Department for
Science, Innovation
& Technology

Empowering people through data intermediaries

Consultation

CP 1592

Government of the United Kingdom

Department for Science, Innovation and Technology

Empowering people through data intermediaries

Consultation

Presented to Parliament by the Minister of State for Digital Government and Data by Command of His Majesty

June 2026

CP 1592

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at dataintermediaries@dsit.gov.uk.

ISBN 978-1-5286-6567-4

E03616462 06/26

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Introduction

People generate large volumes of personal data through everyday activities, yet they currently derive limited benefit from it. Instead, this data is held by data controllers, creating a clear power imbalance between individuals and those organisations that collect and control their data.

Data intermediaries offer a way to rebalance this relationship. They offer the potential to empower individuals to take control of their own data, operating as third parties to enable those individuals to better access, share and manage their personal data. The types of data intermediary are varied, but they generally allow users to either regain control of who can access their data, or to share their data on their own terms. By revolutionising where and by whom data is held, intermediaries can unlock new, unrealised benefits from people's data, ranging from innovative personalised AI services to groundbreaking new research enabled fully by the user's informed consent.

Although personal data is constantly produced, its value is still overwhelmingly captured by traditional data controllers rather than by the individuals who generate it. While people have rights as data subjects to access their data, these rights are often under-utilised. Our call for evidence last year found that people's awareness of what they can do with their data through third parties is limited.

There is a huge opportunity for the UK to use data more strategically, to unlock stronger competition across markets, helping to stimulate innovation and deliver sustained economic growth. The government recognises that intermediaries can play a vital role in unlocking competitive data-driven markets and supporting innovation, productivity and growth, and is committed to creating the conditions for the easy and secure sharing and reuse of high-quality data that intermediaries enable. This is a nascent and rapidly developing area of activity in the UK and globally, offering significant potential to enhance outcomes for people, businesses and the wider economy.

Responses to our call for evidence last year indicated there are three things that need to be achieved for intermediaries to be able to function better in the UK: legal ambiguities need to be addressed; data controllers must be confident providing people's data to another party; and user awareness of intermediaries and their potential value needs to grow. Currently, the barriers around these three areas are limiting the uptake and growth of the sector. Responses suggest these barriers appear interrelated and mutually reinforcing, leading to a sector with potential that is yet to be fully realised.

If the barriers to the sector are addressed, the potential is huge. What if, instead of a data controller typically deciding how your data is used, you were able to exercise greater control over your data and confidently determine who has access to it? Or if you could donate it to research projects to enable new discoveries? Or if it were powering personalised, innovative new AI services that could securely combine your data from multiple sources to provide you with new insights or suggestions? Data intermediaries are essential to unlocking this vision.

We are therefore launching this consultation into potential measures that could be taken to drive growth in the intermediaries market within the UK, giving individuals true power to control their data while ensuring that safety, trust and consent are all baked into the process. Any

action we take will be with the ambition of improving data access and portability, supporting economic growth through the use of this data and the development of innovative new services. After the consultation has closed, the government will carefully consider responses and take them into account when finalising proposals.

Part 1: Data portability and data intermediaries in the UK

Rights as a Data Subject in the UK

The UK General Data Protection Regulation (UK GDPR) gives individuals (data subjects) a set of rights regarding their personal data. These rights include the right to be informed about how and why their data is collected or used; the right of access to obtain a copy of their personal data; the right to rectification of inaccurate or incomplete data; and, in certain circumstances, the right to erasure.

Individuals may exercise their UK GDPR data subject rights themselves or may choose to delegate them to someone else acting on their behalf, such as a parent or guardian, a legal representative, or another third party. Delegation can help ensure that data subject rights are exercised effectively by someone better equipped to act.

Rules on the delegation of data subject rights are clearly defined for certain rights. Chapter VIII UK GDPR rights, such as the right to lodge a complaint with the Information Commissioner, the right to an effective judicial remedy, and the right to compensation, have explicit permission for delegation provided. However, there is not the same clarity for all rights. Some data subject rights under Chapter III of the UK GDPR, particularly the right to data portability, are often interpreted not to be delegable because explicit permission to do so is not stated.

This lack of explicit permission for third-party delegation for some rights, contrasted with clear permission for others, creates uncertainty for third parties such as data intermediaries. Data controllers cite this ambiguity as a reason for rejecting requests submitted by intermediaries to access data on behalf of individuals.

Table 1: Data subject rights with and without explicit delegation provisions

Chapter III Rights: These rights do not have explicit permission to be delegated	**Other Rights: These rights have explicit permission to be delegated**
the right of access; right to be informed about how why data is collected and used; right to have data rectified, erased, or restricted; right to object; rights related to automated decision making, including profiling; the right to portability.	the right to lodge a complaint with the data controller; the right to lodge a complaint with the Information Commissioner; right to an effective judicial remedy against the Information Commissioner; right to an effective judicial remedy against a controller or processor; right to compensation.

Data Portability

While each of the UK GDPR data subject rights play an important role in empowering individuals, the one with the greatest potential to unlock new business opportunities and drive growth is the right to data portability as this enables the safe and structured movement of data from one organisation to another.

The right to data portability allows individuals to move, copy, or transfer their personal data in a usable, safe, and secure way. It strengthens individuals' control over their information and enables them to reuse their data for their own benefit or to support wider societal benefits, should they choose to do so. It plays a vital role and underpins the operation of many types of data intermediaries and related initiatives such as Smart Data schemes. Open Banking sets the precedent for these schemes and has been the driver for several innovative services and enhanced competition in the banking sector.

Data portability is essential for unlocking data currently held by data controllers, enabling it to be reused, for example, by allowing individuals to switch their data from one service provider to another. This capability could help stimulate innovation and the development of new services, including AI-optimised solutions that create opportunities for growth. However, a study carried out by the University of St Andrews on the implementation of the UK GDPR right to data portability found that not all data controllers were providing data in formats compliant with UK GDPR requirements[1]. It also revealed confusion among controllers about the distinctions between various data subject rights, such as the right to access, erasure and to restrict processing.

