Executive summary

If carefully thought through and well executed, data portability can help drive fair and equitable innovation and economic growth by:

- Enriching and enhancing the services currently made available to citizens and consumers in both public and private sectors
- Creating a new class of citizen/consumer services meeting needs that have never been met before, improving both the wellbeing of households and the operation of competition and the economy
- Removing cost and friction from the operation of both sets of services (new and old) by removing duplication of effort and streamlining and automating data sharing processes.

The new class of citizen/consumer services will:

- often be provided by new market entrants,
- requiring the development of new data tools and services, thereby helping to
- develop the skills, capability and infrastructure that puts UK economy on a footing that's fit for 21st century, and helping to
- open up new avenues for innovation and growth

These potential benefits apply not just in private sector business/consumer markets but in all sectors, including public services and the third sector.

Along the way, data portability can be used to:

- Provide individuals with rich new data assets that appreciate in value over their lifetimes (like owning a home or building up a pension pot, only safer)
- Create in-built checks and balances into how the data economy works, because now data is distributed to millions of individuals (which means that large data monopolies no longer wield such relative power)
- Open up new dimensions of competition as organisations find they need to compete for access to individuals' data (especially the data they cannot collect in the course of their day-to-day business activities) as well as over the quality and price of their products and services
- Help to rebuild trust and confidence, because individuals now have genuine control over their own data
- Promote citizen engagement, because individuals are now empowered participants and not passive, excluded data subjects

For these benefits to be realised the UK needs to develop a new personal data infrastructure where every individual is provided with a bona fide personal data store

which:

- Enables individuals to store their data safely in perpetuity
- Makes it easy for them to share data with bona fide service provides on a Safe By Default basis (see below)
- Attends to the creation of standardised, efficient data management processes that remove friction and cost from data sharing and use for both individuals and service providers in both the private and public sectors.

However, if badly thought through and badly executed, data portability could:

- Encourage a new 'data free for all' where:
- individuals lose what little control they have over their own data, resulting in new Cambridge Analytica-style scandals.
- Current problems relating to loss of trust, a sense of unfairness over the distribution of benefits, and increased concentrations of data power are exacerbated
- The full potential value-creating benefits of data portability (e.g. new types of service) are not realised

Policies and strategies which simply perpetuate and extend today's organisation-centric approaches to data collection and use (where organisations maintain an effective monopoly on the collection and use of customers' data), are highly likely to generate these negative results.

The ability to deliver the positive results of data portability depends on the development of a Personal Data Store infrastructure where individuals are genuinely empowered with their own data. **This infrastructure already exists:** the UK currently leads the world in the development of the new industry of personal data and information management services. This is an opportunity to consolidate and extend that lead.

With services like Mydex - up-and-running, operational, rapidly scalable, safe, secure personal data store infrastructure providers - **it is possible to implement positive data portability quickly, safely and at scale.**

This Mydex CIC briefing paper explores the opportunities and challenges as they relate to:

- The **structure and architecture** of the digital economy
- What **value** it is able to create and how
- The **infrastructure** needed to unleash the full personal, social and economic benefits of personal data
- **Strategies** needed to realise the benefits and avoid the pitfalls
- Resulting **policy priorities**

Background

Today's data ecosystem has evolved to be *organisation-centric*: that is, it is a data ecosystem where organisations (mostly large organisations in both the public and private sectors) are the only entities collecting and storing data about individuals, and where they use this data overwhelmingly for their own operational purposes. [1]

While citizens and customers have benefited in many ways from organisations' uses of personal data, the structure and architecture of today's digital economy means:

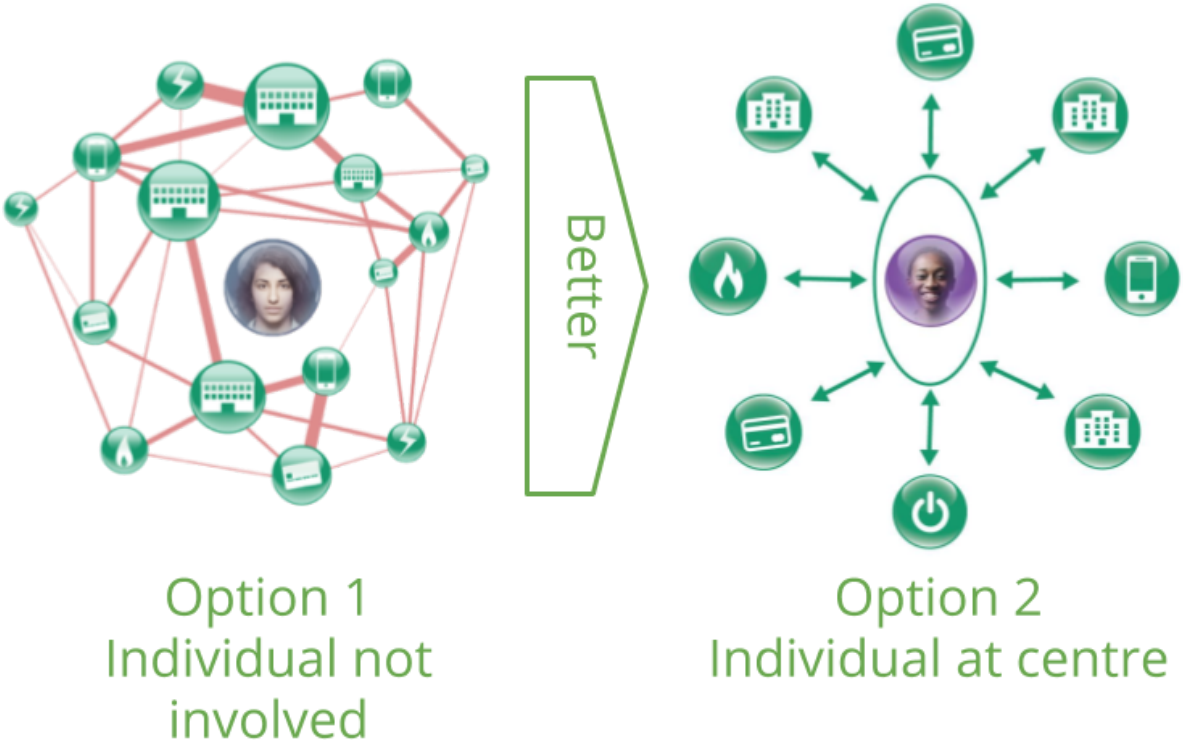
- Individuals do not have the means to collect and use their own data for their own purposes; individuals only experience the potential benefits of their data indirectly (via data controllers using their data to provide services) and not directly (by being able to use their own data for their own purposes);
- their data is dispersed across many different, separate data silos with multiple barriers to access, integration and interoperability of a technical, legal and commercial nature
- individuals are largely excluded from active participation in the data economy, treated as data 'subjects' (as European data protection regulations call them).

