MyData

MyData in Motion: Evolving Empowerment for 2025 and beyond

Fourth edition (fully revised 2025)

AUTHORS

Alex Bowyer
Viivi Lähteenoja
Christopher Wilson

WITH THANKS FOR REVIEWS AND INPUT TO

Henrik Biering
Tim Davies
Kai Kuikkaniemi

WITH THANKS TO THE CO-AUTHORS OF EARLIER EDITIONS

Antti Poikola
Kai Kuikkaniemi
Ossi Kuittinen
Harri Honko
Aleksi Knuutila
Viivi Lähteenoja

Contents

Foreword from the Ministry of Transport and Communications

The world of 2025 is undergoing a profound data-driven transformation amid growing global uncertainty. The rapid rise of artificial intelligence brings vast opportunities — but also risks undermining our ability to ensure these opportunities are used ethically and fairly. The right to control one's own data has never been only an individual issue; it is part of the democratic order we must actively uphold.

The first MyData whitepaper, published in 2014, introduced a human-centric vision for the data economy. In the decade since, it has grown into an international organization and global movement embedded not only in European digital policy — from GDPR to data governance — but also in emerging frameworks across the world. This confirms that human-centricity is a shared global answer to the trust challenges of digital society.

The core principles of MyData — human-centricity, trust, and transparency — are more vital than ever. Seeing individuals as integration points for data redefines how we build infrastructure: embedding agency into design allows for innovation that is both ethical and resilient.

This approach also supports small enterprises and protects data used in AI training, by ensuring respect for the rights of individuals, other data holders, and content creators — including intellectual property. Data sovereignty, then, is not only about individuals, but also the autonomy of businesses and nations in a shifting digital landscape.

The EU's upcoming Data Union Strategy will lay out a roadmap to complete the internal data market and seek answers to global governance. It is more than an economic initiative — it is a rights-based infrastructure vision. But strategy alone won't suffice. We need commitment, demand, and viable business models to activate this vision — linking data spaces, interoperability frameworks, and tools like eIDAS wallets into a seamless ecosystem that empowers rights-holders to act.

As we mark the tenth anniversary of MyData, I extend my congratulations and gratitude to everyone who has contributed — and renew invitation to continue building a future where data serves not only markets, but people, digital communities, and our shared planet.

Maria Rautavirta
Head of Data Policy
Ministry of Transport and Communications, Finland

Preface

The dawn of the 21st century heralded an era of unprecedented digital optimism. The internet, still in its adolescence, promised to act as the great leveller, democratising information, offering global communication and audience-reaching capability to all and empowering individuals globally. Early platforms emphasised connection and sharing, with social media emerging as a tool for grassroots movements and democratic participation.

By 2010, this landscape began shifting dramatically. Major tech platforms discovered the immense value of personal data, transforming casual digital interactions into profitable datapoints. The platform economy took shape, with companies like Facebook, Google, and Amazon consolidating their power through sophisticated data collection and analysis capabilities. Subscription models and walled gardens backed by big data capability became the dominant way to offer digital services online, at great cost to user experience and individual agency.

It was in this context that the MyData movement emerged in the early 2010s. Beginning in Finland through Open Knowledge initiatives, MyData represented a response to growing concerns about digital power imbalances. The movement's original 2014 whitepaper, developed with the Finnish Ministry of Transport and Communications, articulated a vision for human-centric data management that would influence European policy for years to come.

The period from 2015-2020 marked a turning point in public consciousness. High-profile data breaches, election interference scandals, and growing awareness of surveillance capitalism led to increased scrutiny of tech platforms. The EU's GDPR in 2018 set new global standards for data protection, while the establishment of MyData Global that same year created an international framework for advocating individual data rights.

The years 2020-2025 brought unprecedented challenges and technological acceleration. The global pandemic catalysed digital transformation across sectors, while advances in AI and machine learning further complicated the data landscape. Generative AI and large language models emerged as transformative technologies, blurring traditional distinctions between personal and non-personal data.

By 2025, the data economy stands at a critical juncture. New regulatory frameworks like the EU's Data Act and AI Act attempt to govern an increasingly complex digital ecosystem, but there is an increasing need for better enforcement and regular updating of those rules which slow-moving political forces struggle to meet. The MyData movement, while influential in policy discussions, grapples with fundamental questions about individual empowerment in an age of AI and automated decision-making.

This evolution reflects broader societal challenges: the tension between technological innovation and human rights, the balance

between individual privacy and collective benefit, and the ongoing struggle to ensure digital technologies serve democratic rather than authoritarian ends. The path forward requires careful navigation of these competing interests, with frameworks like MyData offering potential solutions for a more equitable digital future.

This fourth, updated edition of the MyData White Paper asks provocative and fundamental questions to the MyData community and the global community writ large about what this means, and how empowering people with control over their data can help to create the better, more fair and flourishing digital society to which we aspire.

1. What's at stake with data in 2025

In 2025, data is not just the oil that fuels our modern economy,[1] it is the fundamental material through which we experience, understand and function within society. Since the emergence of MyData thinking in 2014 and the formalisation of the MyData Global organisation in 2018, digital platforms have become the dominant mechanism for interacting with the world. The ability to access, harness, control and disseminate information derived from our data gives tremendous power - the power to influence populations, transform current markets and business models and shape the algorithms, infrastructures and laws that will determine how we live in the future. It is critical therefore, that societies, companies and institutions use data in a conscious, responsible way that serves humanity's interests and builds a society where individuals can flourish and businesses can compete in an ethical, competitive and fair digital landscape.

