



## DATA SHARING DURING CORONAVIRUS

# Legislation to support data sharing

## *Summary of a private roundtable*

Gavin Freeguard and Paul Shepley

---

### Introduction

This short paper summarises a roundtable discussion held in summer 2022 about legislation to support data sharing in the UK. It brought together public servants and others involved in previous attempts to pass and implement data sharing legislation (including the Data Protection Act, General Data Protection Regulation and Digital Economy Act). The roundtable was held under the Chatham House Rule – nothing anyone said is attributed to them or their organisation, unless they have asked for it to be. The discussion does not represent the views of the Institute for Government.

The roundtable forms part of a wider piece of Institute for Government research looking at government data sharing during the pandemic. The project takes six case study areas and uses a roundtable on each to explore what worked well, what could have worked better and what lessons government should learn for the future. Reports on each of the roundtables will follow through winter 2022–23 and we will publish a short report drawing together key themes and recommendations in February 2023.

---

## Overview of legislation to support data sharing

Legislation to regulate information and how it is recorded, stored, shared, maintained and accessed is not new: for example, the UK's Public Records Act 1958 remains in force. But the recent growth in digital information has brought successive bills around the use of data and how it is protected and shared.

An early example was the Data Protection Act 1998, which enacted various European Union (EU) provisions around the processing – “the obtaining, holding, use or disclosure” – of information about individuals, giving individuals certain rights over their data. In 2003, the Privacy and Electronic Communications Regulations (again derived from EU law) came into force in the UK, covering subjects including marketing, customer privacy and cookies (small files of information that a website sends to a computer that is browsing it).

Over the past decade, major pieces of legislation focusing on data sharing include:

- The **Digital Economy Act 2017**. This includes provisions on data sharing across the public sector, and followed a major stakeholder engagement exercise with civil society.
- The **Data Protection Act 2018**. This supersedes the 1998 Data Protection Act to set a framework for data protection, incorporating and sitting alongside the General Data Protection Regulation (GDPR).
- The **General Data Protection Regulation (GDPR)**. This sets out principles, rights and obligations for the processing of personal data. There is now a distinction between the 'EU GDPR' – the original European regulations on which the UK version is based – and the 'UK GDPR', which came into effect in 2021. The latter made some changes to the EU GDPR after the UK's departure from the EU and the government is proposing further changes: significant divergence from the original could risk the UK's 'data adequacy' with the EU – a status where cross-border data flows are possible because the UK's data regime is considered to offer similar protections to the EU's for personal data.

During the pandemic, the Department of Health and Social Care also used Control of Patient Information (COPI) notices to mandate the sharing of patient information across the health system for Covid purposes. The government also tried and failed to introduce a new scheme for sharing patient data beyond the pandemic – General Practice Data for Planning and Research or GPDR (which should not be confused with the GDPR and which is covered by a separate roundtable and write-up in this Institute for Government project).

---

Following its pandemic experience and under the auspices of the National Data Strategy, the government published the *Data: A new direction* consultation in autumn 2021.\* This covered:

- data sharing in the public sector
- the powers of the Information Commissioner's Office (ICO)
- the grounds on which personal data could be stored and used
- other parts of the data protection regime (proposing to replace existing requirements that organisations should appoint data protection officers and conduct data protection impact assessments)
- international data flows.

Based in part on responses to the consultation, the government introduced a new Data Protection and Digital Information Bill, formerly known as the Data Reform Bill, to parliament in July 2022. This is now paused and at the time of writing it is not known when it will return.

## One thing legislation enabled

As an icebreaker question, we asked participants in our roundtable to name one thing the legislation they worked on improved or allowed to happen that could not have happened before. Their answers were that:

- It brought clarity to data sharing.
- It allowed public authorities to fill the gaps and identify the mismatches between what they wanted to achieve in policy objectives and what they are not able to do under the law.
- Government could not have delivered services and support to people during the pandemic (like the Clinically Extremely Vulnerable People Service) if it had not had the protection that legislation offered that gave people confidence in terms of what was going to happen to their data.
- It simplified the legal landscape, although cultural barriers meant that powers were not taken up as much as expected.
- Not that the legislation was designed with a pandemic in mind, but it allowed a relatively balanced approach to be taken, which may not have happened previously. Information sharing probably would have happened anyway, because it was necessary, but where it went well was typically where privacy was built into it; you do not just share everything, you share what you need for the purposes of performing whatever the task is. Ultimately it comes back to the point that legislation is not just a hurdle that cannot be overcome.