Article 20 of the new European General Data Protection Regulations creates a new right to data portability: a right "to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided." Depending on how it is ultimately interpreted and implemented, this new right is a potential game changer, opening a door to a fundamental restructuring of the digital economy that frees personal data from its current organisational 'prisons' and makes possible the development of a wide range of exciting new services, sparking a new phase of innovation and economic growth.

Article 20 envisions two different ways of implementing data portability:

- Option 1: Data being ported from one data controller to another on the individual's request
- Option 2: Data being ported from the original data controller to the individual, to be held by that individual (and, potentially, shared forward on a different occasion)

[1] For example: more efficient administration (e.g. billing, keeping records of transactions and interactions with customers), operational delivery of services (e.g. it is not possible to provide a banking service without data about transactions), to organise and coordinate activities (e.g. deliveries),to gain new insights, make better decisions, do marketing and advertising, package data for rent or sale.



This Briefing Paper argues that, pursued as the main approach, Option 1 (of organisation-to- organisation data porting) is highly likely to result in the negative, counterproductive effects outlined above. Only by placing the main emphasis on Option 2, with data being ported to a bona fide Personal Data Store, can the full positive potential of data portability be realised. This Mydex CIC briefing paper explores the reasons for this in detail in the section on Strategy below.

While the new right to data portability is a key enabler and catalyst, it is not enough to realise the full personal, social and economic benefits of new approaches to the collection and use of personal data. Additional provisions and initiatives are needed. This briefing paper explains what they are and why they are needed.

It looks at:

- The need for fundamental reform of the structure and architecture of the digital economy so that individuals are empowered with their own data
- The value, innovation and growth opportunities this creates
- The infrastructure needed to make this happen
- The strategic decisions that are needed to support this reform
- The policy initiatives that are needed to bring these strategic decisions to life

1. A structural challenge

The structure and architecture of today's digital economy is no longer fit for the purposes and requirements of a prosperous, flourishing 21st century digital economy.

As outlined above, the future development of the digital economy is hampered by a critical structural flaw at its heart: currently, the only entities able to make full use of personal data are the organisations that originally collected this data. This means:

- It is extremely difficult, both operationally and legally, for other organisations to access and use this data to add value in new and different ways
- It is almost impossible for individuals to access and use their own data for their own purposes
- It fails to work positively with the unique and essential characteristics of data e.g. that it can be reused many times without getting 'used up' and that it can be copied, shared, added to and 'sliced and diced' at very low cost

Under this structure, the full value-creating potential of personal data can *never* be realised. That is why fundamental structural reform is needed: to lift the restrictions on the uses of data created by our current organisation-centric set-up. GDPR provisions for data portability open the door to this structural reform.

In considering this structural reform, it is important to note that the ways personal data are collected and used in today's digital economy have created different types of issue and problem which need different types of response. For example, there are:

- 'business as usual' problems arising from lack of professionalism, mistakes, etc; deliberate uses of data to maximise profits in ways that cause nuisance or harm for consumers, and criminal activities e.g. fraud, identity theft. These are specific problems that require specific detailed policy, regulatory and other solutions.
- systemic abuse (e.g. the adtech industry's widespread collection and sharing of personal data by third parties unknown to citizens, acting without their consent). Robust enforcement of GDPR can help to tackle these abuses which are hopefully a temporary phase, not the future of the data economy.
- unfair outcomes (e.g. consumers not getting a fair share of the rewards/value their data generates, and the emergence of new forms of data monopoly (such as Google and Facebook) which may be stifling competition and may require intervention by the competition authorities.

Mydex CIC is fully aware of these issues and problems and we fully support efforts to tackle them. Our central point is different, however. **Even if all these issues and problems were addressed in a satisfactory way, the fundamental structural flaw at the heart of digital economy (the fact that the full potential uses of data are**

restricted by the role of today's data controllers e.g. its overwhelmingly organisation-centric nature) would remain.

