Design Principles
for a
New Data Economy
21st June 2022

Index

Introduction and Summary

This White Paper, based on a talk given by Mydex CIC in Korea, outlines the key design principles that are needed if our society and economy is to unleash the full benefits of personal data via a fit-for-purpose data economy.

Access to personal data is essential for individuals to manage their lives better. It's also essential for the delivery of all services dealing with individuals. It has social and economic impact across every aspect of individuals' lives and every consumer/citizen-serving industry in the public, private and third sectors.

Our society's current approach to the collection and use of personal data is dysfunctional. Citizens have little or no control over their own data and are not benefiting as they should from it. Service providers often lack access to the data they need and face high costs in accessing and using it. The system as a whole experiences high costs along with low levels of trust and restricted innovation.

Aside from the usual operations of power and politics, these problems are caused by the structure and architecture of today's data infrastructure: its siloed, organisation-centric nature. To address these problems and liberate personal data's potential we need a different data infrastructure that:

- enables citizens to participate directly in the workings of this economy for their own benefit,
- enables *bona fide* service providers to access and use the data they need at lower cost,
- builds the data assets needed to enable further data-driven innovation.

There is one way to do this: provide every citizen with their own personal data store which enables them to collect, store and use their own data for their own purposes, independently of the organisations that may have collected data about them. These personal data stores should act as safe, efficient citizen-controlled hubs for the sharing of their data.

To work efficiently and effectively this new layer of personal data infrastructure needs to operate to design principles that ensure its fitness for purpose. Figure 1 provides an overview of these design principles, the nature of the infrastructure that achieves this, the institutional framework for this infrastructure, and its underlying economic and business logic.

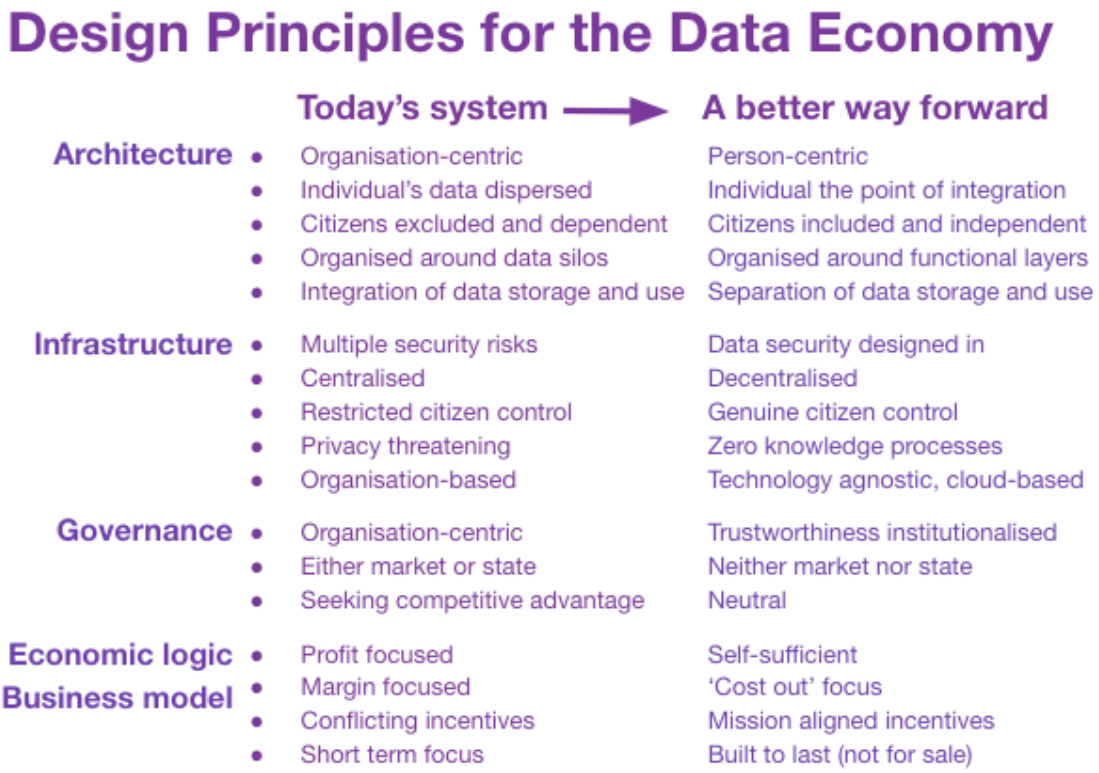

Figure 1: Overview of the key design principles needed for a safe, secure, efficient data infrastructure that unleashes the full potential benefits of personal data

One critical point needs emphasising. Design principles like these do not represent a pick-and-choose menu. They are interrelated, intertwined and enmeshed. They- create an integrated system that only works as a whole. If one of these design principles is missing or dysfunctional the health of the entire system may be compromised.

The following four tables, relating to system architecture, the infrastructure itself, its governance and economic/business models, summarise the salient points behind the design principles outlined in Figure 1. The White Paper itself expands on these themes.

Design principles for the new data economy	
Architecture	
Person-centric	Today's system is organisation-centric, with organisations collecting and using data about individuals for their purposes. Individuals need to be able to collect and use their own data for their own purposes.
Individuals as the point of integration of their own data	Today's system disperses individuals' data across many different organisational data silos. Individuals need to be able to aggregate any and all data about themselves in their own personal data stores under their control.
Citizen independence	Individuals should be able to collect, store, manage and control their own data independently of the organisations that originally collected or minted this data.
Layered, not siloed	Today's system is organised around multiple separate isolated data silos, each acting like moated data castles. For data to be shared we need a new 'data exchange' layer that enables data to be shared with and between individuals and organisations. Personal data stores can act as this exchange layer.
Increasing separation of data storage from use	In today's system, data storage is integrated with data use, with each organisation collecting and storing the data it needs to use. If the same data is to be used many times for many different purposes, data storage and use need to be separated out. Personal data stores enable this to happen.