---

\* Department for Digital, Culture, Media and Sport, *Data: A new direction*, 10 September 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1022315/Data\\_Reform\\_Consultation\\_Document\\_-\\_Accessible\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document_-_Accessible_.pdf)

- 
- The GDPR enabled responsible data sharing between public bodies during the pandemic, which was really important for delivering vital services for vulnerable groups, without sacrificing people's information rights.
  - The Digital Economy Act reframed the conversation. Whenever data-related provisions and revisions came to parliament, they would be shot down for 'Big Brother' type considerations. Instead, as the Act went through, there was a shift from "We need to share data" to "Why? What's the purpose?", which shifted the centre of the conversation from data to the purposes it can be used for.

## Key themes from the discussion

- Legislation around data sharing has helped give certainty, scale good practice, force useful conversations (for example, around Data Protection Impact Assessments) and get things done, including facilitating data sharing that needed to happen during the pandemic. But legislation can be difficult to get right first time (especially with lobbying from individuals and organisations with an interest in a particular bill – see the section "Engaging others", below), can have unintended consequences (such as embedding inequalities and turning what had been small problems into bigger ones by enshrining them in law) and can be difficult to understand.
- Engaging the public from the start about how their data is used is critically important. Too often, the public and other stakeholders are convened around abstract discussions about data rather than around policies, purposes and decisions. Government needs to work hard to reach those affected by data-related decisions at an early stage.
- Looking at everyday scenarios and case studies that talk about the benefits of data sharing (and missed opportunities from not sharing data) is useful for helping politicians understand data issues, but senior leaders should also be expected to have a degree of data literacy.
- Legislation is not the main barrier to data sharing across government – other cultural and organisational barriers are more of a problem, including a lack of awareness of powers, fear about using them and different levels of capability and capacity across government. The pandemic has helped overcome some of them, but there are concerns as to whether that will continue.

## The benefits of legislation – and challenges

Jessica McEvoy, now at Scott Logic but formerly a deputy director at the Government Digital Service, recalled a digital product she had worked on in government, before the Digital Economy Act and Data Protection Act came into force. Her team thought that working without a legislative framework would help them to be more nimble and agile. Instead, they came to believe they were mistaken: without legislation, attention fades, leadership changes and priorities shift. Looking at other countries, it was clear that

---

**data sharing underpinned by legislation allowed things to get done.**\* It helps give people confidence that what they are doing is right, helps build and maintain momentum, and provides something 'solid' that civil servants can point to in order to make things happen. (Jessica's team, working without legislation, without anything to point to, took 12 months to get another government organisation to share data.) According to Jessica: "We learned that, counter-intuitively, rules help you go faster." Participants also said that legislation is a way of scaling and elevating bespoke advice to support people across government.

Legislation can **help force the right conversations** and put data protection at the heart of the process from the start. For example, one participant recounted how Data Protection Impact Assessments (DPIA) – a process to help "identify and minimise the data protection risks of a project" required by the GDPR\*\* – led to conversations in their team, forced them to address "hard questions" (such as: Did the DPIA address concerns around the needs of individuals versus the organisation's need to process their data?) and helped enable greater transparency, with the public and civil society able to analyse their assessments. For instance, during the first couple of years of the pandemic, the Department of Health and Social Care came under pressure to produce and publish its DPIAs. Their existence, setting out information including the department's approaches to data sharing and whether it was proportionate, created a sense of accountability that might not have existed otherwise.

But legislation has to be approached carefully: it can result in unintended consequences. So **government needs to take a step back and think about the original intent of the legislation.** For example, the Privacy and Electronic Communications Regulations (PECR) were intended to protect citizens and consumers from private companies infringing their privacy, but people having to constantly click on cookie pop-up windows without reading them was not the intent and does not work well for businesses or the public. The power of lobbying makes getting legislation right more difficult as people and organisations try to influence a bill (see the section "Engaging others", below) and governments try to keep different parties happy. There will also be a need to iterate legislation to achieve the desired outcomes: participants described it as a moving picture, difficult to get right the first time.