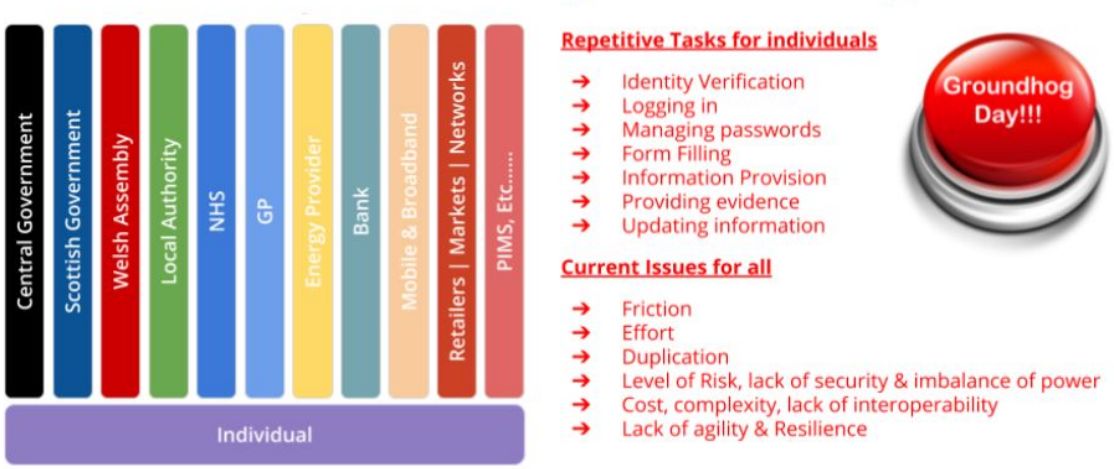
Addressing this flaw is not about addressing things that *are* happening but should not be happening (as listed above); they are about addressing things that *should* be happening but are not happening. They are about unleashing so-far unrealised potential.

2. Value

Today's structural flaw restricts the value that personal data can be used to create. Specifically, it stifles value creation where it:

- depends on the combination and integration of data currently held in separate organisational data silos - for example, creating a rounded picture of an individual's financial circumstances for the purposes of financial advice
- does not fit the existing data controller's purposes or priorities. This means that the development of a whole class of person-centric Personal Information Management Services (PIMS) is being held back (see below)

To see the full value-creating potential of personal data we need to step outside our current mental and operational frameworks (of organisations collecting and using data for their particular purposes), look beyond industrial age roles such as 'consumer' and 'producer', and look at the needs and activities of individuals and households in managing their lives from their point of view. In this Paper we concentrate on the value adding, innovation and growth potential of new classes of services, assuming that it is already agreed that incumbent service providers could innovate better if given access to additional data.



Status Quo with individual's trying to manage multiple relationships with different organisations.

Individuals and households undertake all the tasks that large organisations do, except at a smaller scale and without professional help. They:

- Source inputs from suppliers ('shopping')
- Buy capital equipment (cars, washing machines, ovens etc)
- Use this capital equipment to process and add value to the inputs they have purchased
- Undertake maintenance of their capital equipment
- Make plans, set priorities and timelines, allocate budgets
- Undertake administration, dealing with public authorities, the tax man etc.
- Face logistical challenges of moving things and people to and from the right places at the right times
- Employ people (e.g. services like plumbers, physiotherapists, decorators, keep fit instructors, child care minders)
- Develop human resources: teaching and learning skills and capabilities
- Develop and manage relationships with suppliers
- Plan and deploy financial resources, making savings, taking out loans, managing cash flow, paying taxes.
- Manage and juggle the multiple different 'life' departments (e.g. money, health, home, transport, career, etc) and the requirements needed to keep the whole undertaking going
- Make decisions about all the above
- Search for, organise and use the information they need to make these decisions and undertake all the above tasks efficiently and effectively [2]

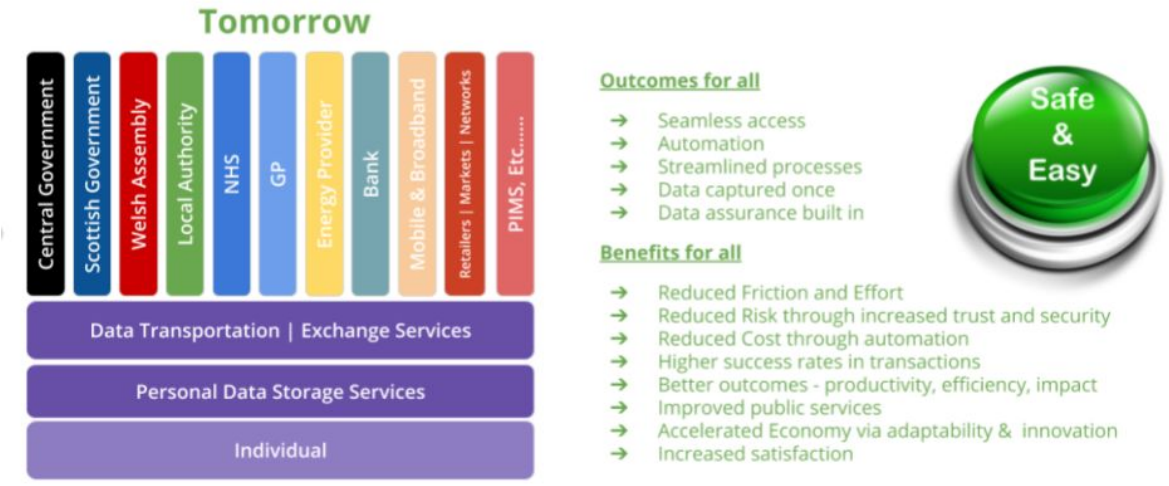
Unlike large organisations and corporations, individuals and households do not employ large armies of professional staff to manage these operations and they do not (yet) build and deploy large databases and information management systems to assist them. The result is a significant market and value gap: a wide range of needs and wants that are not being addressed.

At the same time, over the last 30 years, the costs of collecting, storing and sharing information have fallen over a million-fold. This means that it is now possible to undertaken information processing tasks for individuals and households at very low cost (often for free) that were once prohibitively expensive.

A new class of value-creating services is emerging to connect these new information capabilities to address the long-standing 'life management' value gap. The core focus of PIMS is to deploy sophisticated information services (including AI) to help individuals and households make better decisions about and better manage and optimise the life operations described above. NB: this is about helping optimising the management of individuals' lives and households' operations as distinct to (and in addition to)

[2] See *The New Bottom Line: Bridging the Value Gaps that are Undermining Your Business,* Alan Mitchell, Andreas W Bauer, Gerhard Hausruckinger, Capstone, 2003

optimising the performance of service-providing organisations.