Table 1: Architecture of the new personal data ecosystem

Today's data economy is organised exclusively around organisations, disperses citizens' data across many different organisations, excludes citizens from its workings (with organisations collecting and using data *about* them), operates via separate data silos that act like moated castles of data control, and integrate the collection and use of data behind these castle walls.

The new data economy will enable citizens to collect and use their own data (as well as organisations), make individuals the point at which data about themselves is integrated, and place this new data asset directly under the citizen's control. It will connect today's data silos via a new 'exchange layer' of personal data stores that enable citizen-controlled data sharing and increasingly separates the storage of data from use.

Design principles for the new data economy	
Infrastructure	
Secure	All data should be encrypted in motion and at rest.
Decentralised	Today's system centralises personal data into organisations' data silos that concentrate data power and attract hackers. With each individual able to store and use their own data using their personal data store, power and reward is distributed while hackers' incentives are reduced.
Citizens genuinely empowered	Under today's system, 'control' is restricted to giving or withholding organisations' permission to collect and use the individual's data. Personal data stores enable individuals to *use* their data for their own purposes: a different level of control.
Zero knowledge processes	Personal data store operators should not be able to see into individuals' personal data stores, which should be separately encrypted. Individuals should hold their own private key to their PDS, which the PDS operator does not have access to.
Technology agnostic, cloud based	Personal data infrastructure should not be tied to any particular technology, using any and all technologies that are fit for purpose. Nor should it be device-based, because the data needs to be retained when the device is replaced, lost or stolen. That means it needs to be cloud based.

Design principles for the new data economy	
Infrastructure	
Enabling	The job of the new personal data infrastructure is to make new and improved services possible, not to deliver these services (which is the job of domain experts). But to be truly enabling, the infrastructure has to address key issues such as security and interoperability, resulting in new decisions of labour.

Table 2: Infrastructure of the new personal data ecosystem

Today's organisation-centric approach to personal data use creates multiple separate data silos where data is concentrated in a small number of centralised databases. Citizens' control over their data is restricted to (often only formal) rights to consent to data collection and use. By the very way it operates it is privacy invading: organisations get to know a lot about the individuals they hold data on.

The new infrastructure is distributed, with multiple nodes (personal data stores) where individuals can exert real, direct control over their data. Because each personal data store is individually encrypted, with only the individual holding the key, it operates on a zero knowledge (rather than privacy invading) basis. It has a technology agnostic, cloud- based approach where PDS providers ensure key functions such as interoperability.

Design principles for the new data economy	
Governance	
Institutionalised trustworthiness	Trustworthiness cannot be reduced to an organisation's policy, which may be changed at any time (say, with a new owner). It needs to be institutionalised: built into legally enforceable rules, regulations, audit, accountability. That is why Mydex is a Community Interest Company
Neither market nor state	The new infrastructure cannot be state controlled, because that risks it becoming a political play thing. Nor should it be controlled by people seeking to maximise shareholder value, because that will distort its priorities. As enabling infrastructure it needs to be designed, and run, to benefit all.

Design principles for the new data economy	
Governance	
Neutral	The infrastructure and institution should work - and be seen to work - so that it never favours one group, or organisation over another. It needs to publish a consistent set of rules that everyone has to follow and which are enforced by the infrastructure platforms as it runs.
Legal basis	Current EU and UK data protection regulations make provision for data portability (e.g. Article 20 of GDPR and the UK Data Protection Act). This means citizens have the right to require service providers to provide them with electronic copies of data they hold about them. While some of these provisions may need further clarification, the legal basis for this approach to data sharing has already been established.

Table 3: Infrastructure governance in the new personal data ecosystem

The critical governance challenge is that trustworthiness cannot be reduced to an organisation's policy or promise: a policy that may change at any time or a promise that may be broken at any time. Commitments to ensure data security, privacy etc need to be permanent and legally enforceable, embedded in the constitutions of the institutions providing the data infrastructure. (This relates to the 'built to last' principle - see below).

In today's data ecosystem, many organisations seek to gather and use personal data for the purposes of competitive advantage. To achieve this, they restrict who has access to the data.. For infrastructure designed to empower and include citizens and to enable data sharing of wider, improved data use, while competition between different service providers can be as intense as ever, the data infrastructure needs to be neutral: it must be designed to enable *all* legitimate users, without favour.

Design principles for the new data economy	
Economic logic and business models	
Self-sufficient but not profit seeking	PDS infrastructure providers need to be financially self-sufficient - not dependent on others for their income, so that control over the purse strings does not turn into control over purposes. They should not be profit maximising either. As with all infrastructure the ideal cost of accessing it should be as close to zero as possible, not the highest margins possible.
'Cost out' focus	Today's business models focus on organisations monetising data either directly by renting or selling it or indirectly via enhanced service provision. The new data infrastructure focuses on helping *both* citizens and service providers reduce the friction, effort, risk and cost involved in accessing and using data.
Mission-aligned incentives	PDS infrastructure providers should design their funding and business models so that they are incentivised to sustain and further their purposes - not undermine or game them. For example, they shouldn't have any financial incentives to encourage citizens to sell or share their data unnecessarily.
Built to last	PDS infrastructure providers should be designed to serve individuals over their complete lifetimes and should have legal guarantees of continuity of purpose built into their constitutions. Business models focused on achieving an 'exit' where the organisation's ownership - and purpose - may change at any time are incompatible with this.

