversee, understand, and challenge ADMs is critical for society – to ensure they are fair and non-discriminatory as well as to ensure people can maintain their autonomy.

The Information Commissioner's Office (ICO) and Secretary of State

In its current guise, the DPDI Bill potentially reduces the independence of the ICO and increases the powers available to the Secretary of State on data protection by empowering them to issue instructions and set out strategic priorities for the ICO.

While the current Information Commissioner has been supportive of the proposed changes, the ODI believes that this risks the office of the ICO becoming politicised and could challenge its abilities to maintain its independence as the political landscape changes.

At the ODI, we want regulation to enable the data ecosystem to function – effectively, and safely. Legislation is vital to creating an open, transparent, ecosystem that allows the Government and regulators to protect individuals whilst not stifling innovation and economic growth. We also believe that the independence of the ICO is vital to ensure it remains able to hold the Government to account for its own use of data – this is likely to become more challenging if the ICO is answerable to the Government itself. If the ICO answers to the Secretary of State, and therefore, the Government, it compromises the ICO's ability to do its

[11] The weird and the wonderful: reflections on the Commission for Race and Ethnic Disparities report - The ODI

job. Whilst in many cases, the ICO's priorities may well align with the Government's priorities, any perception of a conflict of interest is likely to reduce trust in both the ICO and the data ecosystem more broadly.

We believe it is vital that the ICO's independence is safeguarded so that it can command public trust in any future decisions that it makes.

Therefore we believe that the best route to enabling quicker adaptation to technological changes whilst maintaining and protecting the independence of the ICO, would be to have the ICO beaccountable to Parliament rather than to the Government.

Reduced data processing safeguards

The Bill reduces certain requirements, such as the need for organisations to have a Data Protection Officer (DPO). Data Protection Impact Assessments (DPIAs) will no longer be needed, and records for data processing will no longer need to be kept unless the data is deemed "high risk" such as medical records.

The Government has highlighted that current rules place a burden on medical researchers who need to reobtain consent to utilise personal data outside the narrow original request. The Government has spoken of its ambition to make it easier for scientists to conduct research for medical purposes and to empower the UK to be a world leader as a "scientific research powerhouse".

While we support the ambitions of the Bill in creating an environment where medical research can progress rapidly, we would urge the Government to consider the importance of building and fostering public trust in data being shared and used, through increased data literacy and education programmes, if it wants to truly unlock the potential of medical data for research and treatment.

The Government should also address the potential risks to individuals about whom data is being processed and the impact this may have on the public's levels of trust in the institutions that are accessing, using and sharing this data. Our work during the Bill's consultation period demonstrated that transparency was "necessary but not sufficient" and that any work towards increasing transparency should be accompanied by accountability through clearly defined standards, and mechanisms for redress – both areas where the Bill could be strengthened.

We see data protection impact assessments as akin to the approach we use for data ethics - organisations need to be able to assess the impact of their data use or project, to help understand how choices made might be considered 'right' or 'wrong'. The DPIA is a tool that

helps to consistently evaluate the impact of data use and application, the same way that our Data Ethics Canvas helps users to navigate the issues and come to a consistent conclusion.

DPIAs serve a valuable purpose and provide a useful framework for considering the impacts of using personal data. They are a valuable tool not only for helping organisations to assess risks but also for enabling them to identify potential opportunities with data. DPIAs ensure that data is considered at the start of a project, provides an opportunity for potential issues to be identified proactively and that data management practices are designed with particular use cases in mind. DPIAs make it more likely that organisations using data will do so in a considered and strategic way, and that data sharing will increase.

While the Government is focused on the potential time and cost saving for businesses, the ODI believes that the privacy of personal data is of the utmost importance and that maintaining DPIAs as a requirement adds significant value to the data ecosystem and economy. Work by the Institute for Government found that those working on pandemic data sharing valued DPIAs as they provided transparency and secured organisational buy-in. Instead of removing the need for DPIAs entirely, focusing on facilitating better data sharing and processing along with education, cultural change, guidance, and incentivisation would all be more helpful than legislative change.