Individual at the centre equipped with tools to make life safe and easy working across organisations

Some common themes distinguish PIMS from traditional service providers.

- traditional service providers (traditional data controllers) view and treat 'the customer' from a standpoint within the organisation; PIMS view and treat individuals' 'suppliers' (traditional service suppliers/data controllers) from a standpoint within the household; as external to it
- traditional service providers (traditional data controllers) each seek to manage their relationships with multiple different customers (Customer Relationship Management, marketing); PIMS help individuals and households manage their relationships with multiple different external suppliers ('Vendor Relationship Management' [3], shopping)
- traditional service providers (traditional data controllers) use data to optimise the performance of their operations; PIMS helps individuals and households use data to optimise their 'life operations'.

This *person-centric* perspective on value includes:

Day-to-day household administration:

- **keeping admin details safe** and easily accessible (e.g. passwords, answers to security questions, recovery keys, appointments, identity credentials such as national insurance number, tax references and NHS numbers, PIN numbers etc);
- **calendar management** (**k**eeping a record of things you need to do - car MoTs, loved one birthdays, pay bills, health check ups etc, with automatic alerts so they're never forgotten);

[3] https://en.wikipedia.org/wiki/Vendor_relationship_management

- **keeping records** for example of current suppliers, contracts with them, correspondence, contracts, contact details etc.

Managing the operational side of household departments, including coordinating and integrating inputs from multiple service providers to achieve a desired outcome. Examples include:

- **managing home move** (timeline of task deadlines, contact details, updates and reminders, things to be aware of, including direct communication channels to key parties);
- **health and social care** for individuals having to deal with many different agencies, (e.g. managing illnesses like diabetes and cancer, dealing with hospitals, GPs, specialist doctors, pharmacists, other health professionals, support workers, care providers, etc). A PDS enables all data to be integrated into one safe place so that information can be shared safely and efficiently in a way that puts the individual in control, at the heart of the process;
- **personal financial advice** drawing on data from a variety of different financial services providers to create a complete picture of an individual's financial circumstances, with ability to set up a rules engine to trigger event-driven automated actions;
- **travel and mobility as a service** Use identity to search and use different modes of travel and to purchase multi modal tickets from different suppliers. Use mobile phone to show token.
- **making better decisions relating to the various household departments**: money, health, home etc - decisions to guide personal/household priorities, actions, behaviours
- **shealthy** Keep a record of your keep fit, nutrition and lifestyle regime to share with personal trainers, medics and others for advice to maintain improvement independently of the wearables and other devices you use to capture the data.
- **managing household budgets** Use data downloaded from banks, supermarket loyalty schemes (e.g. Clubcard, Nectar) plus automatically captured receipt data to better understand where they money goes, and how to manage it better.
- **energy advice** Combine information about lifestyle, energy usage, home details (is it insulated? Is it south-facing) to make recommendations about infrastructure (e.g. insulation, solar panels) and behaviour changes to reduce energy costs and consumption.
- **going green** Build up information about the carbon footprint of different activities to find ways to reduce it

Managing relationships and dealings with suppliers. [4]

[4] This is the difference between 'Customer Relationship Management' and marketing (organisations managing their dealings and exchanging value with customers), and supplier

- **'Always on the best deal'** Specialist utility management service that connects information about the individual's current tariffs, stored in a personal data store, to automatic reviews of what's available on the market, to help the individual always get the best deal without having to spend hours on comparison sites.
- **Identity as a service** Hold a secure encrypted token that proves you are who you say you are, so you can quickly and automatically sign in to, and access, services in both the public and private sector without having to remember or use usernames and passwords;
- **Pensions management** Keep a record of all pension pots from many different employers in the same place, so they aren't forgotten and are easily accessed;
- **Consent and permissions dashboard** Maintain a record of all organisations holding your data, including what consents and permissions have been provided, plus services to easily assert rights under the law (e.g. see a copy of this data, request a copy, withdraw consent). Set your own privacy policy and T&Cs for access to your data;
- **'My wardrobe'** Use receipts from clothes purchases to create a 'virtual wardrobe' so that specialist services can recommend next best purchases e.g. 'this would go really well with that'. [The same concept can apply to any specialist shopping area]
- **Warranty management** Maintain a record of all big ticket purchases and associated warranties and guarantees with information on who to contact if something goes wrong. Automatically link to insurance policies.

Developing information sharing relationships with suppliers to reduce costs and improve outcomes

- Sharing information held in my personal data store about my finances, shopping, health, transport, hobbies etc with specialist suppliers so that they can **recommend the right services for me and gain richer insights** to develop their new product development
- **Live sharing information about contact and other admin details** so that errors are avoided (e.g. inform all the organisations I have a relationship with that I am moving home; changed email address; changed name etc with one click of a button)
- **Personal health record -** Keep my own record of conditions, illnesses, treatments plus basic information such as blood type, allergies, who my physician is, next of kin, specific instructions e.g. organ donation, DNR (do not resuscitate), Lasting Power of Attorney so that I can easily share appropriate details to medical practitioners, whether at home or abroad.
- **Lifelong learning record -** Keep a record of all exams passed, qualifications and experience gained, work experience etc to populate CVs, track continuing professional development, secure reference and commendations from clients,

or ''Vendor Relationship Management' and household sourcing or 'shopping' (individuals managing their dealings and exchanging value with organisations).

colleagues and employers, build your evidence of achievements and get advice on career development.