**Legislation can be too reactive.** The Cambridge Analytica story came to light as legislation was moving through parliament; the response from parliamentarians was "let's throw all these powers at the information commissioner". This did not get to the root of the problem and still allows organisations to follow poor data protection practice. Government needs to be more proactive, but at the moment most things are reactive – even the recent *Data: A new direction* consultation came out of the Covid response.

---

\* One participant noted that: "We look to see what other countries are doing – we don't want to be first to try something."

\*\* Information Commissioner's Office, 'Data protection impact assessments', ICO, (no date), retrieved 4 December 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments>

---

## Legislation has helped, but other barriers are significant

Several legislative barriers to data sharing have been addressed. For example, legislation has simplified the legal gateways for data sharing (which had previously proliferated). But **a lot of cultural barriers to data sharing remain**, meaning the take-up of data sharing powers was slower and lower than expected in the first few years of operation. One participant said: "It's not just about the law, it's not just about the legislation" – many challenges that need to be solved, things that do not happen or things that do not happen in the right way, are not things "we can necessarily legislate our way out of". These barriers include:

- a lack of awareness of the powers available
- different levels of data capability in different organisations
- different levels of confidence and fear in using the powers.

The powers in the Digital Economy Act came at the same time as the GDPR and messages about how careful people had to be with data. This dominated discourse and put a lot of people off data sharing. There was confusion about how powers could be used and it took time to get used to them. Data legislation remains nascent and can still be open to legal interpretation – sometimes public servants may be too quick to accept the advice of their departmental lawyer, who may not be a data protection expert. There are also demands on staff time and resources – in the aftermath of some legislation, some departments could not process all the requests for data they were receiving.

## Engaging others

Some participants said there had been a **"massive amount" of "intense" lobbying** around the GDPR. Lobbying is part and parcel of the legislative process, but when government consults on data issues, it tends to be larger corporates – for instance, big tech organisations – that are plugged into the issues and able to respond. Policy officials find it more difficult and time-consuming to seek out information from grassroots organisations that should have a voice in the legislation or other so-called 'harder-to-reach groups' such as young people.

On the other hand, there was a **"huge amount" of stakeholder engagement around the Digital Economy Act**, an open policy making process that was heralded as a pioneer and a success, where government worked closely with a civil society organisation focused on participation (Involve) to reach different groups and did a lot of work in the open (for example, publishing updates and inviting comments).

A key lesson from that experience was the need to **engage around domains, not data**. **Engaging around data can feel very abstract**, time-consuming and does not make sense to many people. It is "no wonder that people don't want to engage". As one moves out of the data stakeholder sphere, people and activist organisations are focused on all sorts

---

of issues (like health and social care), which all touch on data. Government should stop imagining that these groups will come and talk to it about data and should pay these groups more attention, but “that requires a different way of listening”. Conversations should focus less on data and more on policy decisions – what government is trying to do and why it is doing it, the role of data within those decisions and why it is using data rather than any other mechanism. Also, there may be groups who disagree with what government is trying to do, policy-wise, but the conversation is only about data. For example, the public could be completely trusting of the data that government is sharing about health provision but then their hospital is closed against their wishes and their trust in decision making and the use of data may decline as a result. “It’s not about the data, or at least it’s not only about the data, it’s about the decisions that you’re taking as well.”

There are **some areas where the public have never been brought into the conversation**, such as law enforcement data. There are multiple publics with different perspectives – some are ‘gung ho’ and say government should be doing more, while others are wary. How government has that conversation about where to draw the line for different purposes is important – it will not solve the public trust problem by putting the right legislation in place, but through ongoing public debate (including about the decisions as well as the data). Government can learn from the Digital Economy Act consultation and other models that exist. One participant discussed building a digital product where their team used an **external advisory group, comprising people with a more informed understanding of data use** around the subject area. They relied on them as a ‘design authority’ when building their product, which meant that when data sharing legislation was introduced, they already had a principles-based approach about the right ways to share data.