We face a critical disconnect between data's societal importance and our current approach to managing it. Data-driven systems are currently designed to optimise wealth generation and are shaped much more by market forces than by individual and societal needs. The largest technology companies use their power and influence to build ever-larger data repositories that fuel algorithmic decision-making in their own interest, securing market dominance. Meanwhile, individuals lack basic visibility into, understanding of, and control over their own digital existence.

This imbalance isn't just a matter of privacy – it represents a fundamental challenge to human agency, economic fairness, and democratic values.[2] The rapid acceleration of AI technologies and data-driven business models has made addressing these issues more urgent than ever, as the gap between data's potential benefits for society and its current implementation continues to widen.

The stakes couldn't be higher: our failure to establish human-centric data governance now risks entrenching systems that concentrate power in the hands of a few, suppress innovation, and limit our collective ability to harness data for societal good. As data increasingly becomes the lens through which we view and solve global challenges, ensuring its ethical, transparent, and equitable management isn't just a technical necessity – it's a crucial step in preserving human dignity and empowerment in our digital age.

1 The Economist, "The World's Most Valuable Resource Is No Longer Oil, but Data," May 6, 2017, accessed March 22, 2025, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

2 World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (Geneva: World Economic Forum, 2014), accessed March 22, 2025, https://www.weforum.org/publications/rethinking-personal-data-trust-and-context-user-centred-data-ecosystems/.

1.1. Visible and invisible, data is everywhere

In today's digitally interconnected world, data permeates every aspect of our lives. From the moment we wake up to the time we go to sleep, our actions, choices, and interactions generate a vast amount of information that is captured, stored, and analysed by an intricate and unseen network of digital systems and organisations.

We deliberately create some of this data, by filling out forms and entering credit card information for online purchases. Other data is generated unconsciously and captured as we go about our lives online and offline, as our searches, purchases, web traffic, and social media interactions are tracked, and as we use our devices, services and products that are connected to the internet and send data 'back to base'.

There is also an unknown[3] but significant amount of data about us that does not come from us, as third parties create and assemble datasets based on our demographic profile or groups we belong to, in order to sell us things or to make decisions that impact how we live our lives.

As this table updated from our "In This Together" paper[4] shows, we can consider three categories of data – 'data from me', 'data about me', and 'data that impacts me'.

Data from me	Data about me	Data that impacts me
Data that is actively provided or generated by an individual.	Data that relates to an individual, but that was collected or inferred by a third party.	Data with implications, associations, and consequences for an individual.
Examples		
Social media posts; address information provided when signing up for a service; and fitness data from a smartwatch.	The inferred interests profile that is created by platforms for advertisers; health records made by the doctor; and ratings of a gig worker.	Wastewater monitoring that is used to decide on health lockdowns; aggregate transport data that is used to plan transit infrastructure; and data that is gathered and used to train LLMs.

TABLE 1. Three categories of data.

Much of the data from us and about us is hidden in plain sight. We know that the ads served to us online are a direct reflection of our internet activity, and that loyalty programmes are designed to sell us more by tracking what we purchase. We understand at some level that using an app for public transit implies that our transportation patterns

3 Studies such as Sitra's #digipower project have begun to investigate this hidden world of third party datasets, but more research is needed and no-one has the full picture. See Jessica Pidoux, Jacob Gursky, Alex Bowyer, and Paul-Olivier Dehaye, Understanding Influence and Power in the Data Economy (Zenodo, 2022), accessed March 22, 2025, https://doi.org/10.5281/zenodo.6554156.

4 MyData Global, In This Together: Pathways for a Human-Centric, Fair Data Economy (Helsinki: MyData Global, 2021), accessed March 22, 2025, https://mydata.org/publication/in-this-together/.

are tracked and analysed, or that our electric or insurer-tracked vehicles are collecting information about how we drive. We even intuit that our maps applications send speed and traffic information in the background, and we may well appreciate this because we know that it enables that same application to warn us about traffic jams and suggest alternative routes.

The convenience and smooth execution of many data interactions make the fundamental extraction of data about us easy to disregard, and the constant and ubiquitous nature of such extractions easy to forget. Even for the most privacy and data-conscious of us, it can be hard to come to grips with the number of times each day we willingly or implicitly consent to our data being taken, stored, and used in ways that we do not understand.

There is also a significant amount of data that is completely invisible and inaccessible to us, even when it is about us and impacts us. The news is filled with regular revelations about data collection practices that have overstepped. There are no formal mechanisms for determining how data about us is shared, sold, or merged with other data (about us) to create new data (about us). Data from satellite imagery, waste-water quality monitoring, or economic reporting might not be about us as specific individuals, but can directly impact our lives when used to make decisions about land rights, lockdowns, infrastructure development, or the local allocation of public resources. This type of data might be profoundly important for us, yet we have no way of knowing how to engage with it, or that it even exists in the first place.