Each of the above tasks requires a different type of 'information product' that draws on specific bits of data to create a specific desired outcome. Information products are the informational equivalent of physical products. A physical product like a kettle is made up of a set of necessary components such as a heating element, a container for the water, a thermostat, a chord and plug to power the heating element, a switch. Many of these components, such as thermostat, plugs and switches are standard components that can also be used to create other products.

Likewise, an information product is made up of a set of necessary informational components. For example, an energy price comparison service requires information about the identity of the individual and the individual's home, their energy consumption, available tariffs on the market. Many of these informational components can be use for other purposes. For example, information about the individual, the individual's home and energy consumption could be used for a service providing advice on how to reduce energy bills by means of home improvements such as insulation, or by means of behaviour changes.

In the case of the kettle, the kettle manufacturer is likely to source standard components from specialist distributors of such components: constructing and assembling the kettle is a different task to making its components available. Likewise, to enable the growth of information products that help individuals make better decisions and manage their lives better, we need services that assemble specific information products using specific bits of information (e.g. price comparison, advice about home insulation, advice about behaviour changes to reduce energy consumption), and we need services that make this information available. While PIMS 'manufacture' specific information products, Personal Data Stores specialise in enabling information availability, first and foremost to the individual, and building on this, sharing this information with service providers (whether PIMS or traditional product/service suppliers such as banks or retailers).

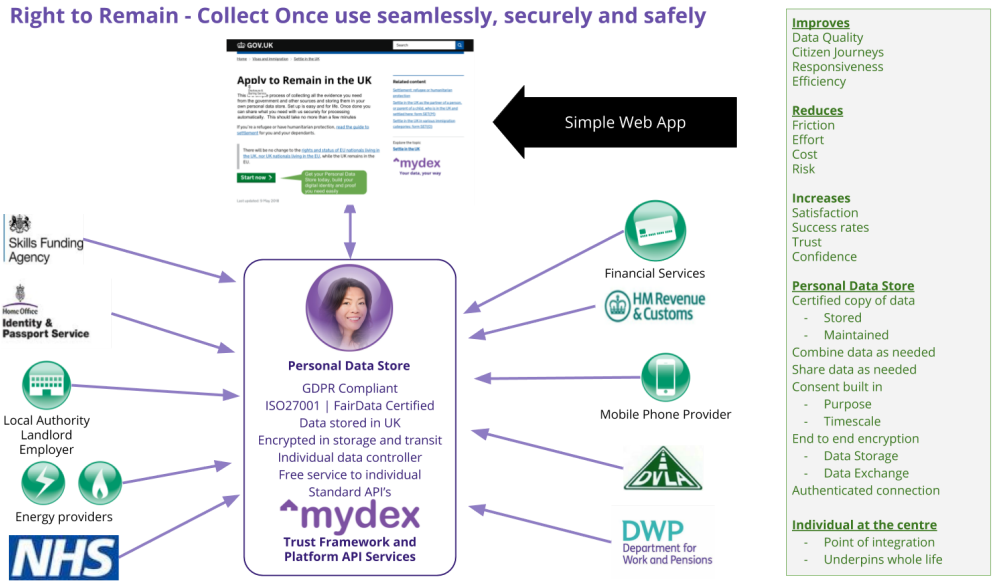
Social benefits

Data portability could also open the door to some unexpected social benefits.

Right to remain

If GDPR data portability clauses are interpreted to include the sharing of verified attributes (see below), the porting of data could be used to tackle issues relating to the right to remain. EU citizens living/working in the UK could request service providers to pass a secure token verifying an attribute about them to their PDS. Such attribute providers could include financial services providers, HM Revenue & Customs, DVLA, DWP, NHS, mobile phone provider, energy suppliers, local authorities, landlords,

employers, Skills Funding Agency etc. See diagram below.



EU citizens could then share these attributes with the immigration authorities to establish their right to remain - thus eliminating huge amounts of work and hassle for both the authorities and the individuals concerned.

Social inclusion

If GDPR data portability clauses are interpreted to include the sharing of verified attributes (see below), the porting of data could also be used to tackle social exclusion. Many individuals today suffer because they lack traditional ways of proving who they are (e.g. driving license, passport). Support services helping individuals leaving care homes, prisons etc can use a personal data store to build up a bank of 'verified attributes' from dealings with different authorities. Each time a new verified attribute is added, it adds evidence of who the individual is and reduces uncertainty and risk for service providers. Over time, this helps them prove their identity.

Creating new opportunities

The common feature of all these services is that to work, individuals have to be able to access, gather, store, share and use their own data for their own purposes. And for this to happen safely, efficiently and effectively, the data needs to be held by or linked to by a bona fide Personal Data Store that puts the individual in control of their own information and makes the individual the point around which data and related services are integrated.

Another common feature of these services is that:

- It's currently not possible for incumbent data controllers to provide these

services (because the data is simply unavailable)
- It's very difficult to access and share the data for administrative and legal reasons (e.g. data protection provisions restricting organisation-to-organisation data sharing without individuals' consent)
- It's not in the interests of incumbent data controllers to provide these services (e.g. services that help individuals manage their dealings with other suppliers as well as themselves, price comparisons)

Porting data to personal data stores therefore opens up significant new opportunities for the development of new services by:

- Personal Data Stores themselves, providing the infrastructure of person-centric data storage, access and sharing
- New 'Personal Information Management Services' accessing and using the data (under individuals' direct control) to provide new services (or 'information products') focused on helping individuals make better decisions and manage their lives better
- Existing service providers accessing enhanced, enriched data sets (under individuals' direct control) to provide better personalised services at lower cost.
- Technology, software and other infrastructure and service providers enabling these services to operate efficiently and safely

In this way, the right, person-centric approach to data portability is a means to unlock both improved productivity and innovation and growth across the economy as a whole, with the benefits applying equally in the public, private sectors and social sectors.