There is a real fear, as with the GDPR and the care.data programme,\* that a large proportion of the public might remove consent for their data to be used and shared. **That fear leads to nervousness about engagement and messaging** and means everything is left very late, until it is unavoidable, which risks causing the fear that government was worried about in the first place.

Government has to be open and honest. If it is worried about something, it is a sign it needs to engage earlier and ‘beyond its bunker’. Greater government transparency, both internal and external, would help get people on board; one participant recounted an experience of their team trying to resolve a problem among themselves, failing and making it a bigger problem, when speaking to others in government could have helped. People in government worried that the engagement around the Digital Economy Act would lead to the public saying “you cannot share data, privacy is king” and were pleasantly surprised when that was not the case: they tended to say “yes, but” or “maybe” more than “no”. The consultation team needed to be given the time

---

\* The care.data programme intended to bring individual GP records together so they could be used for research and planning. The programme was halted in 2014 after controversy about the lack of information given to patients, which was one reason the Major Projects Authority rated the project ‘red’ (successful delivery appears unachievable).

---

to develop strong relationships – with ministers and civil servants, and with civil society – so they were trusted by all sides to run the process. It meant there was understanding of what government was trying to do, if not always acceptance.

**Having a hard deadline for the introduction of the GDPR (25 May 2018) helped encourage engagement.** There was a huge build-up, which forced people to understand its importance, and that the legislation needed to be in place. There were advertisements on the radio, and there was lots of outreach (a whole team in government), and collaboration between government and the ICO. It was vital to talk to organisations to bring them on board, to understand, relay and address their concerns.

## Talking to politicians and senior figures

**Data protection is technical and dense and it is a challenge to explain to ministers.** Civil servants have to support ministers to understand the practicalities and start from a place where data protection is not seen like health and safety: seen as a barrier, rather than a means to facilitate things. The pandemic helped bring home the value of data sharing – useful data sharing case studies included delivering food parcels, scientific innovation and tracking the transmission of the coronavirus – but participants questioned how data sharing would continue in a 'business as usual' environment. Useful techniques for appealing to ministers include simple questions (Why are you sharing this data? How much of it are you sharing? And is that the right amount?), everyday examples and scenarios (of 'Bob the baker' or 'Janet the hairdresser') and case studies. Ministers have also started framing the discussion around not just examples of where data sharing is leading to benefits, but also where government inaction is blocking the full potential of data and wasting opportunities. Data is also coming up more in political and public conversation; for example, with Rishi Sunak making pledges during his Conservative leadership campaign about the Online Safety Bill and the Data Protection and Digital Information Bill in parliament.

Despite all that, people in charge still need **greater data literacy**: "We're long past the point where the people at the top can offload the entire responsibility to a third party to tell them what the right thing to do is." People in decision making positions should have some understanding of the law and of the basic protections people need, so they can understand the implications of saying 'yes' to something and the unintended consequences that could emerge. Leadership and the tone from the top is also vital. One participant gave an example of a former senior government adviser going to a select committee and saying: "We had to throw GDPR out to respond to the pandemic." This helped reinforce the erroneous message that the legislation was the main problem when it already enabled most of what was needed.

## Guidance and openness

**Data-related legislation is often "pretty dry and quite inaccessible" and not easy to read.** From a layperson's perspective, it can be difficult to pick it up and understand what one's rights are. This underlines the importance of the role of the ICO and others



---

in providing guidance to help people navigate their way through it. Participants said the **guidance, codes of practice and hub of resources associated with the Digital Economy Act are especially good** on how to use the powers of and how to comply with the legislation. The register, which shows the data sharing agreements made under the Act, and how the powers are being used for public benefit, is a success for transparency, which should help earn public trust in an area where people are particularly guarded. This approach could be replicated elsewhere.

## Fear, promotion and purpose

The **Digital Economy Act came at the same time as the GDPR**. At the same time as some people in government were saying that public authorities had a new open gateway for sharing data for specified purposes, others were apprehensive about the level of fine that could be applied. The priority became ensuring everybody was GDPR compliant, rather than looking at different and effective ways of using data. The ICO could have reissued its data sharing code earlier than it did to mitigate those fears and shift the focus to sharing data – when the pandemic came, it made a strong statement early on (that people should go ahead and share data), which was helpful.