Table 4: Economic and business models underlying the new personal data ecosystem

To sustain themselves in a way that maintains and fulfils their function, personal data store providers need to be able to cover their costs. This ensures their independence from external parties who may wish to use control over the purse strings to exercise control over purposes. Because the purpose of this infrastructure is to enable others' actions rather than to make and sell a specific 'product', its prime economic logic and benefit is 'cost out' rather than 'added margin'. All its financial and economic incentives need to be designed to ensure this sustainability, neutrality and mission alignment.

A key part of this is continuity and longevity: a personal data store is for life, so the institutions providing personal data stores should be designed for decades (centuries, even). Whatever particular corporate form they take, legal safeguards relating to continuity and longevity of purpose need to be built into how they operate.

The key design principles explained

The following commentary, based on a talk given by Mydex in Korean in May 2022, explains the logic and reasoning behind the design principles outlined above.

Why we need a new system design

Today, we have an organisation-centric, One User, One Use or 'OUOU' personal data system. Organisations collect data about individuals, and they use this data for their particular organisation's purposes - with each organisation collecting and using its own data for its own purposes.

This OUOU approach is a product of technological and institutional history and it has brought many benefits. It is how services are delivered today. But it also has limitations and creates problems.

Because our current system is organisation-centric - built around organisations collecting and using individuals' data - citizens are excluded from participating in its workings. They don't have any real control over their data. They aren't able to access or use their own data for their own benefit. The system is increasingly seen as not safe, and not fair.

Meanwhile, organisations lack access to the data they need or face high costs and hurdles trying to access it. That's because, no matter how much data any single organisation manages to assemble, there is always far more data about its customers that lies beyond the organisation's boundaries - data held closely by other organisations.

Quality issues abound. Organisations spend a lot of time and money (too much time and money) trying to make sure that the data that they collect is correct, complete, up-to-date and reliable.

And across the system as a whole, because each organisation is undertaking the same tasks relating to its data in parallel to all other organisations, there is immense duplication of effort. Everyone is collecting, storing and processing large quantities of basically the same data, many times over. Which means that across the system as a whole, costs are many times higher than they should be.

In addition, because each organisation is jealously guarding its own data behind its own firewalls, and because other organisations cannot access and use this data, economic growth and innovation is being restricted.

On top of this, because citizens lack control and are not benefiting as they should from their data, levels of trust across are very low. That also restricts innovation and growth. For all these reasons we need a system redesign.

From 'OUOU' to 'MUMU'

Because data does not get 'used-up' when it is used; because the same data can be used by many users for many different purposes; the underlying logic of data creates the need for a different 'MUMU' data ecosystem of Many Users, Many Uses of the same sets of data.

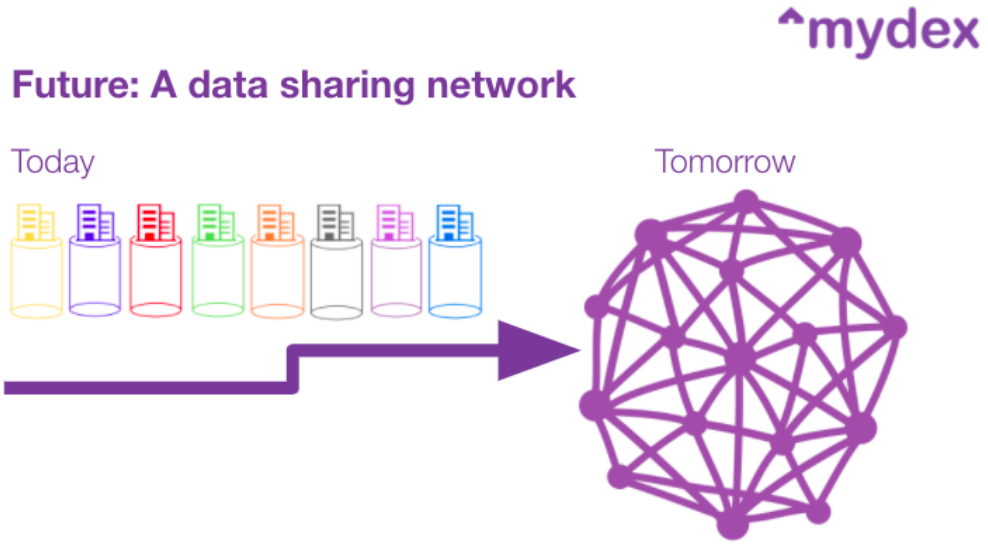

Figure 2: From separate data silos to integrated data networks

Today's data ecosystem is made up of many different, separate data silos, with data trapped inside each organisational silo. This blocks 'MUMU'. To unleash the full potential of data - including personal data - we need to move from many separate data silos to a single data sharing network, where each node in the network can access the data it needs to add the most value.

To do that we need a new data architecture and infrastructure - a ***data logistics*** infrastructure capable of getting exactly the right data to and from the right people and organisations at the right times.

The big question is: how best to do this?

A new data logistics infrastructure

For the past 15 years, we at Mydex have been building a new citizen-centric data logistics infrastructure that opens the door to MUMU - to Many Users, Many Uses. Figures 3 and 4 show how it works.

