

Empowering people through data intermediaries

Open Data Manchester workshop — non-attributable readout

Date: 25 August 2026 **Format:** One-hour online session **Participants:** Around fourteen, spanning data cooperatives and community data initiatives, place-based data trusts, digital identity and verification services, trade union and worker data rights, academia, geographic information, and software and data businesses.

Open Data Manchester convened this session to help people prepare responses to the government consultation *Empowering people through data intermediaries*, which closes at 11:59pm on 31 August 2026. The session was structured as an overview of the consultation followed by open discussion.

This readout is non-attributable. Points are recorded as raised, without attribution to individuals or organisations. Where a participant described a specific operating model, it is summarised in general terms because the substance of the point depends on it.

Background: the consultation

This section is context on the consultation itself. It is not a record of the discussion.

The consultation was published on 8 June 2026 and follows a call for evidence run the previous year. That call for evidence identified three barriers limiting the uptake and growth of data intermediaries in the UK:

- **Lack of legal clarity** — UK GDPR explicitly permits delegation of Chapter VIII rights (complaints, judicial remedy, compensation) to a third party, but is silent on Chapter III rights, which include access, objection and, critically, data portability. Controllers read that silence as a prohibition and refuse requests from intermediaries on that basis.
- **Friction between controllers and intermediaries** — delay, unclear obligations, non-compliant data formats, and a lack of standardised processes for responding to delegated requests.
- **Low user awareness** — of intermediaries' existence and of their potential utility.

The consultation is deliberately narrow in scope. It covers **personal** data intermediaries that help individuals exercise the right to data portability on their behalf and with their explicit permission. Non-personal data intermediaries sit in a separate workstream, and data brokers and aggregators are explicitly excluded, having been the subject of a separate call for evidence.

It proposes a taxonomy of intermediary types — data wallets, personal information management systems, data unions, data cooperatives, data trusts, and trusted research environments — and sets out seven options, which government states are not mutually exclusive:

Legislative

1. Amend UK GDPR directly to permit delegation of Chapter III rights. 2a. Align with international frameworks such as the EU Data Governance Act — notification, register, certification mark. 2b. A UK authorisation framework, ranging from light-touch notification to full licensing, potentially also setting expectations on how controllers respond to delegated requests.

2. Mandate portability APIs for firms designated with Strategic Market Status under the DMCC Act 2024.

Non-legislative 4. A non-statutory, industry-run authorisation scheme with a public register or trust mark. 5. A statutory ICO code of practice. 6. An industry-led voluntary code. 7. New ICO guidance.

Government's stated position is that comprehensively resolving the legal uncertainty is likely to require legislation, and it explicitly invites views on whether a register or similar, absent that legal clarity, risks becoming an additional layer rather than a solution.

Discussion: points raised

1. Where do data intermediaries sit in relation to everything else government is doing?

This was the most persistent theme of the session and was raised independently by several participants.

Participants found it difficult to place the consultation within the wider landscape of digital identity, smart data, and digital competition work. Specific gaps identified:

- **The digital verification services trust framework** established under the Data (Use and Access) Act 2025 already defines roles for holding and sharing individuals' data, including the holder service provider role. Participants working in that space take the view that data intermediaries fall outside the trust framework and would sit as relying parties on it — but the consultation does not address the relationship at all. The concern is that intermediaries positioned outside the framework will encounter precisely the compliance obstacles the trust framework was built to resolve.
- **Smart data schemes** and the well-defined APIs and access governance developed under them are not clearly linked to the consultation, despite being the closest working analogue. It was noted that open banking, which goes considerably further than portability, originated in competition policy rather than data protection.
- **Digital competition work** — the portability API option (Option 3) is recognisably the kind of asymmetric obligation on large firms that the CMA has historically imposed, but the consultation does not situate it that way.

One participant summarised the difficulty as feeling like reassembling something and being left with a part with no obvious place to go.

2. The proposed definition of a data trust may be too narrow

A substantive challenge to the taxonomy. The consultation describes data trusts as collecting, storing and aggregating personal data. At least one operating model does none of these: the individual settles the *rights* to their data into a trust while the underlying data remains with whoever already holds it, and the trustee governs the interaction with that data rather than possessing it.

The direct question for government: **is it the intention that a data trust must collect or store the underlying personal data, or can an intermediary be a trustee holding authority over use and interaction without ever holding the data itself?**

Related points raised in this discussion:

- The fiduciary structure was described as answering the problem of people who want to act on their data but do not want to engage with the technical detail: a trustee under a duty of undivided loyalty, who cannot be incentivised by money, acts in accordance with the settled purposes.
- Such purpose-bound structures depend on legal mechanisms that are not available in every jurisdiction. The model described relies on a non-charitable purpose trust under Jersey law; participants noted that the equivalent is not available under English trust law. Jersey is a Crown Dependency and outside the UK, so the question this raises for the consultation is whether the proposed framework would recognise an intermediary constituted under the law of another jurisdiction while acting for UK data subjects.
- Handling **granularity of purpose** is an open problem: a single clear purpose works well, but real consent is partial and conditional. One approach discussed was using agentic AI to interpret incoming requests against the settled purposes of the trust, with enforcement remaining with the trustee.