**Clarity of purpose can encourage data sharing.** For example, the argument that it is sometimes more harmful not to share data cuts through in some areas – such as child safeguarding. People should consider the objectives they are trying to achieve and what their role is as a public service provider – and appreciate that by not sharing data, which they could realistically and responsibly do, they are missing those objectives and doing more harm than good. During the early stages of the pandemic there were “too many” examples across government of people seeking legal advice prematurely; lawyers can advise on the right data sharing gateway if they know what data people want to share, with whom and why, but this was often unclear or lacking.

## The regulator

The ICO has embarked on a “massive expansion” since the GDPR, in terms of numbers but also its capabilities. Government must continue to recognise that the regulator **should be properly resourced and able to take action**. The ICO took a proactive role during the early part of the pandemic in talking to people in government and others about how they could share data and the harms that can come from not doing so. There are some questions about its changing role. For example, should it be a ‘data protection officer for hire’ that has a larger advisory function for public bodies? The regulator also needs enough information from government organisations to do its job: in some cases it was apparently not provided with such information (for example, about Covid apps) early enough, particularly how they used data and what the privacy implications might be.

As the GDPR went through, there was **lots of discussion around the ICO’s ability to fine people and organisations**, prompting questions about whether public sector organisations should be fined, whether fines levied on companies would have an impact

---

on the UK economy and so on. These discussions grabbed headlines, even though fines are only part of the regulator's role. This may have contributed to the fear in sharing data.

The regulator can come under pressure from civil society and campaign groups to take more enforcement action, even though it would probably rather avoid this from happening by working more upstream. It may be that **civil society organisations press for fines because it is seen as the only tool in the box** – and might react negatively to quiet behind-the-scenes conversations with big business. Whenever the public are involved in discussions about science, technology and innovation (not just data), they are interested in governance, regulation, accountability and how they can trust processes (legislation is only part of the jigsaw). Legislation for transparent, trustworthy governance mechanisms could make that upstream process of quiet conversations more trustworthy.

## Key lessons and recommendations from participants

Participants drew out several key lessons and recommendations for government based on their experience of previous data sharing legislation. These included:

- When it comes to the public, government should engage early, engage often but not engage about the data – engage on particular policies, purposes and problems. It should do so openly and honestly, rather than being scared to talk to the public and creating bigger problems (for example, people opting out of their data being used) by not engaging until it is too late. Engagement should also include going beyond data stakeholders to those dealing with domains touched by data (like health and social care) and to the people affected by it.
- Government should use the Data Protection and Digital Information Bill as a way to grip the messaging around data – and highlight and promote the benefits of data sharing, rather than focusing on managing fear.
- Making data sharing agreements and how data sharing powers are being used for public benefit transparent could increase public understanding and support.
- Government should find the best case studies and ensure that it learns the right lessons from the pandemic. "There were lots of positive cases of data sharing during the pandemic. People took a proactive approach. Barriers we thought were insurmountable turned out not to be. Now we're returning to business as usual, are those barriers resurfacing or are we applying the right lessons?"

**Gavin Freeguard** is a freelance consultant and associate of the Institute for Government  
**Paul Shepley** is a data scientist at the Institute for Government

**The Institute for Government is the leading think tank working to make government more effective.**

We provide rigorous research and analysis, topical commentary and public events to explore the key challenges facing government.

We offer a space for discussion and fresh thinking, to help senior politicians and civil servants think differently and bring about change.

**Copies of this IfG Insight are available alongside our other research work at:**

 [instituteforgovernment.org.uk](https://instituteforgovernment.org.uk)

 [enquiries@instituteforgovernment.org.uk](mailto:enquiries@instituteforgovernment.org.uk)

 +44 (0) 20 7747 0400     +44 (0) 20 7766 0700

 [@instituteforgov](https://twitter.com/instituteforgov)

**Institute for Government, 2 Carlton Gardens  
London SW1Y 5AA, United Kingdom**

**December 2022**

**© Institute for Government 2022**

The Institute for Government is a registered charity in England and Wales (No.1123926) with cross-party governance. Our main funder is the Gatsby Charitable Foundation, one of the Sainsbury Family Charitable Trusts.