Our call for evidence last year found that data controllers often create friction when responding to portability requests submitted through intermediaries, delaying or limiting individuals' ability to access or transfer their data. Respondents also highlighted that legal and regulatory ambiguity around portability, combined with incentives that favour retaining data rather than facilitating its movement, enables and in some cases encourages controllers to maintain these barriers.

The EU's Digital Markets Act (DMA) takes the right to data portability a step further by requiring designated gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, Booking.com) to offer individuals free, continuous, real-time access to the data they generate through core platform services. This obligation has prompted the development of tools such as data-portability APIs (Application Programming Interface) that streamline the process of exporting user data. While these have been made for compliance with the EU's legislation, some of the APIs have been made available in the UK. However, there is currently no obligation for the providers to continue to do so.

A recent assessment by the Competition and Markets Authority (CMA) found that introducing a mandatory Google Search API in the UK would enable several benefits, including allowing more users to monetise their data, generating meaningful time savings, and reducing costs[2]. In

[1] University of St Andrews, School of Computer Science (2018) How portable is portable? Exercising the GDPR's right to data portability. https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/15946/claw2018.pdf?sequence=1&isAllowed=y

[2] Competition and Markets Authority (2026) Data portability conduct requirement. https://assets.publishing.service.gov.uk/media/6979d0915da1fd4ddea98c73/_Data_portability_conduct_requirement_v2.pdf

monetary terms, the intervention could generate in the order of £1 million per year in user benefits if an additional 50,000–100,000 people engage with the API, reflecting the lower end of expected user growth and illustrating the scale of value that even modest increases in uptake could deliver. However, while the potential is great, significant challenges persist around the UK right to data portability, particularly the absence of clear guidance on data formats and transfer mechanisms. As a result, much of the data about people remains siloed, hindering its reuse and preventing the full benefits of the portability right from being realised.

Exercising data subject rights - are data intermediaries the answer?

The term “data intermediaries” is used across a range of settings and does not have a single, universally applied definition. It can refer broadly to any entity that facilitates the flow, exchange, or coordination of data between parties. This expansive interpretation may at times encompass organisations such as data brokers or data aggregators.

In our call for evidence last year, we introduced a proposed taxonomy of data intermediaries (see Table 2 below), encompassing a broad range of organisations that facilitate access to or sharing of personal and non-personal data for example, data trusts, personal data stores, and commercial data exchanges, but excluding brokerage or aggregator services. A separate call for evidence was carried out on data brokers, and we continue to consider these distinct from intermediaries.

Under the EU Data Governance Act (DGA), data intermediation service providers offer services in both business to business and business to consumer contexts, acting as neutral parties that enable data sharing between individuals, organisations, and data users. The UK Government’s Industrial Strategy commits to supporting the development of content and data marketplaces and exchanges to enable the creation of value from business assets and drive innovation. This aligns with our taxonomy’s definition of non-personal data intermediaries (including commercial data exchange and industrial data platforms).

We have therefore chosen to focus this consultation on personal data intermediaries that support individuals in exercising their right to data portability by acting on their behalf and with their explicit permission. These services can strengthen individual empowerment by enabling consumers to take greater control of their data. We will ensure consistency and coherency with the parallel work on the development of Smart Data schemes, including in the digital markets sector, to balance robust consumer protections with the development of new and innovative services. Complementary work is also underway to develop and invest in data sharing infrastructure in the economy. This activity will support businesses to improve the maturity of their data practices, better preparing and enabling them to interact and use data intermediaries.

Our call for evidence highlighted a common set of blockers impacting how effectively intermediaries can operate in the UK. While the specific challenges differ by intermediary type, a common theme across the evidence was uncertainty stemming from the UK GDPR,

particularly regarding whether, and how, data subject rights can be delegated and exercised through third parties.

Table 2: Proposed taxonomy published in call for evidence

Type	Description	Examples
Data Wallets	Enable individuals to gather, securely store and manage their personal data in one place, controlling access to their data on a case-by-case basis.	MEECO - MEECO wallets securely store digital assets like identity documents, financial information, tokens (such as NFTs), and loyalty points.
Personal Information Management Systems (PIMS)	Use combinations of data that has already been shared to add new value, extract insights or provide specific services, based on goals set by the user.	Smarter Contracts - allows ad-hoc granting or revocation of permissions by a data subject, permitting decentralisation and highly transparent compliance with data protection law. Allows the delegation of data subject rights in real time with quite granular controls and assists in enforcing two-sided contracts.
Data Unions	Pool together and processes personal data donated voluntarily by users. Access to the aggregated dataset is sold to third parties and shares of the resulting revenue are distributed between the data donors.	Swash - collects data from its members as they browse the web. This data is pooled and sold to buyers, with the revenue shared among the members. This allows individuals to monetise their data while maintaining control over their privacy.
Data Cooperatives	Pool together and processes personal data donated voluntarily by users. Third parties are granted access to the aggregated data to generate insights that benefit members or to further a common aspiration, not for monetary gain.	Rodeo App - facilitates earnings aggregation and insights for delivery couriers and private hire drivers offering services through app-based platforms. Use cases focus on planning income for gig workers and recommending locations and times for job opportunities. Rodeo pools their user base of gig workers to provide a delivery service for businesses and charge a commission. Databonds - a UK company that lets people use their shopping data to get new insights into their habits and

		contribute to research while providing them with rewards for doing so.
Data Trusts	Collect, store and aggregate personal data, determining how to process the data through the management of the individual's data rights on their behalf in order to pursue their aspirations and create benefits for them within a fiduciary responsibility.	Brixham Data Trust – intends to manage the data rights of residents of Brixham in relation to local data, and collects, pools, and negotiates data on a range of civic and communal use cases. Current use cases relate to service provision, environmental monitoring, energy use, with a view to collective activation of rights and collective decision-making over place data. Worker Info Exchange - submits data subject access requests on behalf of gig-economy workers to allow better transparency and so workers can challenge unfair practices or automated decisions. Roberta Data Trust - being developed by the University of Southampton, empowers individuals and communities to donate personal health data and share experiences with pregnancy loss for research and policy change in a safe and transparent way.
Trusted Research Environments	Provide approved parties with secure, restricted access to analyse anonymised and protected personal data donated by data subjects. Approved parties can extract results of their processing but not the data itself.	NHS England Secure Data Environment (SDE) - provides approved researchers with secure access to de-identified (pseudonymised) and minimised patient data. Researchers log in to a desktop environment and use tools to analyse data.