1.2. The power of data is immense

Data is one of humanity's most powerful tools, shaping decisions from the mundane to the monumental. Every click, purchase, and sensor reading creates information that can illuminate patterns and possibilities we might otherwise miss. Medical researchers use vast patient databases to identify promising treatments and spot early warning signs of disease. Urban planners analyse traffic flows and energy usage to build more livable cities. Farmers leverage soil and weather data to grow food more sustainably.

Yet, this same power to collect and analyse information can also be wielded in ways that harm individuals and communities. Surveillance systems track people's movements without their knowledge or consent, in service of commercial or authoritarian agendas. Algorithms trained on biased historical data can perpetuate discrimination in lending, hiring, and criminal justice. Social media platforms harvest personal information to manipulate behaviour, amplify division and consolidate power. The data itself doesn't choose these applications – people and institutions do.

Like any transformative technology, data is shaped by the values, goals, and power structures of those who control it. A temperature reading from a weather station is neutral; how that reading is used – to help communities prepare for extreme weather,

or to deny climate change to serve a political agenda – reflects human choices. The key question isn't whether data is good or bad, but rather: Who gets to collect it? Who can access it? How is it analysed and applied? And most importantly: Who benefits, and who bears the costs? As we navigate an increasingly data-driven world, we must actively work to ensure this most powerful resource remains in our control, and serves the common good rather than reinforcing existing inequities.

1.3. Data, and therefore power, is not equally or fairly distributed

The ubiquity and invisibility of data in our daily lives have created a massive imbalance of power between individuals and the organisations that collect and control data about us. This asymmetry stems from the fact that organisations have the sole power to collect, trade, and make decisions based on people's data. Individuals are at best able to decline consent or seek formal redress for legal violations according to complicated data protection regimes, if they have the resources to do so, and know about violations in the first place.

Individuals–our actions, interactions, preferences, behaviour and productivity–remain the lifeblood and well source of today's data economy. It is upon those who are least powerful that the entire data economy relies, and who benefit the least from the value that the data economy creates.

This is problematic in principle because data has become such a crucial resource in contemporary life, driving innovation, economic growth, and societal transformation.

It is also problematic because it risks harming and marginalising individuals, and represents a tremendous opportunity cost by stifling innovation and value creation for people, businesses, markets and societies.

As individuals become increasingly detached and dissociated from their data, their digital literacy suffers, negatively impacting access to opportunities, and risks further marginalising the already digitally marginalised. Lower levels of data awareness and literacy also inhibit individuals' ability to safeguard themselves against digital threats. A siloed database underpinned by disempowered masses is a world in which digital crime flourishes.

The opportunity cost of this power imbalance is profound. The contemporary market logic of data exploitation is premised on data control by a small number of businesses and organisations, often enjoying market incumbency. This has resulted in a siloed data economy of walled gardens and hidden transactions, in which both individuals and new market entrants are excluded. By disempowering individuals to the benefit of large organisations, we obstruct the innovation and value creation that could follow from the free flow and control of people's data, dictated by the needs of individuals (to exert their own rights, preferences, and protect their own well-being) and of

society (to ensure fairness, democratic integrity, and the unencumbered sharing and harnessing of human knowledge).

These dynamics have been long recognised,[5] but have a new urgency in the context of emerging technologies like Artificial Intelligence. The increasing uptake and application of generative AI and large language models blurs the lines between personal and non-personal data, while simultaneously making the machinations of data use even less visible, and raising radical expectations about the potential promises and threats of data for businesses and society.

1.4. The evolving landscape: business, policy, technology, and society

The urgency of the MyData approach is heightened by rapid developments across technological, policy, social, and business dimensions. These four windows highlight the aforementioned dynamics, their salience for our daily lives, and how important they are for enabling a fair, sustainable, and prosperous digital society. Collectively, these changes are reshaping how people's data is perceived, regulated, utilised, and monetised.

Business landscape transformation. The business landscape is undergoing significant change in response to technological, regulatory, and social shifts. In the early days of MyData Global, businesses often viewed data as a proprietary resource and saw little need to involve the people in what they saw as internal business operators. Human-centric thinking struggled to gain traction in boardrooms.

It is now easier for businesses to identify opportunities around human-centric data models. The increased risk of economic penalties and consumer distrust harming bottom lines helps businesses to imagine a world in which individuals and their fiduciary intermediaries reduce businesses' liability for data management. In this scenario, consumer trust is improved, the risk of regulatory infraction is reduced, and companies can make smarter and better decisions based upon data that is more accurate when the individual has had some oversight over it.

This type of thinking is increasingly seen to make sound financial sense and is spurring innovation. Personal AI technologies and assistants that adapt to individual preferences while keeping data under user control have the potential to create new market segments. Digital life management offerings that help people organise and leverage their data across domains are emerging as entrepreneurial ventures. Unlike earlier "personal data locker" approaches that emphasised storage without utility, these new models focus on activating data's value while maintaining individual agency.

Simultaneously, businesses face mounting challenges with

5 Antti Poikola, Kai Kuikkaniemi, and Harri Honko, MyData: A Nordic Model for Human-Centered Personal Data Management and Processing (Helsinki: Ministry of Transport and Communications Finland, 2015), accessed March 22, 2025, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf.

traditional data practices. Increased liability from data breaches, growing costs of regulatory compliance, and difficulties in understanding potential customers at scale have made conventional data-harvesting approaches increasingly risky and expensive. There is also increasing recognition that the status quo of data hoarding and extraction has negative impacts on the quality of data created by online consumers and netizens. This has been most pronounced in the digital advertising market but has repercussions all across the data value chain, particularly for B2B businesses and services in the data economy.