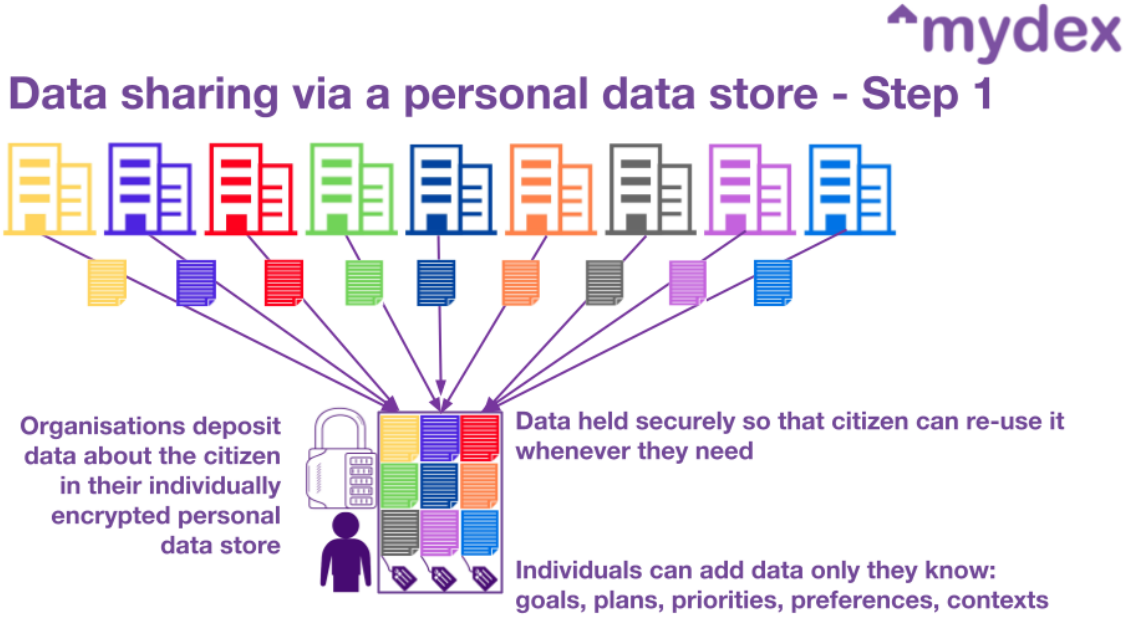

Figure 3: How PDS based data sharing works - step one

Organisations holding data about individuals provide them with copies of this data, verifying details about them via a cryptographically secure token that cannot be tampered with. Individuals hold these verified attributes or credentials in their personal data store where they retain control over this data. Each personal data store is separately encrypted and each individual holds their own private key to their personal data store. This puts them in control of their data and ensures their safety, security and privacy.

Individuals can add more data to their personal data store if they wish to, including data that only they know. Data about their plans, goals, priorities, preferences and so on.

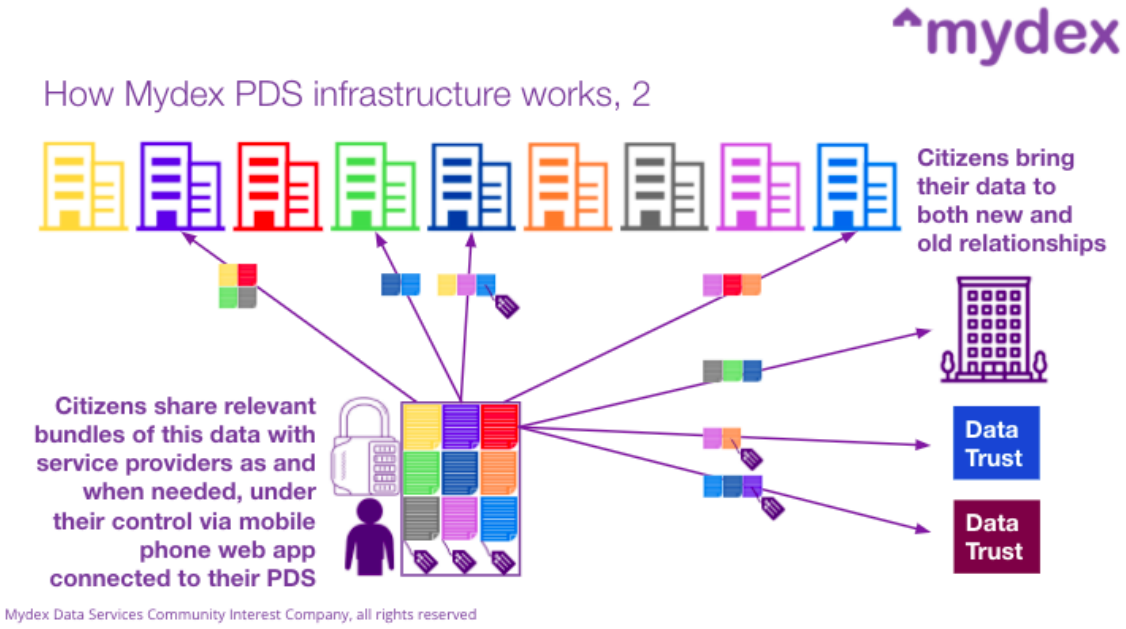

Figure 4: How PDS-based data sharing works - step two

Individuals can then share this data with service providers as and when needed. They may share extra data with service providers they already have relationships with. Or they may bring their data to completely new service providers. That's up to them.

It can be a huge amount of data. What's needed for an important decision about a complex matter in, say, health or finances. Or it could be a tiny amount of data, simply verifying a few details as a next step in a user journey. It doesn't matter. What matters is that exactly the right information is passing to and from the right people and the right organisations at the right time.

Benefits

This new data logistics infrastructure has the ability to transform relationships between individuals and service providers. Figure 5 summarises the main benefits, which are comprehensive and apply to both citizens and *bona fide* service providers. It is now very difficult for non-*bona fide* operators seeking to access individuals' data.

Figure 5: The design principles address all main uses of personal data

The benefits cover all major uses of data for *both* service providers and individuals:

- analytics and decision-making
- assembling components to create solutions and improving coordination between multiple service providers to deliver better quality services
- improved productivity and efficiency,
- improving the processes of matching supply to demand and suppliers to users
- enabling the innovation of new-to-the-world person centric services
- enabling the delivery of social benefits
- enabling the identity assurance that underpins them all.

In particular, service providers benefit greatly if individuals can bring safe, reliable, pre-checked information (verifiable credentials) with them to the relationship. These benefits include:

- Increased access to richer, more reliable data
- Reduced costs of collecting, checking, processing and using personal data
- Improved service quality and timeliness
- New dimensions of innovation

The new person-centric data ecosystem therefore creates better outcomes, reduces friction, effort, risk and cost for citizens and for service providers too, and generates new opportunities for innovation.

