10.5258/SOTON/PP0122

Response to the UK Government Call for Evidence on Data Intermediaries

Authors: Laura Carmichael, Michael Boniface, Age Chapman, Wendy Hall - Web Science Institute Roberta Data Trust Team

Q1. Can you provide examples of where data subject rights are currently exercised by third parties on the instruction of, or in the interest of, the data subject?

The Roberta Data Trust — under development by the University of Southampton, Web Science Institute as part of the Southampton Biomedical Research Centre —is a leading example of a data intermediary model that exercises data subject rights on behalf of individuals. The intention is to enable individuals and communities to voluntarily donate their personal health data to support others, e.g., through research and policy change, in a way ensures their data is handled with care, transparency, and consent. Through co-designed governance structures, the Roberta Data Trust model aims to facilitate responsible, safe and secure data access and use by third parties for health research and innovation. Data subject rights are exercised in accordance with the preferences and values of participants, thereby ensuring the data use is truly in their interest.

While this approach is still under development, similar models already exist. For instance, in personal finance, Open Banking enables users to grant access to their data to third-party providers who act on their behalf (as also highlighted in the call for evidence). In healthcare, some patient-facing platforms enable individuals to authorise applications or carers to access and manage their records. These examples highlight the feasibility and growing demand for trusted intermediaries that act in the individual’s interest while exercising data rights on their behalf.

Q2. What barriers do individuals, businesses, or other organisations face in the uptake of the right to data portability or other data subject rights?

Several significant barriers include:

- Lack of interoperable technical systems and APIs across healthcare providers.
- Limited public awareness or understanding of data rights.
- Uncertainty around the legalities of secondary data use and consent models.
- Absence of trusted intermediaries to act on behalf of individuals.

The Roberta Data Trust model is taking such barriers into consideration such as, by evaluating the acceptability of different models for data sharing, and the extent some of these barriers could be addressed through the approach (e.g., by implementing participatory governance).

Q3. Aside from personal data protection laws, how do other areas of law interact with the operation of data intermediaries?

Relevant legal domains include:

- Contract law — e.g., governing agreements between data subjects and data intermediaries.
- Medical law and ethics — e.g., relating to informed consent and duty of care.
- Equality law — e.g., concerning inclusive access to health data services.
- Intellectual property law — e.g., related to proprietary data management systems.

The Roberta Data Trust model operates within these intersecting frameworks, ensuring ethical and lawful operation. It should also be noted that the Roberta Data Trust model is based on Jersey trust law. Therefore, an additional legal domain is also highlighted (where applicable):

- Trust law — e.g., in terms of fiduciary obligations.

Q4. Does the taxonomy above fully reflect the range of models of data intermediaries in the UK or elsewhere?

While the current taxonomy outlines useful archetypes, it does not fully capture hybrid or participatory models like Roberta. The Roberta Data Trust model combines characteristics of data trusts, data stewardship, and participatory governance, necessitating a broader or more nuanced classification in policy frameworks.

Q5. Is the current law around the operations of data intermediaries sufficiently clear? What changes and/or additional guidance would be required to provide clarity to data intermediaries? Does this differ based on operating model?

The legal framework lacks clarity on:

- The delegation of data subject rights.
- Liability and accountability of intermediaries.
- Standards for ethical governance.

The Roberta Data Trust model's design process highlights the need for statutory guidance or certification mechanisms for data intermediaries, particularly for trust-based and public-interest models.

Q6. What are the main barriers to performing data intermediation services in the UK, and how do they differ across sectors and models?

Identified barriers include:

- Interoperability and infrastructure gaps, especially in the NHS.
- Fragmented and non-interoperable data access policies.
- Sustainable long-term resource and funding limitations.
- Low levels of public trust and understanding.

The Roberta Data Trust model faces these challenges in attempting to coordinate data access across community, public and private health data holders.

Q7. What role should the government have in addressing these barriers? Are there examples of effective or ineffective government interventions in other countries or markets?

Government can:

- Provide legal recognition and certification for intermediaries.
- Invest in public infrastructure and interoperability.
- Support inclusive public engagement and ethical frameworks.

Internationally, Findata (Finland - https://findata.fi/en/) and the Health Data Hub (France - https://www.health-data-hub.fr/) demonstrate state-supported models for secondary data use operating under a centralised model of data governance, offering some parallels to “trusted research environments” (TREs) and the NHS Secure Data Environment network in the UK.

These public services operate more as a centralised data platform and infrastructure provider than as a traditional "data intermediary" in the sense described by the UK government's taxonomy (e.g. data trusts, fiduciary stewards, or portability agents). They do not act on behalf of individual data subjects to exercise their rights, such as delegating access, modifying consent, or enforcing portability. Governance decisions are made at the institutional level, not through participatory models involving data subjects. They operate under state authority and legal mandates, not as an independent steward or fiduciary representing individuals' interests,

Q8. Can you provide examples of successful data intermediaries and the technological and non-technological factors that contributed to their success?

There are several notable examples of successful data intermediaries across healthcare and other sectors that demonstrate the importance of both technical infrastructure and social governance.

In Switzerland, MIDATA (https://www.midata.coop/en/home/) operates as a data cooperative allowing individuals to store and control access to their personal health data. Its success stems from a secure digital platform combined with a cooperative governance model, where members co-own the organisation and decide how data is used. This blend of user agency, transparency, and technical trust has enabled meaningful participation in biomedical research.

In Finland, Findata (https://findata.fi/en/) serves as a government-mandated health data intermediary, streamlining access to sensitive datasets through a secure computing environment. Its legal mandate, standardised processes, and strong institutional trust have positioned it as an effective public data steward.

Meanwhile, MyData (https://mydata.org/), an international initiative rooted in Finland, has advanced the model of personal data intermediaries, where certified operators act on behalf of individuals to manage data flows. Success here relies not just on APIs or consent tools, but on shared human-centric principles, cross-sector collaboration, and a certification framework that ensures compliance with ethical standards.

These examples show that successful data intermediaries combine technical capabilities — such as for data minimisation, secure access, and interoperability — with non-technical elements — like participatory governance, clear legal frameworks, and trust-building practices.

Importantly, they reflect different models, from public authorities to cooperatives, each suited to specific social and legal contexts.

Q9. Can you provide any evidence on potential risks for the wider exercise of data subject rights by third parties (such as data stewards) on behalf of a data subject? Can you identify any risks associated with the activities of data intermediaries?

Potential risks associated with the activities of data intermediaries include:

- Misrepresentation of participant interests.
- Consent mechanisms becoming outdated.
- Governance capture or mission drift.
- Lack of data related expertise

It is important that consideration is given to how such risks can be mitigated from the outset (e.g., planning and co-design phases of a data intermediary), such as through structured co-design, independent governance boards, and adaptive consent strategies.

Q10. Are there potential implications for digital inclusion of delegation of data subject rights and the activity of data intermediaries? Are there any disproportionate effects on those with protected characteristics under the Equality Act 2010?

Without inclusive design, data intermediaries could exacerbate inequalities. It is important that data intermediaries incorporate diverse voices into governance structures to prevent exclusion and ensure alignment with the Equality Act 2010.

Q11. Can you provide any evidence of a best practice approach to managing those risks? What should the roles of Government, regulators, and the market be?

Best practices from the Roberta Data Trust approach include:

- Co-design of governance frameworks.
- Independent oversight.
- Clear, adaptive legal models for data access.

Government and regulators should facilitate regulatory sandboxes, establish accreditation schemes, and support ethical infrastructure development. The market can contribute by innovating with integrity within these frameworks.