Policy landscape evolution. Following the GDPR's implementation, jurisdictions worldwide have introduced or updated data protection frameworks, from California's CPRA to China's PIPL and India's Digital Personal Data Protection Act. The European Data Act and Data Governance Act have established new rules for data sharing and intermediaries, while sectoral regulations in finance, health, and mobility increasingly address data portability and interoperability. This regulatory evolution reflects growing recognition that data flows need governance structures that balance innovation with fundamental rights.

Technological developments. Large language models and generative AI are blurring the boundaries between personal and non-personal data, as they can derive insights about individuals from seemingly anonymous information. Edge computing is moving data processing closer to its source, creating new challenges and opportunities for local control. Digital wallets are emerging as potential interfaces for personal data management, offering individuals secure storage and selective disclosure capabilities. Meanwhile, advancements in cryptography and privacy-preserving techniques like federated learning and differential privacy offer promising tools that align with MyData principles but require human-centric implementation frameworks.

Social awareness shifts. Following high-profile incidents such as the Cambridge Analytica scandal, COVID-19 mishandlings, corporate data leaks and democratic interference, public awareness around issues of data privacy and misuse has grown. Individuals increasingly expect transparency and control over their digital footprints, with younger generations particularly conscious of their data rights.

Alongside this, there is a perception that our capacity to control our technologies in comfortable and useful ways is being constricted, as features are removed or paywalled, or data cannot be seen, verified or used for one's own ends. People increasingly feel burdened by complex digital lives that are optimised for platform and provider subscription loyalty, advertising consumption, and profit rather than helping them to live friction-free and fulfilling lives. Civil society organisations have mobilised around digital rights issues, helping translate technical complexities into public discourse, and responding to a broad dissatisfaction with current data market practices.

2. The MyData approach

MyData offers a human-centric framework for data management that places individuals at the centre of their digital lives by giving them control over the data about themselves.

Emerging in 2014 and formalised through the establishment of MyData Global in 2018 (as an international non-profit headquartered in Finland), this approach asserted a model for how personal data should be managed and has grown into an international movement committed to realising this vision for empowering people with the data about them.

The community of actors identified and identifying with the moniker MyData has expanded significantly over the last ten years,[6] and there have emerged myriad groups of other entrepreneurs, activists, data collectives,[7] researchers and businesspeople across the world now pursue agendas that put people back in control of the technologies that shape our worlds. MyData is already firmly established as an international concept.

At its core, MyData seeks to empower individuals by improving their right to self-determination; MyData envisions a world where people can access, control, and benefit from data about themselves – whether it's shopping history, health records, movement data or financial information – while maintaining privacy and agency. The model doesn't require complete data lockdown — which would stifle innovation — nor does it permit unrestricted data exploitation.

Rather, it creates a balanced system where:

- People have real control over their data, not just on paper;
- Data protection and useful data applications work together, not against each other;
- Small businesses can compete with big tech platforms; and
- Data can flow freely between different services when people choose to share it.

2.1. The MyData Declaration and vision

In 2017 this vision was articulated in the MyData Declaration. A public document now signed by over 1,700 organisations and individuals and translated into 15 languages. The MyData Declaration takes stock of the challenges and opportunities presented above, and asserts a set of principles according to which that vision should be pursued, and three systemic shifts that would need to change in order to achieve this vision.

6 See for example The Berkman Klein Center's ProjectVRM, at https://cyber.harvard.edu/research/projectvrm.

7 Alex Bowyer, Mirko De Bortoli, and Paul-Olivier Dehaye, Data Collectives: A Practical Guide to Experimentation (Zenodo, 2024), accessed March 22, 2025, https://doi.org/10.5281/zenodo.13769788.

The MyData principles

#1 Human-centric control of personal data

Individuals should be empowered actors in the management of their personal lives both online and offline. They should be provided with the practical means to understand and effectively control who has access to data about them and how it is used and shared.

We want privacy, data security and data minimisation to become standard practice in the design of applications. We want organisations to enable individuals to understand privacy policies and how to activate them. We want individuals to be empowered to give, deny or revoke their consent to share data based on a clear understanding of why, how and for how long their data will be used. Ultimately, we want the terms and conditions for using personal data to become negotiable in a fair way between individuals and organisations.

#2 Individual as the point of integration

The value of personal data grows exponentially with their diversity; however, so does the threat to privacy. This contradiction can be solved if individuals become the "hubs" where, or through which cross-referencing of personal data happens.

By making it possible for individuals to have a 360-degree view of their data and act as their "point of integration", we want to enable a new generation of tools and services that provide deep personalisation and create new data-based knowledge, without compromising privacy or adding to the amount of personal data in circulation.

#3 Individual empowerment

In a data-driven society, as in any society, individuals should not just be seen as customers or users of pre-defined services and applications. They should be considered free and autonomous agents, capable of setting and pursuing their own goals. They should have agency and initiative.

We want individuals to be able to securely manage their personal data in their own preferred way. We intend to help individuals have the tools, skills and assistance to transform their personal data into useful information, knowledge and autonomous decision-making. We believe that these are the preconditions for fair and beneficial data-based relationships.