This gear-shift from information processing by and for organisations to the additional layer of information processing by and for individuals and households is the second big wave of the information age: a massive new growth opportunity akin to the shift from steam to electrification in the industrial revolution. It will become a key priority for Governments and policy makers over the coming decades.

3. Infrastructure

For the benefits of person-centric, citizen-empowering data portability to be realised, the UK needs to develop new data infrastructure. **Specifically, every individual in the country needs to be provided with a bona fide personal data store.**

It is important to establish the criteria by which to judge whether or not a service claiming to offer Personal Data Store services is bona fide or not. Policy makers and regulators could usefully undertake further work to establish these criteria but in our view certain fundamental principles need to apply. They include:

- **Zero-knowledge operations** The organisation/s providing individuals with Personal Data Stores should not be able to look into or control what individuals do with their data: individuals should hold their own encryption key that the PDS provider does not have access to. The PDS's job is to provide safety and access to individuals (a bit like a Swiss bank providing a vault where individuals hold their own unique key)
- **Separation of functions** PDS providers should not use the data held in a PDS to provide specific services (such as price comparisons or health advice). These services should be provided by specialist operators with specialist domain expertise, accessing individuals' data specifically for these purposes on a Safe By Default basis (see below). PDS providers should restrict their own activities to providing personal data *management* services to individuals e.g. enabling data to be stored safely, enabling individuals to access and manage this data and to share this data safely and easily.
- **Aligned incentives** PDS providers should not be allowed to, or have any financial incentive to, share sell or rent individuals' data. They should not be in the business of monetising individuals' data; they should earn their keep from fees/charges for the provision of data management services.

For more details on Mydex's view of what defines a bona fide personal data store, see our blog on the subject Design Principles for a New Data Infrastructure.

Operationally, data portability faces many hurdles before it can become safe enough, simple enough and easy enough to be carried out on a large scale. Key obstacles include:

- **Governance**: ensuring clear, fair rules of conduct for all concerned
- **Two-way identity assurance**, so that individuals know that any data they share is with a bona fide service provider and organisations know that any individual seeking access to data is making a bona fide request
- **Interoperability**, which covers a wide range of technical issues including data formats, metadata (e.g. clear descriptions of data being shared), ensuring data provenance (where did it come from? Is it from a trustworthy source? Has it been interfered with in transit?)
- **Security** of both data storage and data transmission.

Tackling these operational hurdles is the job of the new PDS infrastructure. **Without it, data portability is likely a) never to take off or b) result in errors, unnecessary cost, complexity and confusion.**

4. A Strategic Choice

Given that data portability opens the door to a fundamental (necessary and positive)

change to the structure of the digital economy, and that it needs new data infrastructure to achieve its potential, it will take time to establish, spread, embed and fully apply. Therefore, it requires a strategic approach, designed to last perhaps longer than the lifetime of individual parliaments.

What the right strategy looks like

We suggest this strategy should specifically seek to realise benefits that only come from Option 2:

- encouraging the development of new person-centric services that help individuals (as well as organisations) manage their lives better, independently of current incumbents;
- deliberately helping individuals build personal data assets of their own which appreciate in value and utility over their lifetimes and which create in-built checks and balances in the way the digital economy works;
- encouraging the active participation of individuals in the digital economy
- fostering the new data sharing infrastructure, including enabling the provision of a Personal Data Store to every UK citizen, that enables the above

We expand on how to do this in the Policy section below.

What the wrong strategy looks like

A truly positive strategic approach contrasts starkly with a non-strategic approach which could be characterised as follows:

- Assumes Option 1 (organisation-to-organisation data sharing) because 'that's how it's currently done'
- Focuses solely on the private sector and 'consumer' issues while ignoring the huge opportunities opened up by data portability in the public and third sectors
- Focuses mainly on data's role in aiding switching, while overlooking the immense opportunities for additional value creation elsewhere
- Focuses mainly on competition issues: that is, improving how competition works for *existing* products and services while overlooking the immense opportunities opened up the development of entirely *new* products and services (and the skills, capabilities and infrastructure needed to deliver them) which, in turn, open up new dimensions of competition (e.g. competition to access individuals' data)

Unfortunately, the UK Government's current Modernising Consumer Markets Green Paper [5] displays some of these characteristics (please see separate Mydex CIC submission).

5 https://www.gov.uk/government/consultations/consumer-green-paper-modernising-consumer-markets

First key ingredient of any data portability strategy is a choice of priorities. Do we see data portability's main role in the future digital economy as based primarily on:

- **Option 1:** organisation-to-organisation data sharing permissioned by the individual?
- **Option 2**: data returned to individuals who then controls its further use?

Option 2 breaks into two alternative modes. The first mode is data being downloaded to individuals' current devices, without specialist professional services to ensure security and undertake data management and curation. We would not recommend such an approach. The other mode as identified by the Article 29 Working Party's Guidelines of Data Portability [6] is to download the data to the individual's Personal Data Store, as outlined above.

Mydex CIC's strongly held view is that if Option 1 is adopted as the main approach it will simply perpetuate, extend and exacerbate the problems and drawbacks already experienced with the status quo: with individuals feeling they are losing control, not getting the full benefits of their data, and with multiple concerns about invasions of privacy and poor data protection.

One possible benefit of Option 1 is that, in the beginning, it is more streamlined than Option 2: transferring data to the individual before it is forwarded to a new service provider creates an extra step in the process and, potentially, places an additional cognitive and administrative burden on the individual.

However, this apparent benefit is largely illusory (see below), and if Option 1 becomes the default mode, many of the strategic benefits of data portability will not be realised, and many of the harms of the current system will be exacerbated.