Great in theory …

But there is an 'if' and it is a very big 'If'.

These benefits can only be realised if the new ecosystem is implemented the right way. And over our 15 years' experience we at Mydex CIC have learned there are many ways to get it wrong. So what is the right model for implementation? When it comes to system architecture, infrastructure, governance, economic logic and business models, what design principles should we adopt?

System architecture

Organisation or person-centric?

The pivotal question that sets the direction for everything else is: should our approach be person-centric or organisation-centric?

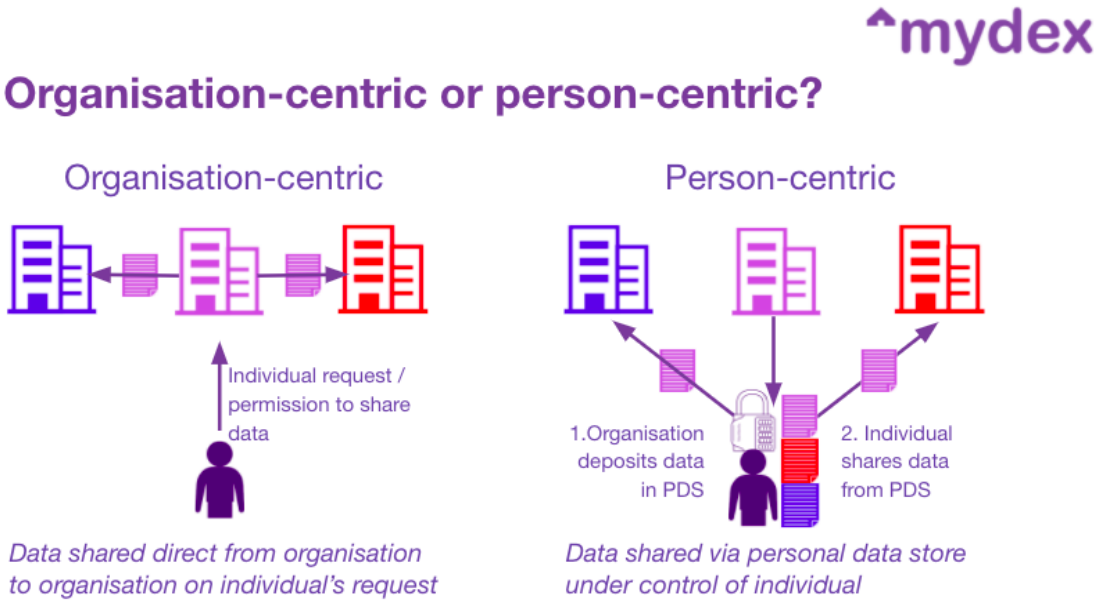

Figure 6: Two alternative ways of sharing personal data

Figure 6 illustrates two alternative ways of sharing personal data. The first approach, on the left of the diagram, is the organisation-centric approach, individuals request or give permission to one organisation holding data about

them to share some details with other organisations. The data flows directly from organisation to organisation, without the individual ever handling it and probably having no record of the transaction. This is the approach currently adopted by the UK with its Open Banking initiative.

The right hand of the diagram illustrates the person-centric approach. Here, organisations deposit details about the individual in the individual's personal data store, under the individual's direct control. The individual then shares this data with other organisations as and when needed. They have their own records of what data is shared for what purpose. They have their own proofs.

Looking at it from the perspective shown in this diagram, the organisation-centric approach seems simpler and easier. Why bother inventing a completely new entity - the personal data store provider - and a new layer of infrastructure, with new steps to the process when you don't need to?

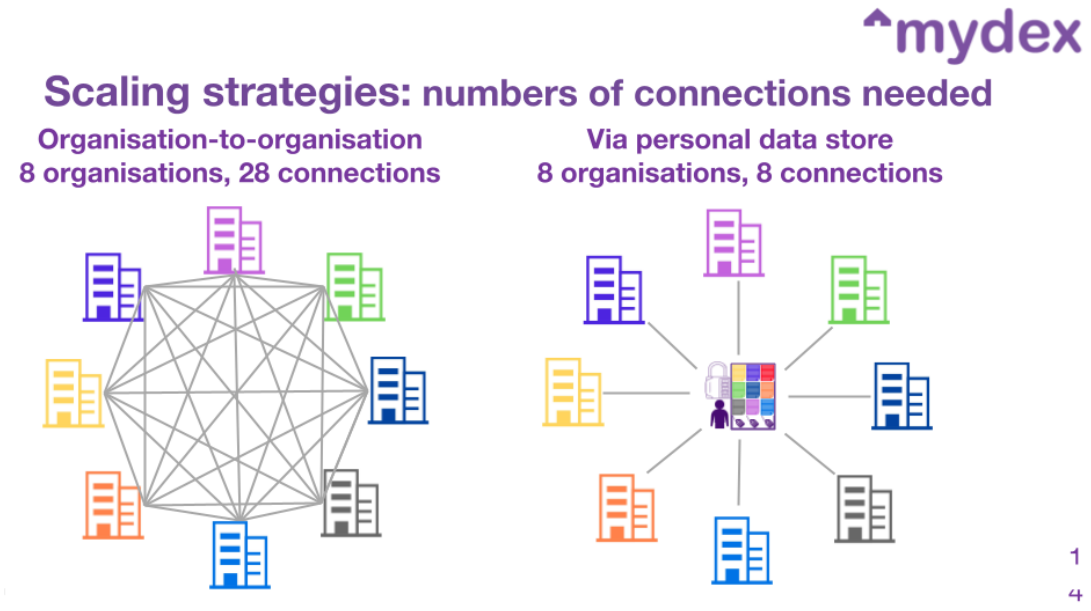

Figure 7: How the organisation-centric approach to data sharing creates a complexity catastrophe.