In addition to appropriate impact assessments, we strongly believe that more prominence should be given to data ethics. Data ethics along with the responsible use of data cannot be seen as an add-on: rather it should be embedded into every aspect of data policy, and at every stage of data use. DPIAs should be broadened to cover responsible and trustworthy data governance based on the principles of ethics, engagement, and equity.

At the ODI, we've developed a number of tools to help all actors in the data ecosystem to identify and manage ethical issues with data collection, sharing and use; and to identify the data skills required by different people in organisations, including management skills to ensure ethical handling of data, and methods for assuring data..

Good data governance produces economic benefits - for individual organisations and for the wider economy. These economic benefits come through increasing responsible data use and innovation which in turn increases the benefit to society. However, to realise these potential benefits we need to ensure good data governance - DPOs play an important role in holding responsibility for data protection governance, and can provide organisational leadership and senior buy-in.

We know that data leadership is far wider than requiring a data protection officer. We believe the Government should encourage organisations to go beyond their legal requirements and to establish data leadership roles at a senior level, across roles. Data responsibilities and opportunities cover many angles from data governance, data protection and data assurance through to data science and data exploitation through machine learning and AI. Establishing

data responsibilities for leadership roles would help to establish data as a critical function for any twenty-first century organisation, providing a new direction for the role of data within the UK economy.

This would create a chance to frame data governance as a positive opportunity for organisations, with those that do well managing their data gaining a competitive advantage while at the same time improving the overall economic performance of the data ecosystem. Having data leadership in place would improve transparency and auditability on how data is being collected, used and shared; allowing also for a better understanding and accounting of how value from data returns to people and organisations. These two are conditions outlined in Our Value of Data report as necessary to realise the full potential value of data for society.[12]

Moreover, good auditing of data and data practices is essential to better understand company risk profiles, and can impact on an organisation's reputational, legal and financial exposure,[13] and thus also its overall performance in the long run.

The evidence shows that good data governance produces economic benefits both for individual organisations and for the wider economy through increasing responsible data use and innovation. However, to realise the potential economic benefits of good data governance organisations require organisational leadership and senior buy-in, which starts, but should not end, with a DPO.

The ODI's extensive experience working with organisations of all sizes, and from different sectors has shown us that insufficient data literacy among leadership teams tends to prevent organisations from being able to appropriately consider the potential long term benefits of good data governance practices. In addition, low levels of data literacy makes it harder for the organisations to adopt good data practices. We would urge the Government to consider how it could incentivise organisations to include data governance roles in their leadership structures. We believe that the DPO should be retained and that the development of data skills and data literacy should be encouraged and incentivised.

We acknowledge that SMEs in particular may find it more difficult to develop good data protection and data governance practices, and therefore we believe that the Government should explore options to strengthen data capabilities and data literacy across this sector to reduce the burden of data protection compliance.

We believe that removing the requirement for organisations to appoint a DPO could affect the capacity of organisations, and those operating with data, to respond to the public's expectations.

---

[12] Bennett Institute for Public Policy & The ODI (2020), 'The Value of Data'

[13] The ODI (2021), 'The ODI responds to the UK government's restoring trust in audit and corporate governance consultation'

Having a DPO provides assurance and trust to the public that there is someone responsible and accountable in all public organisations irrespective of the organisation's size.

Subject Access Requests

We have previously written about Subject Access Requests (SARs) and the importance of allowing people to submit requests to those who hold data about them to see this data. The Bill offers companies more flexibility in refusing to comply with these requests on the grounds of being "excessive or vexatious."

While we recognise the cost and burden on SMEs of responding to SARs, an analysis of the Government's impact assessment by Connected by Data suggests that the saving to SMEs from SAR reform will be around £59 per year – certainly not enough to justify this change, given the limitation on people's rights that it contains.