#4 Portability: access and re-use

The portability of personal data, which allows individuals to obtain and reuse their personal data for their own purposes and across different services, is the key to making the shift from data in closed silos to data which become reusable resources. Data portability

should not be merely a legal right but combined with practical means.

We want to empower individuals to effectively port their personal data, both by downloading it to their personal devices and by transmitting it to other services. We intend to help Data Sources make these data available securely and easily, in a structured, commonly-used and machine-readable format. This applies to all personal data regardless of the legal basis (contract, consent, legitimate interest, etc.) of data collection, with possible exceptions for enriched data.

#5 Transparency and accountability

Organisations that use a person's data should say what they do with them and why and should do what they say. They should take responsibility for intended, as well as unintended, consequences of holding and using personal data, including, but not limited to, security incidents, and allow individuals to call them out on this responsibility.

We want to make sure that privacy terms and policies reflect reality, in ways that allow people to make informed choices beforehand and can be verified during and after operations. We want to allow individuals to understand how and why decisions based on their data are made. We want to create easy-to-use and safe channels for individuals to see and control what happens to their data, to alert them of possible issues, and to challenge algorithm-based decisions.

#6 Interoperability

The purpose of interoperability is to decrease friction in the data flow from data sources to data-using services while eliminating the possibility of data lock-in. It should be achieved by continuously driving towards common business practices and technical standards.

In order to maximise the positive effects of open ecosystems, we will continuously work towards interoperability of data, open APIs, protocols, applications and infrastructure, so that all personal data is portable and reusable, without losing user control. We will build upon commonly accepted standards, ontologies, libraries and schemas, or help develop new ones if necessary.

The MyData shifts

#1 From formal to actionable rights

While many jurisdictions have enshrined data rights in law (such as the GDPR in the EU and the UK), these rights often remain theoretical—difficult to access and exercise in practice.

The MyData approach calls for transforming theoretical legal protections on paper into practical, everyday capabilities by:

- Converting complex consent processes into simple, understandable choices
- Turning data access rights into "one-click" solutions as seamless as the best digital services
- Making data portability between services as easy as sharing a document
- Providing transparent oversight of where your data is and who has access to it
- Enabling revocation of permissions is as straightforward as granting them

This approach ensures that control over personal data isn't just a legal concept but a practical reality for everyone. By designing systems with human needs at the centre, MyData makes it possible for people to meaningfully exercise their rights without needing legal expertise or technical knowledge. This bridges the gap between formal rights and actual agency, transforming abstract protections into tangible control mechanisms that work in people's everyday digital lives.

#2 From data protection to data empowerment

Current regulatory frameworks primarily focus on protecting people from harm. While essential, this defensive posture misses the opportunity for people to proactively use their data for personal benefit.

Beyond just controlling who can access their data, the MyData approach seeks to enable people to leverage their data to improve their lives. This could mean:

- Combining health data from multiple sources to receive personalised wellness recommendations
- Using financial data across services to make better economic decisions
- Managing digital identities across platforms to simplify online interactions
- Creating personal AI assistants that work for the individual, not for corporations

This empowerment dimension transforms data from something to be protected into a resource that actively enhances people's agency and capabilities in the digital world.

#3 From closed to open ecosystems

Today's digital economy concentrates power in a few platforms that collect and process vast amounts of personal data. These closed systems restrict competition and innovation while limiting individual choice. MyData envisions interconnected ecosystems where data flows freely according to people's choices, creating an open and fair digital economy that balances fairness, diversity, and competition.

MyData aims to level the playing field by:

- Enabling data portability between competitive services
- Supporting interoperability standards that allow different systems to work together
- Fostering networks of operators that facilitate data sharing under individual control
- Creating space for innovation where businesses compete on service quality rather than data hoarding

This ecosystem approach ensures that both individuals and organisations of all sizes can benefit from the data economy.

2.2. The MyData operators model

To realise the vision represented by the MyData Principles and the three shifts, the MyData Declaration asserted an operator model for personal data intermediation, as elaborated in the first edition of this white paper.[8] Specifically, this model was developed to address a data economy in which personal data moves between services in two ways:

- Direct connections between apps and services through APIs
- Big platform companies that collect and control data centrally

Both of these approaches focus on what organisations need, not what people need. They make it hard for individuals to understand and control how their data is being used.

In contrast, the MyData operator model places the person at the centre of the ecosystem as the point of integration between organisations that hold and use personal data about them. In the MyData model, the providers of personal data management services are in competition with each other but form interoperable ecosystems and, together, provide the infrastructure for the transmission of personal data.