The reason is that the organisation-centric approach does not scale. As more data gets shared between more organisations - it gets more and more complex. Figure 7 illustrates the situation looks like if just 8 organisations are involved in accessing the same individual's data. The number of connections between organisations jumps to 28, if organisations are directly sharing data with each other. But if data is flowing via the individual's personal data store, the number of connections that are needed rises to just 8.

Each time a new organisation starts sharing data, the number of potential connections between organisations grows exponentially. By the time 100 organisations are involved (which is about the number of data relationships each individual has with different organisations) the potential number of connections needed in the direct organisation-to-organisation model of data sharing rises to 4950. This is 50 times more complex, cumbersome and expensive, generating a cost, security, interoperability and trust catastrophe whose detailed workings are explored in this blog.

While the organisation-centric approach to the sharing of personal data can work for a few specific, limited use cases, any long-term strategic approach based on organisation-to-organisation data sharing, can only result in a strategic dead-end. A person-centric approach where citizens are empowered with their own personal data stores and data sharing tools is the way forward.

Individuals as the point of integration of data about them

A second architectural design principle is that individuals should become the point at which data about themselves is integrated. With the current system, data about individuals is dispersed across many different organisations - probably over far more than 100 organisations for each individual. That means it is practically impossible to build up a rich, complete data picture of an individual, without engaging in the biggest invasion of privacy ever.

But if individuals are able to aggregate data about themselves and their lives in their own personal data stores, it is possible to build these new, rich, person-centric data assets - ***data assets that are impossible to create under today's siloed, organisation-centric data architecture.***

As the new ecosystem beds down, service provision and innovation will increasingly revolve around these new person-centric data assets, precisely because they will be richer, more complete and more useful than any data set that any individual, separate organisation's data silo can build. However, if an organisation-centric approach to data sharing is adopted, the innovations and services that these new person-centric data assets make possible will never happen. The full potential of data-driven innovation will be stifled.

Citizen independence

A third architectural design principle is that individuals' data should be stored, managed and controlled independently of any particular organisation.

If any organisation can dictate to individuals who they can share their data with, for what purposes - or if any particular organisation hosts this personal data in its own systems or under its control - then data sharing risks turning into a new frontier of inter-organisation competition with new levels of privacy invasion.

Therefore a core design principle for a strategically viable personal data ecosystem has to be that individuals can collect, store, manage, use and share their own data independently of the organisations that originally collected, generated or used this data.

Layered, not siloed

As Figure 7 illustrates, today's organisation-centric approach to data is based on multiple separate data silos, where each different, separate organisation collects *and* uses its own data in isolation to all other organisations. But the data logistics infrastructure described in this Paper builds connections between these silos via individuals' personal data stores.

As a result the new system has (at the highest level), three key functional layers:

1. Organisations that originate data about individuals in the first place
2. Personal data stores that enable individuals to collect, receive, aggregate and store copies of this data and to share it
3. Service providers (who may be the same as the originator-organisations) accessing the data held in these personal data stores in order to provide services.

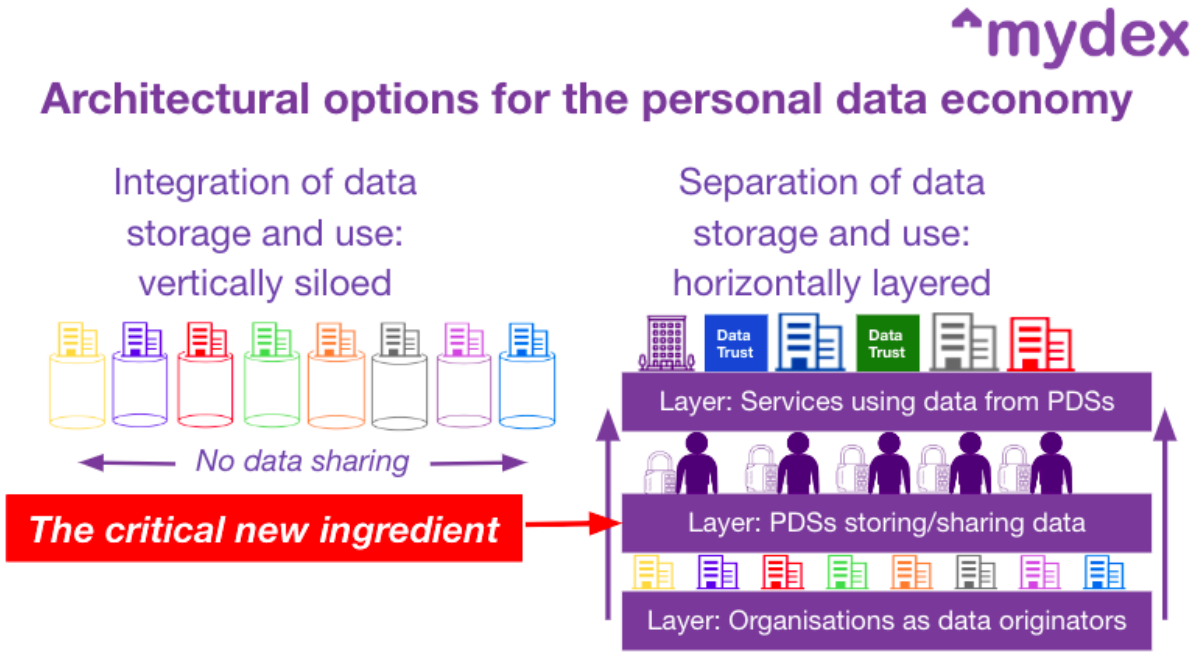

Figure 8: A new era of person-centric data sharing infrastructure enables separated data silos to share data safely and efficiently

Figure 8 illustrates this shift from 'siloed' to 'layered'. The design principles discussed in this Paper relate mainly to the middle layer of personal data store infrastructure - the layer that does the connecting; the data logistics. Within this, the activities of the other two layers of data originators and data users may remain surprisingly unchanged (except for the fact that they have a new type of data sharing relationship with their customers and have easier access to better data at lower cost).

