10 steps to fix government to government data sharing

DATA Alliance

By Fabian Chessell, Mor Rubinstein and Neil McIvor, August 2025. Views are our own.

Our data sharing system is failing citizens

As support for democracies falls and public services are cut back, how is it ok that:

- Councils, police & the NHS share less data for child protection in 2025 than in 2010?
- 230,000 children go to school hungry because we don't use data to auto-enrol them?
- Police redact data from CPS prosecutors for data protection laws?
- "Tell Us Once" a service only available for the dead, not the living?

The costs of not sharing data are extraordinarily high

The impacts hit our wallets and our lives. They include:

Hundreds of billions of pounds. The UK government estimates £45bn p.a. savings from public sector digitisation. How much can realistically be delivered without data sharing? Even in the optimistic scenario where data sharing is eventually forced through, a 2 year acceleration would save £90bn, enough to pay for the New Hospital Programme, doubling our fleet of type 31 frigates, doubling our apprenticeship programme, with money left over to fund adult social care reform for a parliamentary term.

Society is less safe as policing, the NHS, and other public services get worse. It infuriates doctors and nurses, makes medication mistakes more likely and inhibits prevention. It makes lives harder for people with mental health conditions, and frustrates efforts to help children out of cycles of poverty. It makes it harder to catch criminals, keep victims safe from ex partners, or protect children from harm. It is literally a matter of life and death, as the review into the deaths of Arthur Labinji-Hughes and Star Hobson wrote:

> *"Problems with information sharing have been raised by every national child protection review and inquiry going back to 1973. Time and again different agencies hold pieces of the puzzle but no one holds all of the pieces or is seeking to put them together."*

Those are only the biggest impacts. Others include: Policies are made in the dark ✦ Weakened pandemic and emergency response ✦ We waste countless hours filling in unnecessary forms and re-entering information ✦ Local government and devolution is undermined as data is hoarded centrally ✦ Reinforces mental health or digital exclusion barriers ✦ Declining trust in democracy.

As the Afghan "kill list" scandal proves: failing to make secure sharing easy leads to workarounds with disastrous consequences.

N.b. We focus only on UK government to UK government personal data sharing, including:

- *Bulk data, as needed for auto-enrolment, fraud and error, and prevention efforts*
- *Transactional 1-by-1 data, as needed for registrations, like your passport application*

Our scope is not on other government-related data sharing, so we are excluding Open Government (e.g., FOI's), Open Government Data (e.g., bus times), Government to Business, Government to Academia, Smart Data schemes (e.g., Open Banking), or government's data gathering powers (e.g., surveillance), nor on corporates like Meta.

It's not "just a culture problem"

Policymakers and lawmakers are usually confused about data sharing: They experience that data sharing is a problem and some advocates calling for fundamental reform, yet hear from others that existing laws allow most data sharing, and we need to 'just fix the culture'. No wonder they are confused!

Our message is: they're both right. It is right to say there is a cultural problem, but to fix it requires legal reform because the culture is a consequence of the incentives and processes set out in law. And while it is right to argue that existing laws allow most data sharing, the problem is not 'just' culture: **The fundamental problem is not that sharing is illegal, but that it is so slow & expensive, so conservative, and so complex that nearly all efforts are impeded.** The vast majority (90%+) of data sharing time & expense is now paperwork or "sludge", not technical implementation. We see three fundamental challenges:

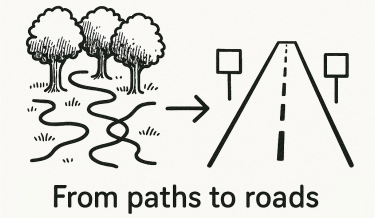
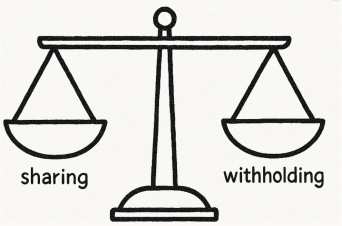
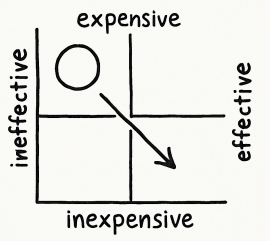
1. **Each new data share is treated as a snowflake**, individually designed, negotiated, legally reviewed, impact assessed, and so on, creating a mountain of paperwork. Even if you are the 219th hospital sharing the same data for the same reason! This is slow, expensive, insecure, unscalable, inflexible, unequal. It encourages transferring data so it is duplicated, instead of making it easy to access it from secure locations. We want services that are as good as or better than the private sector, but no company is signing data sharing agreements with itself, nor creating data infrastructure like this.
2. **It is wildly conservative. It is safer to do nothing.** Risk assessments consider the risk of sharing data but ignore the harms and costs of withholding data. Shares have many approvers (20 is not uncommon) with multiple sets of lawyers, a recipe for conservatism. We ask junior staff to risk criminal sanction for another team or department's effort. It is all stick, no carrot. No wonder they are reluctant.
3. **Proactive, preventative, and prototypes are frustrated** by complex rules on minimisation and proportionality that are interpreted conservatively. How can you be agile, 'testing and learning' in 2 week sprints, when data protection can take 2 years? How can you spot the needle in the haystack if you can't look through the haystack?