8 Poikola, Kuikkaniemi, and Honko, MyData: A Nordic Model, 2015.

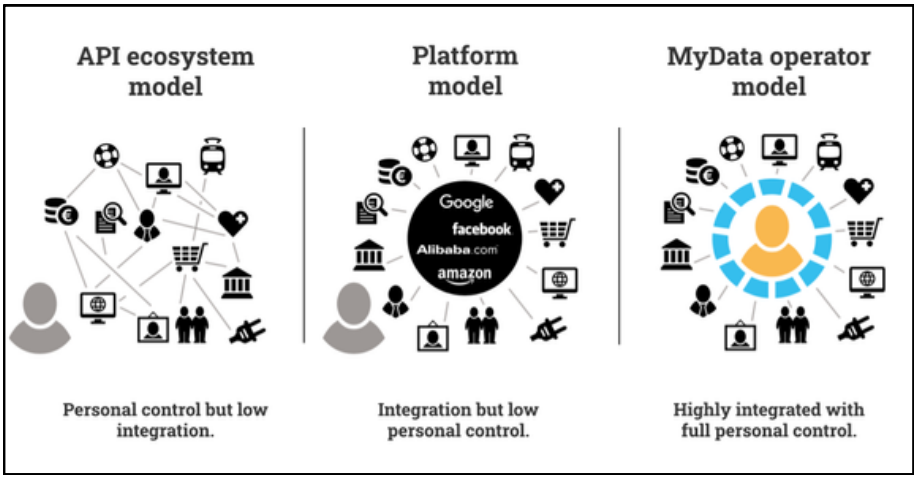

FIGURE 1. In the API ecosystem model (left), if the number of services increases, the number of connections will increase even faster. Centralising data management to platforms (middle) facilitates application development, but there is no incentive for different platform players to seek interoperability between platforms. Compared to the platform model, the MyData operators' infrastructure (right) is robust and scalable because it is not dependent on any one organisation providing the infrastructure.

The anatomy of an operator

Many types of organisations can function in the role of a MyData operator: data intermediation service providers and data altruism organisations recognised by the EU Data Governance Act, as well as data collectives, commons, unions, collaboratives, trusts, and so on.

The key defining feature of a MyData operator is its dedication to the rights and/or interests of people, as individuals or groups, and facilitating the exercise of those rights and advancing those interests via data management, sharing, and re-use.

MyData operators typically involve one or more of the following functional elements in order to perform their role.[9]

- **Identity management** handles authentication and authorisation of individuals and organisations in different, linked identity domains and links identities to permissions.
- **Permission management** enables people to manage and have an overview of data transactions and connections and to execute their legal rights. It includes maintaining records (notices, consents, permissions, mandates, legal bases, purposes, preferences etc.) on data exchange.
- **Personal data storage** allows data to be integrated from multiple sources (including data created by a person) in personal data storage (PDS) under the individuals' control.

9 Joss Langford, Antti 'Jogi' Poikola, Wil Janssen, Viivi Lähteenoja, and Marlies Rikken, eds., Understanding MyData Operators: MyData Global White Paper (Helsinki: MyData Global, 2020), accessed March 22, 2025, https://mydata.org/wp-content/uploads/2020/04/Understanding-Mydata-Operators-pages.pdf.

- **Service management** uses connection and relationship management tools to link operators, data sources, and data using services. Data can be available from different sources and can be used by multiple data using services.
- **Value exchange** facilitates accounting and capturing value (monetary or other forms of credits or reputation) created in the exchange of data.
- **Data model management** is about managing the semantics (meaning) of data, including conversion from one data model to another.
- **Personal data transfer** implements the interfaces (e.g. APIs) to enable data exchange between the ecosystem participants in a standardised and secure manner.
- **Governance support** enables compliance with the underlying governance frameworks to establish trustworthy relationships between individuals and organisations.
- **Logging and accountability** entails keeping track of all information exchanges taking place and creating transparency about who accessed what and when.

2.2.1. Networks and ecosystems

The operator model asserts that human-centric personal data ecosystems are composed of actors holding one or more of the following main roles:

- **People**: Control their own data and decide how it's used
- **Operators**: Provide tools and services that help people manage their data through any of the functions described above
- **Data sources**: Organisations that collect and store data
- **Data using services**: Services that use data to provide value
- **Network governors**: Organisations that set and enforce the rules

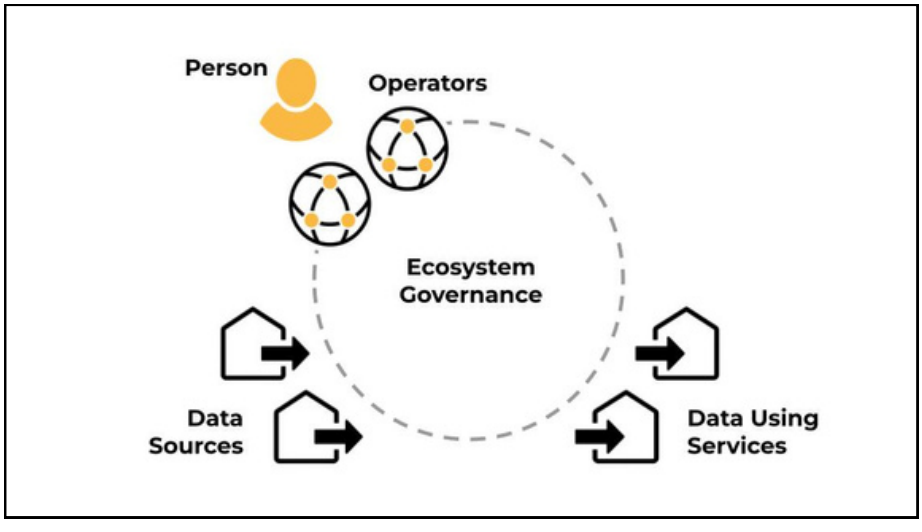

FIGURE 2. Roles in the MyData operators model.

Different kinds of actors like governmental organisations, private companies, and even individual people can take the roles of operator, data source, data using service, or ecosystem governance.