Separation of data storage from use

Introducing new functional layers into the architecture of the personal data economy also requires new divisions of labour. As we shift from silos to layers, we also move from integrating data storage and use to the increased ***separation*** of data storage and use, with service provider accessing personal data, with individuals' permission, on an 'as and when needed' basis. That's what specialist infrastructure suppliers such as Mydex CIC do: increasingly take on the jobs of data storage and data sharing so that others don't have to.

It is this increasing separation of data storage and use that enables individuals to become the point of integration of their own data: that makes new, hugely powerful citizen-centric, citizen-controlled data assets possible.

Enabling infrastructure

For the above architecture to work, its new layer of data logistics infrastructure needs to operate according to fit-for-purpose design principles.

Decentralised and distributed

With the current organisation-centric approach to data collection, each organisation holds personal data in its own, big, centralised database - big centralised databases that inevitably become a target for hackers. With the person-centric approach, each individual personal data store needs to be separate: not one, new, huge database of individuals, but millions of separate personal data stores, each one separately encrypted, under the control of the individual whose data it is.

Genuine citizen empowerment

The infrastructure also needs to deliver *genuine* citizen empowerment. This goes beyond just having a say ('voice'), having a 'choice' between accepting or not accepting a set of terms and conditions), and 'exit' (having the ability to go to a different provider). All of these things are important. But they are nothing without the ability to *specify and act*.

Currently, there is much damaging confusion today surrounding the idea that citizens should be able to exercise 'control' over their data. This word 'control' can be used to mean two opposite things:

- Control over data held by an organisations *OR*
- Control over data held by citizens themselves where they are able to collect, store, and use their own data for their own purposes in their own personal data store.

As a parallel, the difference is between being allowed to ride in a taxi but not being allowed to own your own car. Genuine citizen empowerment means being able to own your own car and being able to drive it wherever and whenever you want. This level of genuine control is essential for the new ecosystem to succeed.

Zero knowledge processes

Genuine consumer empowerment means that PDS providers like Mydex CIC should not be able to see into each individual's personal data store. If they did, they would become a new source of privacy invasion themselves.

Personal data store providers should not be able to look into or exert any control over the data individuals hold in their personal data store or what they do with it. This data is the individual's data, not an infrastructure provider's data. That is why with Mydex, each individual holds their own private key to their data store, which Mydex does not know and does not hold. Even though Mydex hosts the data store itself, only individuals can access and control its contents and who can deliver data or collect data from it.

Technology agnostic, cloud-based

A further consideration is which tech solution to adopt. Some people think that new solutions such as distributed ledger or blockchain technologies are a magic bullet that will solve all our problems. They won't. Like all technologies, they are good for some things and bad for others. The new personal data infrastructure should be technology agnostic, choosing whichever technology solutions do the job best.

Other people argue that the best solutions are device-based because if the data is held by the device, the individual's data is much better protected. But devices can get lost or stolen, and they all have to be replaced in the end. If the individual's data gets lost or stolen or dies with the device, it's a disaster. The data needs to be backed up, and the cloud is the place to do it. So it is best to run things in the cloud, using devices that interact and sync up with it.

Mobile devices are brilliant for making access to personal data stores easy and for creating user interfaces where they can exercise control. But technology agnostic, cloud-based solutions are the only strategically viable way forward to ensure lifetime storage of data and always-on access over secure connections.

Necessary functionalities and divisions of labour

PDS infrastructure providers need to provide all the functionality needed to fulfil their role. For example, they must work to the highest standards of data security at all times, designing their systems to minimise risks to data security. They must enable comprehensive interoperability. Services depositing data in a personal data store or receiving data from one should not have to worry about which systems, formats or standards they are using. Translations between them should be handled by the infrastructure provider (a significant task).

In addition, infrastructure providers need to attend to the multiple details that are needed for their service to work smoothly and efficiently. For example, trust needs to be portable so that a service provider can deposit a tamper-proof token verifying information about an individual in their PDS and other service providers can use this token. The infrastructure provider needs to provide the systems that enable this to work.

Governance

Trustworthiness must be institutionalised

For the right infrastructure to work well, it needs to be governed properly, the key requirement with personal data being trust. The level of trustworthiness needed for the ecosystem to work means it cannot just be a marketing slogan. It needs to be institutionalised: built into rules, regulations, audit, accountability, It needs to be enforceable - so that everyone can see it working.

That is why Mydex is a Community Interest Company under UK law. A Community Interest Company is a business which acts like any other business - disciplined, commercial - but which uses its business skills to pursue a social mission. In our case, our mission is empowering citizens with their own data.

It is a legal requirement of our Community Interest Company status that if we make any surplus, two thirds of it must be reinvested in furthering our mission.

Mydex does not exist for shareholders. It exists for citizens. That's not a slogan. It is built into its legal status. All specialist PDS infrastructure providers must have legally enforceable trustworthiness built into how they operate.

Neither market nor state

Trustworthiness raises important questions about the incentives by which infrastructure providers operate. When it comes to provision of personal data infrastructure they should not work either under direct state control or as traditional profit-maximising free market operators.

With state bodies, there is a high risk that the state will start using access to citizens' data for state and political purposes. The mere fact that this risk is present could be enough to undermine citizen trust in the institutions concerned. With market actors, the risk is that they will prioritise profit maximisation and shareholder value above serving and protecting citizens.