Risks created by adopting the wrong strategy

Lack of Consumer control

Under Option 1, individuals could find themselves consenting to multiple data transfers to multiple new service providers without any means (other than personal effort) to keep track of who their data has been shared with, for what purposes, under what terms and conditions. Over time, this means individuals' data will be dispersed across many more service providers than now, with individuals feeling even less able to understand or control what is being done with their data. (One of the core jobs of Personal Data Stores is to provide consents and permissions management dashboards, with active/ automated monitoring and action facilities, to address this need.)

Failure to realise true value potential

[6] https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Many of the potential new services highlighted above are only made possible (or made much easier and cheaper to provide) by creating a new shareable data asset aggregated around the individual (rather than dispersing individuals' data further across multiple new data controllers). If the UK adopted only Option 1 (organisation to organisation data sharing) it is highly likely that the full range of innovation opportunities would not be unleashed.

Inability to create new data assets

Under Option 2, every time data is transferred, a copy of that data is kept in the individual's Personal Data Store. This means that over time individuals are building their own personal data assets that are continually appreciating in scope and depth. In fact, over time, this personal data asset will create a richer, rounder view of that individual (behaviours, preferences, circumstances etc) than any of today's existing databases - simply because it is aggregating and combining the data that is held in these databases. The data held for the individual becomes an asset that is continually appreciating in value, much like owning your own home or building up a range of pension pots. **This never happens under Option 1 where the opposite happens: where the individuals' data is dispersed even further** across an ever growing number of different service providers.

This new type of rich personal data asset can become increasingly valuable to individuals *and* to service providers wanting to provide highly personalised, joined-up services that rely on multiple data points. This would have the twin effects of:

- Opening up new dimensions of competition as organisations find they need to compete for access to consumers' data (especially the data they cannot collect in the course of their day-to-day business activities) as well as over the quality and price of their products and services
- Creating in-built checks and balances into how the data economy works as personal data is no longer concentrated into a small number of large data silos controlled by large organisations: it is also distributed with each individual holding their own data assets. This would reduce the relative power and impact of today's data monopolies.

Reduction in Efficiency

Option 2 would also be more efficient because it would minimise duplication of effort. Example: say three new service providers want to provide different aspects of financial advice and service, drawing on a rounded picture of an individual's financial affairs. They require data from two different current accounts, two credit cards, a savings account, and a loan. Each of the three service providers would therefore need to aggregate data from six different data controllers.

Under Option 1 (organisation-to-organisation data sharing), each of the new service providers would raise six different requests to the six different data controllers via the

individual. Each data controller would get three different data sharing requests. Under Option 2 however (data ported to the individual's personal data store), once the data has been ported to the individual, the individual can decide to share it directly - obviating the need for repeated requests to data controllers.

Option 2 would also promote efficiency in another way. Under Option 1, each new service provider is likely to adopt their own formats, definitions of data, security protocols etc - a proliferation of approaches with the inevitable consequence of undermining interoperability. A PDS-based approach would have the opposite effect of encouraging the creation of standardised, efficient data management processes that remove friction and cost from data sharing and use for both individuals and service providers in both the private and public sectors.

Reduced Safety

Option 2 would also be much safer. One of the core jobs of a bona fide personal data store is to create and enforce data sharing agreements that protect the individual's data. The PDS would recommend standard terms for data sharing (see Safe By Default below) and would strongly recommend that individuals do *not* share data if the proposed terms and conditions give the new service provider access to data it doesn't need to provide the service in question, or rights to share or use the data for purposes other than the provision of the service in question. In other words, onward data sharing from a bona fide Personal Data Store brings with it built-in data and privacy protection.

Personal Data Stores would also provide consent and permission dashboards where individuals can see and monitor all the data sharing permissions they have given.

In contrast, under Option 1 the cognitive and administrative burdens of understanding exactly what service providers are asking permission for means that individuals are much more likely to take the approach that they often take now: in the interests of a quiet life and accessing the service they want, simply sigh and tick the consent box … except that now this approach is being replicated across a growing number of service providers. Option 1 therefore exacerbates risks of a new data 'free-for-all' making new Cambridge Analytica-style scandals much more likely. On the other hand, using bona fide PDSs is more likely to result in increased data protection and genuine control of their data by individuals.

Option 2 is therefore likely to contribute to rebuilding trust and confidence in the data economy because individuals now have genuine control over their own data, and also helps transform the psychology of data, promoting personal agency and citizen engagement. Individuals are now genuinely empowered by and with their data. They are participants in the data economy; no longer passive, excluded data subjects.

In considering options about data portability policy makers have two key decisions to make:

1) Do we want to prioritise data portability as a means to unleashing the full personal, social and economic potential of personal data? In Mydex CIC's view, the answer has to be a resounding 'Yes'. There is enormous unrealised potential for new value creation and innovation waiting to be released.
2) If we do want to actively promote data portability, what approach should we adopt?
    - 'Let the market decide' which approach to data portability to adopt? (In which case, the likelihood is that Option 1 will be adopted by default, because key parties are already familiar with it.)
    - Favouring Option 1 as the default approach?
    - Favouring a PDS-based Option 2 as the default approach?
      In Mydex CIC's view, the answer should be to promote Option 2 as the default approach a) because it will unleash a greater degree of innovation and value creation, b) because it will help restructure the data economy rather than ensuring 'more of the same', c) because it would be more efficient and d) it would be safer.

The question, then, is how to implement this strategy.

5. Policy

Policy makers could adopt a number of policies to implement the above strategy, using GDPR as a springboard.

A) An economy wide approach

Ensure that the potential benefits of data portability are applied across all sectors of the economy. In all their work, policy makers should ensure that the policies and initiatives they pursue apply equally to the public sector and third sectors as well as the private sector.

B) GDPR implementation

While GDPR opens the door to a restructuring of the data economy by allowing data to be ported from its current resting place in organisational data silos, it does not specify exactly what data should be included, or how data portability processes should operate.