The potential for AI and data intermediaries

Artificial intelligence (AI) has the potential to significantly amplify the value of data intermediaries by enabling more personalised and user-centred uses of personal data. With an individual's permission, AI-powered intermediaries could securely combine data from multiple sources to deliver innovative services and wider societal benefits. For example, intermediaries could support trusted data donation for research through secure environments or enable

personalised AI services that draw on an individual's data across sectors to provide tailored recommendations, predictions or support.

AI could also enhance how intermediaries help individuals manage and exercise their data rights. A personal data store, for instance, could allow an individual to hold their personal data in one place, with AI-enabled services managing access for processing in line with the user's specified consent and agreed terms and conditions. When acting on behalf of individuals, intermediaries could use AI tools to facilitate data portability requests, manage ongoing consent preferences, and translate complex datasets into meaningful insights. This could help lower practical barriers by reducing time costs, streamlining interactions, and making data rights easier to exercise for individuals. As these technologies develop, data intermediaries could be enabled to act more autonomously on an individual's behalf through Agentic AI, managing permissions and data access within agreed boundaries.

Example: Emerge Data (emergedata.ai)

Emerge Data is a London-based data and AI company focused on enabling more personalised digital experiences. It does this by allowing users to securely connect and share data from their existing accounts (e.g. Google, Amazon, TikTok, and Meta). Access to this rich, permissioned data enables Emerge Data to generate higher-quality insights, which in turn powers more relevant and context-aware AI experiences, rather than the generic outputs typical of many AI chatbots or analytical tools.

User control is central to Emerge Data's approach. Data wallets are used to allow individuals to store their data and manage access permissions, which can be switched on or off as preferences change. Users always remain fully in control: explicit consent is required to access linked accounts, and individuals decide exactly what data they choose to share.

Blockers to data intermediaries in the UK

Responses to the call for evidence last year made it clear that the UK has a strong foundation on which to build a thriving data intermediaries sector. Businesses, civil society organisations and emerging service providers all recognised the substantial potential of intermediaries to unlock new value from personal data. A better-functioning market could deliver benefits for consumers, stimulate competition, and support the development of innovative products and services.

However, stakeholders consistently highlighted that this potential is not yet being realised. Three interlinked barriers were raised repeatedly. Firstly, legal ambiguity - particularly around whether and how Chapter III data subject rights in UK GDPR (including the right to data portability) can be delegated to a third party - creates uncertainty for both intermediaries and data controllers. Secondly, many data controllers are either reluctant or unsure how to respond to delegated requests from third parties, often citing risk, unclear obligations, or lack of standardised processes for doing so. This introduces delays into the process and can create friction when intermediaries try to operate as intended. Finally, low public awareness and limited understanding of intermediaries mean that individuals are not yet making full use of the services that could help them exercise greater control over their data.

These barriers reinforce one another: uncertainty reduces controller confidence; controller friction reduces user trust and uptake; and low uptake hinders the growth and maturity of the sector. As a result, many intermediaries struggle to operate effectively, despite strong interest in the value they could provide. Respondents emphasised that without clarity, greater trust, and more consistent practices around data sharing, the market will continue to develop slowly. Addressing these barriers will be essential for enabling the sector to scale and for individuals to fully realise the value of their data.

The risks with data intermediaries

The exercise of data subject rights through third parties introduces a number of potential risks that need to be carefully managed. Given the significant responsibility involved in exercising rights on an individual's behalf, stakeholders and respondents to the call for evidence last year emphasised that trust between data subjects and data intermediaries is essential. Without strong safeguards, there is a risk that individuals may lose confidence in intermediary services if consent mechanisms are unclear, preferences are not accurately reflected, or there is a lack of clarity over responsibility. Trust will be essential for a successful intermediaries ecosystem to flourish, with clear rules and expectations for how intermediaries should handle people's data. As the call for evidence highlighted last year, it is also important that data intermediaries are designed with accessibility, transparency and inclusivity at their core to prevent risks of coercive delegation of rights and power imbalances. Part 2 below discusses a range of approaches taken elsewhere that could be applied to intermediaries in the UK to help users to find trusted providers.

As intermediaries become more widely used, there is a risk they could attract malicious activity, including cyber-attacks, and attempts to impersonate legitimate services or gain unauthorised access to personal data. Especially as large volumes of personal data are brought together within a single system, the impact of any security breach could be greater, affecting many individuals at once. At the same time, data controllers may face additional challenges in verifying that third-party requests are genuinely authorised by the individual, particularly where consent has been delegated, updated over time, or exercised through automated tools. As data-intensive intermediary activity grows, effective oversight will be important to ensure security and prevent misuse of authority.

Increased use of data intermediaries may also create operational and market-level risks that need to be considered. Higher volumes of data portability requests could increase costs and technical demands for data controllers, particularly smaller organisations that may need to invest in new systems, processes or infrastructure to respond effectively. There also is a risk of market concentration, where a small number of intermediaries gain significant influence, potentially reducing competition, limiting user choice, and shaping how data rights are exercised in practice. In addition, misaligned incentives between data controllers and intermediaries could undermine the effective exercise of data rights, particularly where commercial interests discourage timely or meaningful data sharing.

Measures introduced should therefore seek to manage these risks in a proportionate way, supporting the effective operation of the intermediaries market and ensuring the safe use of people's data while avoiding additional burdens or unintended impacts for individuals, intermediaries, or data controllers.

Part 2: What has been done elsewhere that could increase awareness of data portability and trust in data intermediaries?

As discussed in Part 1, the right to data portability offers great potential both for growth opportunities and for personal management and control of data. Intermediaries offer a promising way of managing this right as third parties. Internationally, different governments and sectors have adopted a variety of approaches to establish trust in services that handle or transfer data on behalf of individuals or organisations. These approaches differ in how they authenticate, authorise, or oversee third-party services, reflecting local policy priorities, regulatory structures, and the maturity of digital markets. Across these models, the common objective is to give users confidence that intermediary services are trustworthy, secure, and operating within a clear set of rules.