SARs should not be costly if organisations have appropriate data governance, and their data management frameworks and systems in order. The capabilities that underpin being able to respond to SARs are necessary for good data management and for supporting further interoperability and data sharing between businesses (i.e. data portability). These are vital capabilities which should be encouraged, as they promote responsible data use and innovation.

For organisations to be able to respond to SARs with ease, and low costs, they need to maintain good data records including minimising data collection and having good processes for data retention and deletion - and we do not believe that good record keeping is a burden. The Government's own work demonstrates the need, and value, of good record keeping. In fact, maintaining good data records can lead to efficiencies, innovation, and opportunities for companies that can serve the public interest, as shown when organisations like the Environment Agency release open data which relies on understanding and mitigating any risks in the data before opening it.[14] This is also emphasised by the Government's own approach to Managing Public Sector Knowledge Assets, which urges Departments to have an understanding of their own knowledge assets, of which data is one type. Without good records of their data assets, they would have never known what data they had and therefore would not realise the benefits of releasing it as open. Other benefits to effective record keeping include: being able to identify gaps in existing datasets such as potential research opportunities, gaps around representation, or potential for increased engagement of minorities and vulnerable communities.

[14] Open Data Institute (2015) Environment Agency: Going open. London, UK. https://theodi.org/article/environment-agency-going-open-2/

Work we did for our Open Cities project demonstrated that local authorities could reduce the administrative cost of Freedom of Information (FoI) requests by choosing to classify them as a measure of customer service failure (a failure to anticipate needs). By doing so, they could utilise FoIs as indicators of how to improve customer service, and therefore be more proactive about publishing data relevant to users. By doing so, local authorities could reduce the number of FoI requests while also improving engagement with local residents and businesses. Increasing the data that the local authorities published had the additional benefits of increased transparency, trust and engagement. Our work shows that SARs do not need to be seen as an administrative burden, but as a trigger to think strategically about transparency and data sharing, as well as to encourage companies to develop better data management practices and processes.

By following openness principles[15] organisations may reduce the number of SARs they receive. These principles are also likely to reduce the costs to organisations of addressing SARs by implementing good data management practices and record keeping. At the ODI we believe that organisations handling personal data should:

- Be open with people about what personal data they are collecting.
- Be open with people about how they use personal data.
- Be open with people about the way personal data is shared.
- Be open with people about the way personal data is secured.
- Explain to people how we make decisions using data about them.
- Be open about their accountability mechanisms for misuse of personal data.
- Help people understand and influence how their data is collected and used.
- If collecting or using personal data, make their analyses and outputs as open as possible.
- Apply good data management practices.

We strongly believe that everyone can, and must, benefit fairly from data. Access to data empowers people as consumers, creators and citizens. By making it more difficult for individuals to access data about themselves risks promoting inequity in data access and penalising those with limited resources.

Case Study of where SARs have been applied effectively:

Until 2019, it was not publicly known that learners' religion and equality monitoring data from applications to Higher Education were being collected and stored on named records and retained by the Department for Education. This was made public after a SAR by Defend Digital Me after which the first publication of the DPIA of the National Pupil Database was made. In addition, it only became public knowledge that religion was being added into named student records after lobbying for a DPIA to be completed, and published.

[15] The ODI (2016), 'Openness principles for organisations handling personal data'

This is an important case study to demonstrate both the importance of DPIAs before actions are taken, and of SARs in order to enable transparency of the system and accountability.

Our research into the public's attitudes about data about them revealed that people's levels of understanding and feelings about data differ vastly. Some people are highly cautious about how data about them is used while others are willing to share access to data about them liberally. Our work is just one contribution to the wider debate around data rights and data governance, but our work showed that in spite of people's differing views on data, what people do have in common is that they care about their data rights and the responsibilities around them.[16] Most people told us that they make choices and decisions around data about them based on how they feel at a moment in time and their current life circumstances, but that they would like to have the right to change their minds when they feel differently.