Building fit-for-purpose PDS infrastructure might therefore require a degree of institutional innovation - the invention of new types of institutions that are neither state or market controlled. Community Interest Companies. Trusts. Foundations. Cooperatives. There are many different ways of doing this, but it needs to be done.

Neutral, enabling operations

The infrastructure and institution should work - and be seen to work - so that it never favours one group or organisation over another. It cannot be seen to be allowing some organisations access to its platforms, but not others. It cannot charge some organisations more for access than others; or favour the competitive advantage of one organisation over another. It needs to publish a consistent set of rules that everyone has to follow and which are enforced by the infrastructure platforms as it runs.

Its job is to protect and serve the citizens and enable trustworthy data sharing to happen. Full stop.

The new EU Data Governance Act has already recognised this, saying:

> "A key element by which to increase the trust and control of data holders, data subjects and data users in data intermediation services is the neutrality of data intermediation services providers with regard to the data exchanged between data holders or data subjects and data users. It is therefore necessary that data intermediation services providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose.

> "Data intermediation services providers that intermediate the exchange of data between individuals as data subjects and legal persons as data users should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data subjects."

Regardless of Brexit, these principles are correct. They now need to be implemented.

Legal basis

For a new personal data infrastructure to work it must have a solid legal basis. The UK Government is currently considering new legislation to make it possible for organisations to share data with each other, perhaps without individuals' consent. But there is another, simpler, legal basis for the new personal data ecosystem discussed in this paper.

Article 20 of the EU's General Data Protection Regulations and the UK's Data Protection Act provide for data portability. The Article states that:

> "The data subject shall have the 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."

There may be some wrinkles that need clarifying: what exactly does "which he or she has provided" mean? But the essence of it is there already: individuals have a right to receive, and to share, copies of data held out about them by organisations 'without hindrance' from the original data controller.

This provides a solid basis in law for the new data ecosystem - one that focuses on extending and enriching existing relationships between service providers and individuals and that doesn't create the need for new types of relationships between organisations that otherwise have nothing to do with each other.

Economic logic and supporting business models

PDS infrastructure providers' business models need to support rather than undermine the right architecture, infrastructure and governance. This generates some key design principles that relate to their financial operation.

Self-sufficient but not profit-oriented

Infrastructure providers need to be financially self-sufficient - not dependent on others for their income, so that control over the purse strings does not turn into control over purposes.

The other side of this coin is that they should not be profit maximising either. Whatever infrastructure we are talking about - roads, electricity, internet broadband - the ideal cost of accessing such infrastructure is as close to zero as possible, not the highest margins possible, because that is what maximises access and use.

Cost out focus

Achieving infrastructure costs as close to zero as possible requires a mindset and operational priorities that are very different to many of today's business models which focus on organisations monetising data, either directly by renting or selling it or indirectly via enhanced service provision.

When PDS infrastructure providers enable citizens to bring pre-verified data with them to service providers, the main economic contribution is to reduce friction, effort, risk and cost for both citizens and service providers when accessing and using data.

It's not about making a margin on the trading or sharing of data. It's about enabling system-wide cost reduction; an economy-wide leap forward in productivity and efficiency.

Mission-aligned incentives

PDS infrastructure providers should design their funding so that they are incentivised to sustain and further their purposes - not undermine or game them. For PDS infrastructure to work, it needs neutrality about data sharing and to be citizen empowering. So it should not have any incentives to encourage citizens to sell or share their data unnecessarily (by, for example, earning a fee every time data changes hands) or charge different fees for different data.

That is why Mydex CIC charges fees for organisations to connect to its platform, to enable data sharing - fees that are neutral about how much data is shared with who. These charging structures reflect Mydex's job, which is to enable, not to intervene in favour of special interests.

Built to Last

Perhaps most important of all, PDS infrastructure providers need to be designed to last - not for sale. Individuals start accumulating data about themselves before they are born, and they continue to generate data about themselves after they die. The infrastructure that serves them should therefore be designed to serve them for their whole lives and beyond.

Is it possible for a business set up by investors with an eye to a profitable 'exit' to deliver this continuity and longevity? We don't think so. Legally enforceable safeguards need to be introduced so that, if ownership or control of a PDS infrastructure provider changes hands, the new owners/controllers cannot simply change its fundamental purpose and (for example) start monetising the data that has been accumulated.

This last design principle represents a fundamental challenge to the assumptions behind most current status quo visions of what a successful business looks like. But that is one of the effects of this transformation: it extends much deeper and much further than many people first realise.

Conclusion and Questions Arising

This White Paper has outlined design principles which are necessary if the new personal data economy is to work safely, efficiently and effectively.

The new citizen-empowering data sharing infrastructure described in this Paper will enable our economy and society to unleash the full personal, social and economic benefits of personal data. It does this by enabling a shift from the operating to the principle of One User, One Use (OUOU), to a citizen-centric system of data sharing that operates to the principle of Many Users, Many Uses (MUMU). To achieve this, it also needs to shift from an organisation-centric system of data collection and use to a person-centric one.

If the wrong design principles for the sharing and use of personal data are adopted, we risk the opposite:

- An inability to achieve system wide progress
- An inability to unleash the full potential of personal data
- And loss of public trust as faulty designs make new abuses possible and likely.

We have the opportunity to make immense progress to the benefit of all. But to do so, we need to get the details - the design - right.

These design principles do not represent a complete answer. Indeed, they raise other important knock-on questions, including:

- Is it really worth the bother? Just how big are the potential benefits of doing this versus not doing it?
- How exactly are these changes going to happen?

These are subjects which we will explore elsewhere. But the simple answers to them are:

1) Yes, the potential benefits are definitely worth it and
2) change like this never happens as an overnight flip from one state to another. It evolves, starting at the edges and growing towards the mainstream.

And that is already happening.