The EU approach: a register of intermediary services

The EU introduced rules covering data intermediaries through the Data Governance Act in 2022. There have been recent proposals to reform this legislation, which are detailed below, but the current rules regulate data intermediary services by subjecting them to a 'notification procedure' and setting the conditions of providing intermediary services. Before providing an intermediation service, an organisation must notify a relevant competent authority (regulator). They may also request that the competent authority confirms their compliance with the conditions under which a service in the EU must act, which if done, allows them to display a common logo to show that they are a recognised provider.

Having an official, union-level register for intermediaries would likely help alleviate the issue that we have heard reported in the UK of data controllers being unsure as to whether a given intermediary service is genuine or trustworthy. Furthermore, the register provides assurances to individuals that their data will be handled responsibly should they provide it to the third party, which could in turn help increase uptake of these services. The rules work on the basis that Chapter III data subject rights in the EU GDPR may be exercised by third parties and therefore operate without any additional clarity being provided in the data protection legislation compared to the UK version.

In November 2025, the EU announced the Digital Omnibus Regulation Proposal, a consolidation of existing digital legislation designed to assist businesses, public administrations, and citizens. The proposal aims to stimulate competition while ensuring compliance with rules at a lower cost. It includes amendments and the repeal of several regulations related to data, bringing them together into a single, unified framework that will sit within the Data Act.

The proposed system will replace the mandatory registration regime for intermediaries with a voluntary one. It is argued that this new system will benefit data intermediary organisations by delivering cost savings through the removal of the mandatory requirement to register with the

competent authority and eliminating the need to provide intermediary services via a separate legal entity to other parts of a business, avoiding one-off and ongoing overhead costs[3]. It will also reduce market entry barriers for new players, fostering innovation and accelerating industry growth. By streamlining definitions, the system harmonises data rules, making them easier to understand and apply. For data altruism organisations, the removal of the rulebook lowers compliance costs, while member states benefit from scrapping national policy reporting obligations, reducing administrative and reporting expenses[4].

The Australian Consumer Data Right

The Consumer Data Right is an economy-wide reform in Australia that allows individuals to share data with accredited providers via an opt-in service. Accreditation by the Australian Competition and Consumer Commission (ACCC) ensures that a provider meets strict criteria around security and privacy. The model has so far been implemented for the banking and energy sectors, with more due to follow. It is described as giving people more control over their data and enabling access and sharing with accredited third parties.

Once the individual gives permission to the provider to access their personal (or business) data, their identity is verified and they are then asked to confirm which data from the existing provider that they would like to share. This consent can be withdrawn at any time. Data is shared between the providers in machine-readable format (set by the Data Standards Body), after which the individual can start using the new service.

Unlike the EU's approach that covers intermediation services that are often facilitating business sharing of data, the Australian approach focuses instead on people's personal data, portability, and being able to provide consumers with new services and better deals.

The South Korean 'MyData' scheme

South Korea's MyData scheme allows data subjects to exercise their rights to portability, by requesting the transfer of their personal data either to themselves or to third parties. Initial rollout has been sectoral with healthcare and communications prioritised, with others to follow. Example use cases for the scheme include the ability for a patient to have their diagnosis data transferred from a hospital to a MyData service provider to provide tailored health management, or for a customer to have their phone usage and bill data transferred from their

[3] European Commission (2025) Digital Omnibus Regulation Proposal. Available at: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

[4] Data altruism organisations are entities that facilitate the voluntary, non-remunerated sharing of data by individuals and businesses for purposes that serve the public good. When shared responsibly, this data can unlock significant value for research and innovation, contributing to advancements in areas such as public health, the environment, transport, and more. European Commission (2026) Data Governance Act explained. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

operator to a provider that can analyse their usage patterns and provide an optimal, tailored plan for that user to save money.

The California Consumer Privacy Act (CCPA)

California's state privacy law allows consumers to use authorised agents to submit data requests on their behalf, for example to access or move data. The business receiving the request may ask for proof from the agent that the consumer approved the request, and to prevent fraud can also ask the consumer direction to verify their identity and confirm that they provided permission to the agent to submit the request. The CCPA does not accredit the 'agents', with any person or company allowed to act as one if authorised by the consumer.

Alternative approaches

Office for Digital Identities and Attributes register of certified service providers

While it is not used in the context of data intermediaries, the 'conformity assessment' approach for certifying digital identity services in the Data (Use and Access) Act 2025 ("DUA Act 2025") and used by the Office for Digital identities and Attributes (OfDIA) provides another useful example of how to help people know which services are trustworthy.

Unlike the EU's registration approach for intermediaries outlined above, the OfDIA process relies on third-party conformity assessments. Service providers must be judged by an independent third party (a Conformity Assessment Body) to comply with the relevant rules. A standardised certification scheme defines what the Conformity Assessment Bodies must do in order to evaluate a service, ensuring a consistent baseline for how they are evaluated, with requirements for them to be evaluated at least annually to ensure continued compliance. The UK Accreditation Service is used to accredit each Conformity Assessment Body, to ensure the certification scheme is being implemented correctly. Certified organisations are included on a public statutory register so that people can find registered services easily and feel confident about the service they will provide.

As with the EU example described above, this provides an example of a recently introduced scheme using registers of certified providers to promote trust in services that are complying with expected requirements. The question of whether certification should be carried out by accredited third parties, or by a regulator or other body is an important consideration for the design of any potential registration system for data intermediaries in the UK.

Smart Data scheme in digital markets

While Smart Data schemes are not designed specifically to regulate data intermediaries, they provide a useful example of how trust, clarity and interoperability can be established in data-sharing ecosystems. The DUA Act 2025 introduces new regulatory powers enabling the government to establish Smart Data schemes across various sectors of the economy. A notable application is in digital markets, where such a scheme could foster economic growth by empowering consumers and businesses to use their data more effectively and encouraging the development of innovative products and services.