This model of personal data intermediation was seen to support the development of several potential personal data ecosystem structures and their interaction:

- **Fragmented**: Markets where many small operator-like entities compete to build small-scale use cases without interoperability between them.
- **Monopolistic data platforms**: A few platforms provide connectivity and data sharing inside their ecosystems with little competition and no incentives for interoperability between the platforms.
- **Fully decentralised**: A peer-to-peer world where standardised technical infrastructure and protocols enable data connections without any specific operator entities. In the decentralised model, the individual manages data flows directly from the end services or by having personal cloud-based applications on their own devices or hosted for them.
- **Competition-based interoperable operator network**: Similar to the current network of telecom operators, energy providers, or banks where many mutually competing providers are interoperable and together provide global-level connectivity.

In addition to personal data, data transmission within such ecosystems may also include non-personal data related to companies or objects, for example. Technologically speaking, there is no significant difference in data transmission depending on whether the data is personal or not, but applicable regulation is different when it comes to the processing of personal data or mixed data sets containing personal data alongside other technical or telemetry data points.

Beyond individuals and organisations: balancing needs in a multi-stakeholder ecosystem

While individuals and data-collecting organisations are central actors in the personal data ecosystem, the MyData approach recognises the importance of additional stakeholders whose perspectives and actions shape how personal data is governed and utilised.

- **Developers and technologists** implement the systems that collect and process data, making their ethical awareness and design choices critical to human-centric outcomes. Their roles in creating privacy-by-design architectures and ethical AI systems are essential for operationalising MyData principles.
- **Civil society organisations** play vital roles in advocacy, education, and representing collective interests that may not be addressed by market forces alone. From digital rights organisations to consumer protection groups, these entities help ensure that technical and business developments remain aligned with social values.
- **Policymakers and regulators** establish the legal frameworks that either enable or hinder human-centric data practices. Their challenge lies in creating regulations that protect rights while fostering innovation and interoperability across jurisdictions. These frameworks vary significantly by region—from the European emphasis on fundamental rights to the market-oriented approach in the United States to emerging models in regions like India, Brazil, and across Africa that often seek to balance multiple priorities.
- **Researchers** advance our understanding of both technical possibilities and social implications of personal data systems. Their work on privacy-enhancing technologies, data governance models, and the societal impacts of data practices provides critical foundations for human-centric approaches.
- **Media organisations, thought leaders and educators** shape the public understanding of issues around privacy, identity, expectations we can have of our technology, and societal benefits of data and personal technologies. It is unfortunate that amongst these actors that influence how we see the world are many actors who primarily serve political, commercial or personal agendas because it is only through increased attention and elevated awareness that people can be enabled to recognise online harms, abuses of digital power or data misuse and thus be motivated to demand a better digital life.

- **Regional and cultural contexts** shape how data systems are deployed and governed. While discussions of data governance often center on European and North American perspectives, other regions face distinct challenges and opportunities. In the Global South, questions of digital infrastructure, inclusion, and alternative models of collective data rights significantly influence how personal data management can function. Approaches that respect indigenous data sovereignty, address digital divides, and adapt to diverse legal systems are essential for MyData to achieve truly global impact.

Each of these stakeholders and contexts brings unique perspectives, incentives, and constraints to the personal data ecosystem. The challenge before us is to align these diverse interests around human-centric principles, creating an environment where ethical data practices become the most beneficial option for all involved, regardless of geographic location or cultural context.

2.2.3. Beyond data ownership: rights and shared interest

While the phrase "people should own their data" is intuitively appealing, the MyData approach recognises that ownership is an imperfect framework for personal data. Unlike physical property that can be exclusively possessed, data can be simultaneously held and used by multiple parties without diminishing its value or utility.

MyData instead focuses on ensuring people have rights, opportunities, and agency regarding data about themselves—without denying that organisations collecting or processing this data may also have legitimate interests in it. This balanced perspective acknowledges the relational nature of personal data, particularly in contexts like customer relationships where both individuals and organisations have valid claims to the same information. People must have visibility, understanding and usability of their data, but also, in those relationships with organisations that hold data about them, they need process transparency, oversight over data (being able to intervene), and be included in data-based decision-making.

Rather than artificial scarcity or exclusive control, MyData promotes a rights-based framework that enables both individual agency and beneficial data use. This approach recognises that the value of data often emerges precisely from its ability to be shared, analysed, and applied in multiple contexts, while still respecting the fundamental dignity and autonomy of the people it describes.

2.3. Looking ahead: from vision to implementation

The current data economy is a cluttered jungle of opportunity costs. In 2022, the average person had more than 240 online accounts,[10] and this number has likely only increased. Within each of these accounts sits data about us and settings about who can see and use that data, but the data itself is often duplicated, out-of-date, not portable, or otherwise difficult to access, understand or make use of.