It is not simply a case of leadership support, or it would have been fixed by now. Over a quarter of a century ago, the Blair government wrote in their 1999 Modernising Government white paper that they will "streamline the collection and sharing of data so that we can better manage government information". This could have been in the 2025 State of Digital Government Review. Civil servants tell us that "sure, Labour say they want data sharing, but so did the Tories, and Labour before them. Nothing's changed." **We cannot hope for the best but do nothing different. Unless we take a different approach, we will fail.**

A focus on speed and balance

Only by making data sharing cheaper, faster, and risk-balanced will we see noticeable improvements.

Our 10 point plan aims to deliver three fundamental changes:

Principles for our 10-point plan		
		
Shared data infrastructures. Every data share shouldn't be a path through the forest. We must build highways. Like in the private sector, data should be brought together, cleaned, matched and secured for many purposes.	**Move the presumption towards sharing** when in the public interest. We must better balance the cost and harms of withholding data with the risks of sharing data.	**Lower compliance costs safely.** We have a system that is high impedance but low protection. We must flip this. We need to deliver citizen outcomes, not process.
While keeping GDPR: Leaving GDPR would cause years of disruption. Targeted amendments will create more value sooner.		

While the strategy of the National Data Library has not been released, we have not seen that it has the political mandate to make changes at the scale that we seek.

10-point plan

Shared data infrastructure

1. **Pre-approve sharing within clusters of public services.** GDPR was written with little regard for how public services are organised. Hospitals, GP surgeries, and pharmacies operate in one system yet are separate legal entities, facing bigger barriers to sharing our data than the global tech giants. Within a "crime and justice" cluster, a "health and social care" cluster, and a "human services" cluster (education, councils, benefits) we propose organisations[1] are considered as one organisation with shared public tasks, and sharing data for those purposes is presumed approved. France changed this presumption in 2022, showing it can be done. Shared data infrastructure can be built and used by cluster members. Protections including purpose limitation for use, confidentiality, transparency, etc would continue to apply.

2. **Approve once: permit reliance on other organisations' data-sharing decisions.** Currently, each of the 330+ councils, 202 NHS Foundation Trusts, 6200 GPs must come to their own decisions about what data can be shared, creating a mountain of paperwork and incompatible and often arbitrary determinations preventing shared data infrastructure. Allowing public sector organisations to rely on other organisations' decisions would fix both these problems. A requirement to register such agreements would provide transparency, and the ICO could perform non-binding mediation to address significant public concerns with widely used agreements.

3. **Create light-weight federated data exchange like X-Roads[2] in each cluster.** These exchanges would be lightweight, offering a security, access control, service director, and a legal framework. The APIs are implemented by each organisation, and managed cluster-by-cluster. These exchanges would facilitate hundreds of smaller use cases where there is no justification to create a shared database, or where this would be dangerous, e.g., health records.

[1] Or teams within organisations.
[2] A service that makes it very easy to exchange personal data between public services, pioneered in Estonia https://e-estonia.com/solutions/interoperability-services/x-road/

Move the presumption towards sharing

4. **Create a duty to share data in a citizen's interest.** Currently, there is no requirement for data to be shared, meaning the Data Protection Officer considers potential future risk of sharing data but not the harms of withholding data. Creating a duty to share would restore balance. Such a duty should be considered to satisfy confidentiality obligations, e.g., HMRC's confidentiality obligations for income data. Tell Us Once is a right that should not be available only to the deceased. Belgium and Estonia have both passed "Tell Us Once" laws to oblige the government to use data it already has in preference to asking for it again.

5. **Data protection risks should be held by one team: the receiving business team.** Currently, decisions on whether to share data are taken by the sending Department or organisation, who have no stake in delivery of the public service, and a Data Protection Office within the receiving organisation who again has no responsibility for delivery of the service but takes on potentially criminal liability if the share is found not legal. We need to end the 'all pain, no gain' arrangements. Any data protection responsibility of the sending department should end when the data is shared.

Lower compliance costs safely

6. **Endorse prevention and reverse the burden for 'proportionality' and 'minimisation' principles -** Currently, GDPR requires data shared to be "proportional" and "minimal" for the specific purpose. This is a difficult bar to meet for preventative and proactive use cases, where searching for a needle in the haystack requires looking through a haystack. GDPR should be amended to endorse the use of data for prevention and proactive support and to reverse the burden for 'proportionality' and 'minimisation' in the public sector so that it must be shown why it is justified that data is withheld.

7. **Direct the ICO to shift its focus from 'eliminating risk' to 'support public sector delivery, safely'.** Assign the ICO a purpose of safely increasing the volume of government-to-government data shares and reducing their cost. Amazingly, the ICO does not have such a duty today. It has one to 'promote innovation' but that is not clear enough. The government should also issue a Statement of Strategic Priorities to the ICO under the DPA 2018. The ICO should be asked to measure and improve the volume, speed, and cost of data sharing. This will lead to the ICO reducing low-protection high-cost regulations and guidance.