- What data? One way policy makers could clarify and extend the application of GDPR would be to stipulate that 'verified attributes' should be included as a valid data portability request. If requested, organisations should be required to provide secure tokens verifying attributes about the individual. Some work may have to be done to create a list of verified attributes that individuals can ask for

e.g. 'has a valid driving licence', 'is over 18', 'has completed Bank A's Know Your Customer process', 'has passed these exams' etc. This may be aided by the work that is already underway to publish registers of information [7] and the work currently being undertaken by GDS to develop cross-government standards for attribute assurance.

- What process? Policy makers need to encourage the development of the governance, policies and infrastructure needed to support safe, efficient, mass-scale data portability. This should include:
    - work to develop standard, familiar and consistent design patterns for sharing data and for describing data structures which can travel with the data and be machine readable, reviewing how data is being used, and intervening to stop abuses
    - work to establish mechanisms for two way identity and attribute assurance using a range of means that are based on cryptographic techniques to ensure data and identity is not modified in transit
    - encouraging the sharing of data via well-formed APIs

C) Realising the potential of PDSs

To ensure Option 2 works to best effect, policy makers should:

- Establish a requirement that every request to port data must include an option for delivery to a bona fide Personal Data Store
- Undertake a consultation to define the criteria used to define whether a PDS is bona fide or not
- Ask the Information Commissioner's Office (ICO) to establish a 'whitelist' of bona fide PDS providers. This could become part of the UK's Trust Service List that the UK's Department of Media, Culture and Sport recently took ministerial responsibility for
- Data controllers to be provided with a right to refuse an initial request for porting if they are not satisfied that it is to a bona fide PDS (with strict penalties for data controllers found to be gaming this provision to subvert legitimate requests for data porting)

D) Ensuring new service providers genuinely add value

- Data controllers to be provided with right to refuse an initial request for porting if they are not satisfied that it is to a bona fide service provider (with strict penalties for data controllers found to be gaming this provision to subvert

[7] https://www.registers.service.gov.uk/

legitimate requests for data porting). It will be one of the jobs of PDS service providers to ensure that this is the case.

- To avoid any chances of a new 'data free for all' emerging policy makers should establish 'Safe By Default' as the standard design pattern for data sharing terms and conditions. By 'Safe By Default' individuals should 'just know' that when a new service provider requests to access their data, they will
    - Only access the data needed to provide the service in question, and no more
    - Only use this data for the purpose of providing this service, and for no other purposes
    - Not share this data with any other parties (except, perhaps data processors operating under the same terms and conditions to help deliver the service in question).
    - Adopt standard transparency design patterns, enabling specialist third parties to easily and efficiently review the ways in which new service providers are using data that has been ported.

  In other words, policy makers should establish the expectation and practice that service providers accessing individuals' data under data portability provisions should apply data protection standards that are *higher* than currently required under the law, which minimise chances of abuse while also minimising the cognitive and administrative burdens of consent. (This is because Safe By Default is 'legitimate' data processing under GDPR, and the creation of standard Safe By Default terms and conditions eliminate much duplication of effort). For more on the concept of Safe By Default see our blog on the subject.

E) Recognising the work that has already been done

One of the key messages of this Briefing Paper is that the means to realise the positive opportunities of data portability and to avoid the risks and pitfalls already exist. A number of Personal Data Store operators are already operational: the UK is leading the world both in the creation and development of Personal Data Stores (there are, for example, hardly any operational PDSs in the US), and in the PIMS (Personal Information Management Services) that access the data held by PDSs to provide particular information services.

This emerging industry of PDSs and PIMS is already being built on a common vision of full data portability. PDSs have already developed a wide range of tools and technologies designed to make data portable possible in a way that truly benefits citizens and the bona fide organisations they deal.

For example, Mydex is already ten years old. In that time it has built a Personal Data Store infrastructure that is:

- Operational, providing many of the personal data management tools described above
- Scalable. As one of the five companies chosen for the initial launch of the Government's Verify identity assurance project, Mydex has built a technology infrastructure capable of serving *every* citizen.
- Secure. Every aspect of Mydex's data storage and data transmissions is encrypted to the highest available standards. The *whole company's* operations (not just particular services) are ISO 27001 certified. Because each individual's data is stored in a separately encrypted data store, Mydex has not built a single large database that becomes a honeypot for hackers.
- Recognised. Mydex is already recognised as a public sector services supplier via its listing on G-Cloud.
- Trustworthy. As a Community Interest Company, Mydex is legally required to pursue its mission of empowering individuals with their own data and is *asset locked.* In other words, it is not possible for Mydex to offer services claiming to empower individuals with their data and then sell-up to another entity with a different agenda. Mydex's assets can only be transferred to another entity with the same community interest purpose.
- Aligned incentives. Mydex does not earn its money by monetising consumers' data. It makes its money by charging fees for data *management* services, including fees for permissioned access to individuals' data.
- Designed with privacy in mind. As a zero-knowledge operation, Mydex can not even see the data individuals store in their Personal Data Stores, because each individual has her own encryption key. A key part of its offering is data management tools and services that make it extremely easy for individuals to manage and control their data, *saving* them time and effort rather than making data management a burden for them.

Summary and conclusion

The UK needs fundamental structural reform if it is to realise the full personal, social and economic potential of personal data in a digital economy. Data portability opens a door to achieving this structural change. Done well, it can open up rich, exciting opportunities for value creation, innovation and growth. But done badly, the harms it creates could outweigh the benefits.

Policy makers and regulators have the opportunity to do data portability well using services and infrastructure that **already exists**. They can and should seize this opportunity.

For further information or support
Please contact David Alexander - Chief Executive m: 07717473661 or david@mydex.org