We could use these Smart Data provisions to set the expectations for how intermediaries offering data portability in digital markets would function. This approach could deliver faster improvements in technical data portability, alongside clearer assurances for individuals about how their data is accessed and used.

However, Smart Data schemes will be introduced via sector specific regulations, and will not necessarily cover the entire economy, leaving untapped potential for Data intermediaries. While they may complement a wider intermediaries framework by improving how data portability operates in particular sectors, they would not address broader legal uncertainty under UK GDPR or apply consistently across the economy. As a result, Smart Data schemes on their own may not resolve the challenges faced by the full range of intermediary models or support sustained growth of the intermediaries market.

Part 3: Options to remove barriers for data intermediaries

Returning to the barriers facing intermediaries in the UK, which largely stem from or are intensified due to legal uncertainty around UK GDPR, the question of how this legal uncertainty should be addressed arises. Addressing this uncertainty comprehensively is likely to require legislation to clearly set out the law, although other measures are described below which could sufficiently indicate our intent for this sector. As set out above, the EU's approach to regulating data intermediaries works on the basis that third parties can exercise a data subject's Chapter III rights, which is the area of uncertainty businesses face in the UK.

We are interested in views on whether without addressing these issues explicitly, a register or similar strategy as taken by the EU approach risks becoming an additional layer rather than a solution and may not deliver the clarity or confidence needed for the wider ecosystem to function effectively.

The call for evidence indicated there are three things that need to be achieved for intermediaries to be able to function better in the UK:

- Address legal ambiguities,
- Remove data controller friction, and
- Improve user awareness of intermediaries.

For any intervention in the intermediaries sector in the UK to work, we believe two key objectives should be targeted:

- Provide a clear framework for data intermediaries to exercise UK GDPR data subject rights to address reported ambiguities in the legislation.
- Improve trust between individuals and intermediaries as well as between data controllers and intermediaries.

To meet these objectives, the government has considered the principles below in assessing the options set out in this consultation.

- **Proportionate and evidence-based**
  Interventions should be targeted at evidenced problems; particularly legal ambiguity, controller uncertainty, and low trust and awareness. Measures should be proportionate to the risks involved and avoid unnecessary burdens, particularly for smaller or early-stage intermediaries. The emphasis should be on removing existing frictions rather than adding new layers of compliance.
- **Trust-enhancing and rights-protective**
  Options should aim to build confidence across the data ecosystem. Individuals should feel assured that their data is handled in line with their rights and choices, and that consent works as intended in practice. Intermediaries should operate in a secure and responsible way, with clear expectations around how they act on someone's behalf. At

the same time, data controllers should have the clarity they need to recognise legitimate delegated requests and respond to them with confidence.

- **Clear and practical in operation**
  Measures should be straightforward to understand and apply, with clear expectations on how delegated rights are exercised, how data is shared, and how issues are resolved. Approaches that are difficult to operationalise in practice are unlikely to achieve the intended outcomes.

- **Growth-enabling and innovation-friendly**
  The framework should support innovation and the scaling of intermediary services that deliver benefits for people and the economy. Interventions should avoid entrenching incumbents or stifling new entrants, balancing assurance and oversight with flexibility in a fast-evolving market.

Government has a range of levers available to introduce or influence changes that could help address the challenges currently faced by data intermediaries. Any changes should help to achieve the outcomes of empowering people with greater control over their data, while also helping to drive growth and encourage innovation. The levers available span both legislative and non-legislative approaches, each presenting distinct advantages and drawbacks. For example, while some options may be faster to implement, others may minimise burdens on intermediaries. More direct interventions may offer greater potential to address underlying issues effectively. Importantly, no single measure is likely to address all barriers in isolation. We are therefore seeking views on whether the options set out below are best understood as complementary, and on how they might operate individually or together to meet the objectives of this consultation. The proposed options below reflect the government's ambition to create the conditions for a trusted and dynamic data intermediaries market.

Legislative options

Option 1: Amend UK GDPR directly to provide legal clarity

This option would involve making changes to UK GDPR directly to remove the legal uncertainty around delegation of data subject rights that was reported in the call for evidence. This would include clear provisions on data subjects being able to delegate their Chapter III rights to a third party, and third parties being able to exercise these.

This approach directly and comprehensively addresses legal uncertainty and ensures that the relevant provisions are all found together in UK legislation (within UK GDPR). However, it would be unlikely on its own to significantly improve trust in data intermediaries, meaning additional supporting measures would likely be required.

In terms of the principles that we are considering options against, this option is strongest on proportionality and clarity, as it directly addresses legal uncertainty identified through the call for evidence. It does not fully address trust in practice but is better on growth and innovation because it removes barriers without adding new regulatory requirements.

Option 2: Regulate the data intermediaries sector

Option 2a: Ensuring coherence with international frameworks such as the EU Data Governance Act

As outlined in Part 2, the EU approach to data intermediaries has been to regulate data intermediary services by subjecting them to a notification procedure and to conditions of providing such a service. The Data Governance Act establishes a framework to build trust in data sharing, enhance data availability, and address technical challenges in data reuse. The framework introduces measures to help ensure that data intermediaries will function as trustworthy organisers of data sharing.

Although the UK GDPR can be interpreted as already allowing intermediaries to exercise Chapter III rights on behalf of individuals, the call for evidence highlighted significant uncertainty about this in practice. Introducing explicit provisions clarifying the role of intermediaries would therefore help to resolve this ambiguity and provide greater legal clarity indirectly.

The notification process (general authorisation), register and certification mark would help improve trust and provide confidence in intermediaries for data controllers and users alike as they would have assurances that the intermediary is operating as expected, and if not, the regulator (for example The Information Commissioner's Office (ICO)), would have powers to take action.

Adopting an approach similar to the EU framework would help ensure coherence with international approaches, recognising the importance of international data flows and the need to enable UK-based data intermediaries to scale across borders. This could also potentially create scope for mutual recognition between UK and EU frameworks, reducing friction for data intermediaries operating across both jurisdictions. However, the presentation of this option as “regulating intermediaries,” rather than simply “clarifying UK GDPR,” risks being perceived by the very companies we want to support as adding new regulatory burdens. Placing obligations on the intermediaries also does not address the question of how data controllers should respond to requests – such as the data format or regularity at which data is sent. While these are not included in the EU’s approach, we would need to consider whether any rules are required to govern how data controllers handle third party requests, too.