3. Small-scale and community intermediaries risk being designed out

Several participants work at community or place-based scale, with flat governance structures and no technical staff. The concerns were consistent:

- Any authorisation, registration or licensing burden calibrated to commercial intermediaries could be disabling for small collectives, and the consultation's framing is strongly oriented to market growth and innovation.
- The value of an intermediary at this scale is precisely that it removes the need for participants to understand the technical detail. People want to act collectively on their data; they do not want to learn about it. That is a different value proposition from the market-making one the consultation foregrounds.
- A worked example: household energy data, held by suppliers via smart meters, is detailed enough to support behavioural analysis. The question that matters locally is whether the framework enables or disables a community pooling that data for collective benefit and transacting with organisations of its own choosing.
- A long-running place-based data trust project reported that the hardest part, from a non-technologist position, was finding technology that would actually do what the governance model required. Frameworks that assume technical capacity will not reach these organisations.

4. Technology-specific mandates risk lock-in and market consolidation

Concern that some options, particularly around mandated APIs, are prescriptive about technology in ways that will date badly and may concentrate the market.

- Writing a specific technology into a framework was described as writing itself into a corner: APIs are useful and widely used, but tying the regime to them places it in a moment in time that may not survive a year. The preference expressed was for technology-agnostic obligations, with the technology treated as the means of enforcing legal governance rather than as the governance itself.
- This was reinforced from practice: participants described moving between hardware security modules, quantum encryption approaches and emerging agent-to-system protocols as the field changes.
- A separate concern was that mandating provision by the largest firms may entrench those firms as the reference implementation.

5. Trust in the human sense, not the legal sense

A distinct challenge to the framing. The consultation's trust-building options are concerned with whether controllers and the market can trust intermediaries. Participants argued that the harder and more important question — how an individual decides whether to trust an intermediary, a verification provider, or a large platform offering an API — is barely addressed by any of the seven options.

The related observation was that the consultation repeatedly drifts from empowering people to empowering organisations, despite the former being its stated purpose.

6. Definitional and terminological confusion

- Participants reported confusion between data intermediaries and data brokers, both in wider discussion and, in places, within the document itself, notwithstanding the stated exclusion of brokers.
- The term "data intermediary" already has a settled ordinary meaning for many practitioners — the payment rails and intermediating services people use daily — which sits awkwardly with the consultation's specialised use.
- The volume of new terminology was noted as a barrier in itself.

7. Is amending UK GDPR necessary at all?

Raised as a direct question: given that data intermediaries already exist and operate, does the legislation actually need to change?

The response offered in discussion was that the class of intermediary that depends on the *right* to data portability is the genuinely constrained one, since both the existing holder and the intermediary are data controllers and the position is unclear. By contrast, smart data schemes use the *concept* of portability rather than the right, operate as separate schemes alongside UK GDPR, and function without amendment.

A consequence was flagged: clarifying delegation of portability rights would enable the community-scale and rights-based intermediaries the consultation describes, but it would equally enable the largest platforms to accept delegated portability rights and build products on them. Any clarification is available to everyone.

8. EU adequacy

Concern that amending UK GDPR risks divergence from EU law and the UK's adequacy status, and that the cost of losing alignment would outweigh the benefit of the clarification. This was linked to the observation that divergence would run counter to the perceived current direction of UK policy.

9. Scope: does this apply to non-personal data intermediaries?

At least one participant operating as an intermediary for non-personal data was unclear whether the consultation applied to them or whether responding was worthwhile. The consultation does state that non-personal intermediaries sit in a separate workstream, but this is not evident without reading closely, and the effect is that organisations that might usefully contribute are unsure whether they are in scope.

10. Process and timing

- The consultation runs across the summer holiday period and closes on 31 August. Several participants, including organisations directly in scope, became aware of it late.
 - The previous call for evidence was also missed by participants who would have contributed, including groups convened specifically around data cooperatives.
 - Awareness is one of the three barriers the consultation identifies. The difficulty this room had in learning about the consultation, and the difficulty in assembling a coherent response from a dispersed group within the window, is itself evidence bearing on that barrier.
-

Points that may warrant a direct response

Drawn from the above, the following are questions or observations that could usefully be put to government by respondents:

1. Must a data trust hold or aggregate the underlying personal data, or does the definition accommodate a trustee governing authority over use and interaction without possession?
 2. How do data intermediaries relate to the digital verification services trust framework under the Data (Use and Access) Act 2025, and to smart data schemes? Are intermediaries relying parties on the trust framework, and if so, does that resolve or reproduce the controller friction identified in the call for evidence?
 3. Will any authorisation or registration requirement be calibrated so that community-scale and cooperative intermediaries with flat governance and no technical staff can meet it?
 4. Can obligations be framed technology-agnostically rather than specifying particular mechanisms such as APIs?
 5. How do the proposed options build trust between individuals and intermediaries, as opposed to trust between controllers, intermediaries and the market?
 6. What assessment has been made of the effect of clarifying delegated portability rights on the largest platforms, who would also be able to rely on that clarification?
 7. What assessment has been made of the adequacy implications of amending UK GDPR?
 8. Would the proposed framework recognise an intermediary constituted under the law of another jurisdiction — including the Crown Dependencies — acting on behalf of UK data subjects?
-

Next steps

- Responses are submitted online via the consultation response form: <https://www.smartsurvey.co.uk/t/SKTXDS/>
- The consultation closes at **11:59pm on 31 August 2026**.
- Open Data Manchester will prepare its own response, informed by this session.
- Participants who did not have the opportunity to raise a point are encouraged to send it on before the deadline.

Circulated with this readout: the slides presented at the session, and the full text of the consultation.