In addition, when organisations are open about how personal data is used, and how privacy is protected, trust is built in organisations collecting and using personal data. Greater trust likely leads to less friction when developing new ideas and services, and potentially greater use of existing ones.

Therefore we advocate for maintaining a SAR regime to empower people and enable equity in access to data, rather than making it more difficult for citizens to access information about what data is held on them, and how their data is being used.

Strengthening the Bill - Data Intermediaries

We encourage the Government to make the most of the opportunity to further improve the data ecosystem by supporting the role of data intermediaries.

Data intermediary is a broad term, covering a range of different activities and data governance models for organisations: this is broadly accepted as any organisation which facilitates greater access to or sharing of data by acting as an intermediary between data holders and data reusers.[17] The Government has an important role to play in shaping the activity of data intermediaries.

We have previously written about the valuable role that data intermediaries play in facilitating greater access to and sharing of data and of how the data ecosystem could be further improved by enabling individuals and communities to exercise more control over the collection, maintenance and sharing of data about them or that they have a vested interest in. Whilst the Government has spoken of its intention to use the bill to "put in place the foundation for data

[16] The ODI (2020), 'Data protection and trust at Co-op'
[17] CDEI (2021), Unlocking the value of data: Exploring the role of data intermediaries

intermediaries", we believe the Government could use the bill as an opportunity to set standards for data intermediaries. In addition, the Government could use the bill as an opportunity to allow continuous access to data through SARs – rather than requiring a series of one-off requests – enabling individuals to be able to access data about them more easily. This would build trust in the intermediaries they use – building trust across the data ecosystem.

In facilitating the trustworthy sharing of data, data intermediaries can help to improve data availability and data sharing across the data ecosystem and the economy, bringing potentially significant improvements in terms of both productivity and economic growth. As such they can, and should, be considered a vital component of our economy's data infrastructure. There are limited incentives for individual private sector and third sector actors to build this infrastructure, so it is incumbent on the Government to reshape incentives to create, and support, data intermediaries.

Organisations and individuals collecting, using and sharing data need to be confident or provide *assurance* that data is fit to share and trustworthy - to inform their decisions and support their product and service offerings. Trust (or the absence of trust) in data and data practices can be a significant barrier to data sharing. To encourage data to flow between and within organisations, we believe that it would be beneficial to create a certification scheme for data intermediaries to demonstrate trustworthy data practices. This would complement the ICO's Code of Conduct and certification scheme and build public trust in data intermediaries, the data they are sharing and how they are sharing it. This would also provide additional information to government and researchers about the nature, scope and scale of data intermediary activity. Based on our extensive body of work and experience, we learned that when trust in data and organisations stewarding data increases, there is a related increase in data flow. This often leads to value creation in the form of products, services, insights and analyses from the data, and better decisions by governments, companies and communities, informed by data.

Strengthening the Bill - Smart Data Schemes

The Bill in its current form empowers the Secretary of State and the Treasury to introduce Smart Data schemes in consumer markets – as has been successfully done with Open Banking.

The ODI is delighted to have been appointed to the Government's Smart Data Council, working towards the worthy ambition of enabling the sharing of data about individuals with third-party providers on behalf of the individuals concerned, and at their request, as has been done so successfully with Open Banking.

We believe that if implemented correctly, the potential of smart data is exciting and highly valuable. Whilst the Government will likely utilise these powers in other consumer markets such as utilities and telecoms, it is currently not clear how these powers will be applied, how use

cases will be determined, and how the current lack of data skills and interoperability -the inability to transfer data between systems -will be tackled. We encourage the Government to consider some of the potential challenges around data sharing in these sectors so as not to hold back the positive potential of Smart Data schemes.

The more that the Government can enable and incentivise data portability the more it will enable and incentivise innovation and a wider range of services for consumers and businesses. Increasing data portability is likely to also boost the economy further, lower prices, and improve service offerings, far beyond what we currently imagine.