This assessment also does not account for the EU Digital Omnibus proposal, which, if implemented, could reshape the EU framework by shifting the regime to a voluntary model, thereby changing what “alignment with the EU” would entail.

This option is strong on trust and recognition, providing a clear signal of legitimacy for intermediaries. It is less strong on proportionality and practicality and may have mixed effects on growth due to added regulatory processes.

Option 2b: Regulation through an alternative UK Authorisation Framework

An authorisation scheme ranging from a light-touch notification process to a full licensing regime would formally recognise data intermediaries that meet defined standards set by government and the ICO. Such a scheme could help data controllers and individuals distinguish between trusted and untrusted intermediaries, thereby reducing friction and increasing confidence in delegated data subject rights. The degree of regulatory oversight, legal certainty, and market impact would vary significantly depending on the model selected.

An authorisation framework could be designed at different levels of intensity. At the lighter-touch end, a general authorisation or notification model would allow intermediaries to operate without prior approval, provided they meet published conditions and are visible on a register. More interventionist approaches could require intermediaries to apply for approval or operate under a licensing regime, offering greater assurance and oversight but increasing regulatory demands. Licensing could be paired with amendments to UK GDPR to deliver maximum legal clarity around delegated rights, but it would also represent the highest regulatory burden, likely to be slow, costly, and potentially distortive in a developing market, making it more stringent than EU approaches.

Alongside this the authorisation framework could also introduce clearer expectations on how data controllers should respond to delegated requests. For example, controllers could be required to accept and process requests submitted by authorised intermediaries in accordance with defined standards, reducing scope for ad hoc refusal or delay. This approach would shift the framework from focusing solely on intermediary conduct to also addressing controller behaviour, which respondents to the call for evidence identified as a major barrier to effective data portability.

This option provides strong assurance and clarity, supporting confidence in both how intermediaries operate and how data controllers are expected to respond to delegated requests. By linking intermediary authorisation to clearer expectations on controller behaviour, it may be better placed to address the practical sources of friction identified in the evidence. However, it goes beyond what the current evidence suggests may be required and is less well suited to a developing market, as higher compliance requirements could limit flexibility and slow entry by new providers. While an authorisation scheme could directly strengthen trust and set clear expectations for intermediary and controller behaviour, the trade-off lies in imposing additional barriers to entry and operational constraints on a nascent sector. The policy choice therefore depends on whether greater assurance and trust justify potentially limiting innovation or increasing compliance obligations.

Alternative legislative paths

Option 3: Mandate portability through Portability APIs

Mandating data portability through Portability APIs offers a targeted way to reduce data controller friction and ensure that individuals can transfer their data efficiently via intermediaries. This approach has been adopted in the EU for a small number of firms under the DMA, which requires designated “gatekeeper” firms to provide data portability APIs for end-users and authorised third parties. These APIs have been developed in response to EU requirements and in some cases, gatekeepers have chosen to make them available to UK users on a voluntary basis. This has been a welcomed development for UK intermediaries and users, however as access is voluntary, it can be withdrawn at any time, limiting certainty for users. Imposing new obligations on gatekeeper firms that are already taking voluntary action may have unintended consequences for the UK’s wider business environment and investment climate.

Under this approach in the UK, firms designated with Strategic Market Status (SMS) under the Digital Markets, Competition and Consumers (DMCC) Act 2024 which is enforced by the Competition and Markets Authority (CMA), acting independently of government, could be

required to provide standardised, machine-readable data access pathways to authorised third parties to foster competition. This would guarantee that data is made available in a consistent and interoperable format, helping intermediaries operate more effectively and reducing delays or friction introduced by data controllers. However, because SMS designation similarly to EU gatekeeper designation applies only to a small number of the most powerful digital firms, only in respect of specific activities, and for a fixed time period (designations are limited to five years unless status is revoked), the scope of this intervention would be inherently limited and difficult to extend across the wider economy.

This option is effective at addressing specific sources of friction, particularly in operational terms, however it would only be applicable to a limited group of designated firms within a set time frame. It does not fully address wider trust or delegation issues without being done in combination with another option, and its impact on growth is limited by scope.

Non-Legislative options

Option 4: Non-statutory authorisation scheme

A non-statutory authorisation scheme could be established to help data intermediaries demonstrate that they meet baseline standards for security, oversight, and responsible handling of personal data. Such a scheme could be run by industry, with intermediaries collectively developing and operating a voluntary approval or certification process. Authorised intermediaries could be listed on a public register or permitted to display a recognised trust mark, providing a visible signal to individuals and data controllers that they meet agreed standards.

This approach could help improve user awareness and trust by making it easier for individuals to identify reputable intermediary services. It may also help reduce some data controller friction by offering a common reference point for assessing whether an intermediary is legitimate. A non-statutory scheme would be relatively light-touch, quick to establish, and flexible, allowing standards to evolve alongside the market without introducing new regulatory burdens. As such, it could support innovation and act as an initial trust-building measure in a nascent sector.

However, as a voluntary, non-statutory approach, the scheme would not resolve legal uncertainty around delegated UK GDPR rights or oblige data controllers to accept requests from authorised intermediaries, and its impact would depend on industry uptake and governance. As a result, such a scheme may be most effective as a complementary or transitional measure, potentially informing the design of a future statutory framework if stronger assurances are needed over time.

This option is well aligned with proportionality and practicality, offering a light-touch way to support confidence in the market. It goes some way toward building trust, while remaining supportive of innovation and new entrants.

Option 5: Intermediaries Code of Practice

An ICO Code of Practice would set out clear expectations for organisations carrying out intermediary functions, strengthening trust by signalling that intermediaries are expected to follow high standards. The Data Protection Act 2018 Part 5 allows for statutory codes of

practice to set out guidance that can be taken into account by courts or tribunals. This option helps individuals understand how intermediaries should behave and what safeguards apply. It can also address controller friction indirectly, by providing guidance on how controllers should respond to delegated requests.