8. **Civil service leaders must provide "air cover" and be held to account for rapid delivery.** Multi-year 'data strategies' will do nothing. Civil service leaders and Ministers routinely profess support for data sharing, but the accountability for actually approving data shares falls to relatively junior staff. Leaders should do three things. Firstly, publish risk appetite statements setting out they expect some risk in delivery. Secondly, they should let data sharing teams know they will 'have their backs' if there are problems. Thirdly, they should have escalation routes for data shares that are either denied or bogged down in design-by-committee. PermSecs and CDOs should be managed on delivery of both specific data shares ('canaries in the coal mine'), and overall data share delivery as measured by delivered, declined, and backlogged data shares. These should also be published publicly.

9. **Shift enforcement regime to support improvement and allow for emergent use cases.** The threat of a breach leads public sector leaders to take a very conservative approach to data sharing. The repercussions of a breach may dissuade enforcers to err against finding a breach. A belief that data protection needs to be perfect from the start for even the smallest project inhibits experimentation. The enforcement regime should focus on requiring improvement over time as systems mature. This will allow programmes to move forward at pace in a more agile way, and reduce the all-or-nothing approach to enforcement.

10. **Publish KPIs -** DSIT and Cabinet Office Ministers should publish KPIs on amount of data shared / uses of shared data, the size of data share backlogs, the rollout of key priorities, e.g., for multi-agency child protection, the speed, cost, and size of data protection compliance processes and paperwork. We manage what we measure.

Who are you? How can I help?

We are DATA, the Don't Ask Twice Action Alliance, public sector data experts and builders driven by the urgent need to overhaul government data sharing if the UK is to have the excellent public services that citizens need and demand. This manifesto is our vision for change. Learn more about us at dataalliance.uk.

In government and **want to learn more?**
Reach us at hello@dataalliance.uk

Have you got **infuriating examples** of frustrated attempts to share data?
Share your experience with us at hello@dataalliance.uk

Maintaining protections and addressing civil liberty concerns

A new approach to data sharing, to be politically realistic and sustainable, needs to be trusted. Therefore, as proponents of governmental data sharing and as citizens, we have crafted these proposals mindful of **maintaining essential protections while enabling the progress this country desperately needs**. We are seeing other countries take significant steps to unblock data sharing, such as when France passed its 3 D's law in 2022, and even the EU, following the Draghi report on competitiveness, is simplifying data sharing rules. It would be ironic, then, for the UK to lag Europe on this effort.

We also believe it is **self-defeating to damage a democracy's ability to deliver for its citizens in an effort to create what would be, at best, a mild speedbump for a dictatorship**.

Implementing the 10-point plan can maintain or improve protection in the following 6 ways:

A. **It retains GDPR, and retains existing confidentiality principles,** including purpose limitation for use, confidentiality, transparency, right to object, right to rectification.

B. **We avoid the few "third rail" topics people really do care about. It is not:**
    a. Making it easier for Meta or Google to use your data
    b. Opening up health records to all and sundry
    c. Allowing law enforcement to 'snoop' through all your records
    d. Proposing universal digital ID

    ... it may even be clever politics to package this 10 point plan with greater restrictions on tech firms' use of citizens' data.

C. **We argue for regional shared data infrastructure** including and especially for health where we want to avoid national data sets. Mayoral combined authorities could be a good size for shared data infrastructure for the human services cluster.

D. **We increase transparency and could increase transparency of use.** We propose that "Apply Once" relies on publicly registering data sharing agreements, increasing transparency. The UK could also adopt approaches, like those in Estonia, where governmental access of your government-held data is logged so you see who is using your data and why. We should always be transparent about *what* processing undertaken on citizen's data.

E. **Create processes for constructive, improvement-oriented engagement with concerned advocates,** including through ICO mediation of widely adopted DSAs and moving enforcement to an improvement-oriented footing. The current regime, in determining permissibility, creates a harmful high-stakes 'winner takes all' situation.

F. **Time limitation for prevention / proactive / emergent use cases,** where data sharing or processing permitted under these reasons is reviewed ex-post after a period of time, e.g., at 12 and 24 months.

Our 10-point plan will rightly be subject to scrutiny and opposition. But some data protection advocates will be implacably opposed:

- Critics might argue that today's processes work just fine or we have struck the right balance between progress and protection today. We see too much preventable harm and suffering to agree with them. This will require a political determination, is the status quo really acceptable?

- Others will argue that we could simply address the conservative culture without changing the laws. To this latter group, we argue that a plan that starts with 'if people just…' is not a credible plan. People are conservative because of the balance of incentives and punishments placed on them by today's law - a system that is 'all stick and no carrot'. We cannot hope for the best but do nothing different.

- Finally, others might say they agree, but seek an added protection here or there 'to maintain public trust'. It would be arrogance personified to argue our plan is the only viable plan. But, there should be no confusion: the purpose of this plan is to improve data sharing while maintaining core protections, not to increase protections. When the public are asked about their top concerns, they respond they are the NHS, the state of our economy and public services, and the cost of living. Is sacrificing public service improvement for additional protections the right choice?