However, while an ICO Code of Practice would carry statutory weight and be considered by the ICO and by courts and tribunals, it would not create new direct legal obligations on data controllers or intermediaries. Its effectiveness would therefore depend largely on adherence in practice. Even where intermediaries follow the code, data controllers may still have limited incentives to remove friction such as delays or questioning the validity of third-party requests. This approach places an additional burden on intermediaries to demonstrate adherence without offering reciprocal obligations for controllers. Overall, this approach is light touch and helpful for building trust in intermediaries but limited in its ability to resolve structural barriers or guarantee practical cooperation from data controllers.

This option supports clarity and consistency, particularly in setting expectations for behaviour. It remains low-burden and compatible with innovation but does not on its own resolve uncertainty or change behaviour where incentives are misaligned.

Option 6: Industry led Code of Practice

An industry-led code of practice shares some benefits with an ICO issued code but is even lighter-touch. Developed by intermediaries themselves, it can demonstrate a collective commitment to responsible practice that reassures users. It may demonstrate expectations of how intermediaries should act and could help develop trust that intermediaries will act responsibly. Because it is led by industry, it can be more agile, easier to update, and avoid regulatory overreach, qualities that support innovation in a growing sector.

However, because it's entirely voluntary and non-binding, it would have limited effects on addressing underlying legal uncertainty. Moreover, data controllers may simply ignore a voluntary code, and it provides no authoritative signal comparable to a statutory code of practice. Furthermore, without an external regulator's oversight, the code may struggle to maintain credibility or consistent quality across the sector.

This option is well suited to flexibility and innovation, given its voluntary nature. It does not provide a strong trust signal on its own, as uptake and credibility would vary across the market.

Option 7: New ICO Guidance for Data Intermediaries

New ICO guidance would build on existing material to provide clearer direction on how data intermediaries may exercise data subject rights and how data controllers should respond to such requests. It could help intermediaries feel empowered to exercise data subject rights by showing it is legally permissible and setting out what is expected from them and data controllers. This directly addresses legal ambiguity by clarifying how UK GDPR applies to intermediaries, and data controller friction by reducing uncertainty about how controllers should recognise and handle delegated requests. However, ICO guidance would not be legally binding and previous guidance by the ICO has not had the desired effect in shifting controller behaviour. Without enforcement mechanisms or accompanying regulatory incentives, guidance alone may fail to deter controllers who deliberately introduce friction, for example by requesting unnecessary verification or resisting third party involvement.

This option is better at addressing uncertainty quickly and proportionately, with clear benefits for day-to-day operation. It improves confidence while remaining supportive of market growth, but does not resolve trust issues on its own.

Conclusion and next steps

Data intermediaries offer a significant opportunity to empower individuals, unlock greater value from personal data, and support innovation and economic growth in the UK. As this consultation has set out, however, this potential is not yet being fully realised.

Evidence gathered through our call for evidence last year and explored in this consultation highlights the challenges facing the data intermediaries ecosystem in the UK. Legal ambiguity, particularly around whether and how UK GDPR Chapter III rights can be delegated to third parties, creates uncertainty for intermediaries and data controllers alike. This uncertainty contributes to friction when intermediaries seek to act on behalf of individuals, as data controllers are often unsure how to respond to delegated requests and may be concerned about compliance risks. At the same time, limited public awareness and understanding of data intermediaries reduces trust and uptake, slowing the growth and maturity of the sector. Together, these factors reinforce one another and constrain the development of services that could otherwise deliver meaningful benefits for individuals, businesses, and the wider economy.

This consultation has set out a range of potential approaches to addressing these challenges. These include legislative options to clarify the legal framework, regulatory or authorisation models to improve trust and recognition of intermediaries, and non-legislative measures including codes of practice and guidance. Each option presents different trade-offs in terms of scope, speed, regulatory burden and effectiveness.

We are therefore seeking views on how best to strike the right balance between providing legal clarity, reducing friction, and building trust, while supporting innovation in a developing market. We welcome evidence on whether legislative change is necessary to resolve uncertainty around delegated rights, the extent to which trust-building mechanisms such as registration or certification could support uptake, and the role that non-legislative measures could play either on their own or alongside more formal interventions. Responses to the consultation will inform our assessment of the most effective and proportionate way forward, to best support the growth of a trusted data intermediaries ecosystem in the UK. Government will provide an update in due course.

How to respond

We welcome the views of individuals or of organisations. We are particularly interested in the views of:

Data intermediaries - broadly defined

Academics, research institutes, think-tanks

Representative bodies

Consumer groups

Privacy groups

Relevant regulators

Data controllers

We also welcome views from individuals and organisations with experience of intermediary-enabled data sharing models in other national or supranational jurisdictions.

We ask that responses are submitted online.

This consultation is available from: www.gov.uk/government/organisations/department-for-science-innovation-and-technology

If you need a version of this document in a more accessible format, please email alt.formats@dsit.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.

Annex A: Main Questions

The aim of this survey is to understand how different options could help address the barriers to data intermediaries that were identified in the call for evidence last year. We are keen to receive views from data intermediaries themselves along with data controllers, academia, representative bodies, regulators, consumer and privacy groups.

Introductory Questions

- Respondent Type (Annex B: questions relevant to users of intermediaries)
- Respondent Name / Company Name
- Contact address
- What sector do you work in?
- What services does your company offer?
- Would you prefer responses to remain confidential?
- Would you prefer responses to not be attributed to you/your business?

Legislative Options

Amending UK GDPR

- To what extent do you agree or disagree with this statement: Providing legislative clarity alone in UK GDPR would be sufficient to address barriers faced by intermediaries?
    - Please explain you answer:
- If UK GDPR were amended to clarify the role of intermediaries, do you think any further details should be included alongside explicit delegation of data subject rights, for example, guidance, code of practice, specific data formats, frequency, or how portability should operate in practice?

Regulation

- What obligations on data controllers, if any, would be effective in supporting requests made via authorised data intermediaries?”
- How burdensome would an authorisation or registration requirement on intermediaries be for your organisation?
- What would be the advantages and/or disadvantages of the UK implementing a regime similar to that of the EU’s regime?
- To what extent could it help to build trust between intermediaries, controllers and individuals?

- How important do you view regulatory alignment with the EU for your operations, given potential changes arising from the Digital Omnibus proposal?
- To what extent would a voluntary registration process for intermediaries likely be sufficient, to ensure services comply with rules?
- For data controllers: would an EU-style model make you more likely to accept delegated requests from intermediaries on an official register?
    - Please explain your answer:
- If a certification scheme were adopted for data intermediaries in the UK, who would be best suited to carry out the certification process? For example: self-certification, regulator certification, government certification or third-party certification.
- To what extent do you agree or disagree with the following statement: an authorisation scheme (whether notification-based, registration, or licensing-based) would meaningfully reduce the uncertainty or friction you/your organisation currently face?
- For data controllers: How important is formal recognition of intermediaries (e.g., being listed, registered, or licensed) in giving you confidence as a data controller to accept delegated rights requests?
- Which of the following approaches would best strike the right balance between assurance and proportionality for your sector?
- To what extent would requiring the use of Portability APIs affect the level of friction your organisation experiences when responding to or submitting delegated data access requests?
- How would requiring mandatory APIs affect your organisation's compliance costs, especially relative to existing data portability obligations?
- Which of the following would need further standardisation to make mandatory APIs more workable?

Non-Legislative Options

- For data controllers: To what extent would a non-statutory authorisation scheme, potentially run by industry, increase your willingness in using or accepting requests from data intermediaries?
- What standards or criteria would be most important for an industry-run authorisation scheme to be effective?
- What oversight or accountability arrangements would be necessary to ensure an industry-run scheme remains trusted?
- What measures, if any, would be needed to ensure such a scheme does not disadvantage new or smaller entrants?

- For data controllers: Could a statutory code of practice increase your confidence in using or accepting requests from intermediaries?
- Would an industry-led code provide meaningful reassurance about the credibility of intermediaries?
- Do you believe voluntary, industry led approaches can meaningfully reduce data controller friction that was reported in our call for evidence last year?
- Would updated ICO guidance meaningfully change how your organisation handles delegated rights requests?
- What specific elements of guidance would be most useful to you?
- Would guidance alone be enough, or would you expect additional regulatory or legislative measures to address barriers facing the intermediaries market?

Data Portability Through Smart Data Schemes

- To what extent could a Smart Data scheme provide sufficient trust for intermediaries operating in your sector?
- What measures would be needed to ensure Smart Data schemes adequately support intermediaries, or vice versa?
- How do you see a Smart Data scheme in digital markets interacting with data intermediaries?
- What would each of their respective roles be in supporting effective data portability?

Final Questions

- Are you aware of good international examples where action has been taken to improve the operation of data intermediaries?
    - If yes, please provide details below:
- Do you think one option or a combination of the options discussed in this consultation would work best to improve the operation of data intermediaries in the UK?
- What other options should be considered in your opinion?
- What additional infrastructure, if any, do you think is essential to enable data intermediaries to operate effectively especially in high-priority sectors (for example, finance, energy, health or transport)?
- What interoperability challenges currently limit the effectiveness of data intermediaries?
- What types of infrastructure would help address these challenges? (For example, technical standards, governance arrangements, or supporting services).

Annex B: Questions for Users of Data Intermediaries

The aim of this survey is to understand more about people's awareness of the services available to them through data intermediaries. For people who have used intermediaries before, the survey will seek valuable information about people's experiences with this process so we can understand how well it is working in the UK. For people who haven't used them, or who aren't aware of them, we seek to understand how comfortable people would be using these services and in which context.

Introductory Questions

- Location
- Age group

Questions

- To what extent are you aware of your right to data portability under UK GDPR?
- Do you know about data intermediaries and what services they provide?
    - If yes, please provide details:
- Have you previously attempted to access or move data held by an organisation?
- What was your intended goal when requesting the data?
    - To see what data the organisation held on you
    - To correct some data the organisation held on you
    - To allow another organisation to use the data about you
    - To move from the organisation to another
    - Other / Unsure
- If you have requested data before, how would you rate the process of accessing/porting your data when you tried?
- Did you request the data yourself (e.g. you contacted the organisation holding your data directly) or did you authorise a third party to access the data on your behalf?
- Did using the intermediary help you achieve what you wanted? How?
- What type of third-party organisation did you use?
    - Personal data dashboard / data management service
    - Data portability / switching service

    - Data donation or research participation service
    - Worker or consumer rights support service
    - Other (please specify)
- Was it clear to you how your data would be used by the intermediary?
- How clear was it who the intermediary was representing when it accessed or shared your data?
- Rank below based on what part of the process was easiest to hardest.
    - Understanding what to do
    - Identity verification
    - Granting permissions / consent
    - Connecting accounts or data sources
    - Waiting for organisations to respond
    - Understanding outputs or results
    - Other, please provide details:
- How long did the process take compared with what you expected?
- Did any organisation (for example, a company holding your data) make the process more complex than you thought necessary when the intermediary acted on your behalf (such as by asking for repeated verification of your request or declining to send the data directly to the intermediary)?
    - Optional open text: what happened?
- What could have made the process easier, or if you haven't attempted to access your data before, what would make you more motivated to do so?
- If you were to use a new third-party organisation to access your data held by another organisation, to what extent do you agree or disagree that the following would be important to you?
    - Knowledge that the third party has robust data security and protection practices and that your data will be safe.
    - Ease of the process – such as only having to 'authorise' the move once.
    - Immediacy of the process – how long you have to wait before the third party has your data
    - Ability to be able to easily revoke access to your data later should you desire
- How comfortable would you feel using a third party to access your data in order to provide a service to you?

- If yes, what services would you consider using?
    - Personal data store – where your data is kept in one place and you control which organisations can access different parts of it
    - A research project that can deliver groundbreaking insights by analysing people's data collectively from pooling it together
    - Services which analyse your shopping habits to provide better recommendations and/or monetary returns to you
    - Services that can compare your data against others to ensure you are getting the best deal from a service
    - Personalised AI agents
    - Other (please specify)
    - None

E03616462

978-1-5286-6567-4