Simultaneously, the internet is full of both useful open data and a brimful of inaccuracies and outright lies, commercial interests that run counter to yours, and data that is overwhelming in its abundance. The current logic of the internet is that you need to wade through all this to find the data (service, product, content, etc.) that serves you best, while the data about you is functionally locked beyond your control and benefit. The only data meaningfully leveraged in this system is through black-box behavioural data collection and analysis, sold and shared in digital advertising markets at the speed of light and with minimal human oversight.[11]

We can design better, and the MyData Declaration and operator model provide a useful starting point. In the eight years since the launch of the Declaration, over 70 operators have been certified by MyData Global for developing and launching services and platforms that embody and operationalise the MyData vision and principles. Across sectors and geographies, we have seen a proliferation of innovation and thought leadership towards this end, and we have also seen radical developments in the markets, technologies, and regulatory environments in which data is created and shared. This white paper takes stock of those developments to explore how the MyData vision should evolve apace, and the steps that need to be taken to move from vision to reality.

10 Dashlane, Global Password Health Score Report 2022, accessed March 22, 2025, https://www.dashlane.com/global-password-health-score-report-2022

11 Florian Pidoux, Gabrielle Gursky, Emilie Melin, Christophe Quémard, and Paul-Olivier Dehaye, Understanding Influence and Power in the Data Economy (Geneva: PersonalData.IO, 2022), accessed March 22, 2025, https://doi.org/10.5281/zenodo.6554155.

3. Where MyData can make a difference

This chapter takes stock of recent developments in the global data economy, and how the MyData approach can be leveraged to address some of society's most pressing digital challenges. It begins by reviewing four key problem spaces of unique concern to a flourishing digital society (AI proliferation, the future of democracies, the state of the global economy, and current geopolitical tensions), and suggesting how MyData can help to address them. It then reviews the persistent challenges in the global data context that threaten to inhibit those contributions, as well as the enabling factors that have emerged in recent years.

3.1. Key problem spaces and opportunities

MyData and related concepts are increasingly relevant to the biggest issues and most wicked problems humankind faces in 2025, as illustrated already in the figure below from 2021.[12]

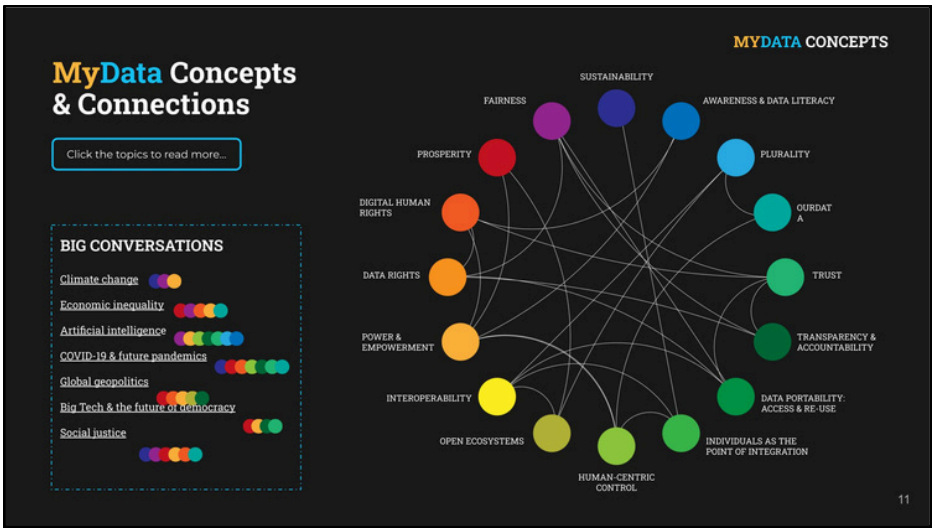

FIGURE 3. Relationships between MyData concepts and big conversations humankind is grappling with.

This section presents a problem analysis and the MyData perspective of four major macro-level developments that affect individuals, communities, and societies today: AI proliferation, the future of democracies, the state of the global economy, and our current geopolitical moment. The purpose of this section is to highlight how the MyData approach, improving people's agency over data, is both relevant and necessary to address the undesirable effects of each.

12 Viivi Lähteenoja and Sille Sepp, State of MyData 2021 (Helsinki: MyData Global, 2022), accessed March 22, 2025, https://mydata.org/wp-content/uploads/2022/07/State-of-MyData-2021_reduced-2.pdf.

3.1.1. AI proliferation

Problem analysis. The proliferation and increasing accessibility of AI systems, particularly large language models and generative AI, has created a complex landscape of opportunities and challenges in our societies and workplaces. While these technologies offer the potential for enhanced productivity and quality of life through improved decision-making and truly personal services, they simultaneously raise significant concerns about privacy, content creators' rights, and algorithmic bias as well as job displacement and worker surveillance. The integration of AI into core infrastructures has further blurred the distinction between personal and non-personal data, enabling more sophisticated data processing but also more pervasive monitoring and potential manipulation.

A particularly pressing challenge emerges from the growing power asymmetry between individuals and the organisations that control their data. As AI systems become more sophisticated, they can process vast amounts of data to make increasingly consequential decisions, yet their complexity often makes meaningful oversight difficult. This creates a situation where individuals, despite generating enormous amounts of data through their digital interactions, lack transparency and agency over how that information is used.

MyData perspective. While emerging technical solutions like decentralised and federated technologies, and governance frameworks such as the EU AI Act, offer promising paths forward, there remains an urgent need for a paradigm shift toward ethical approaches that ensure AI augments human capabilities rather than diminishing them, while protecting individual privacy and maintaining meaningful human control over automated decision-making systems.

Relevant MyData shifts and principles

- *Actionable rights* ensure that GDPR and similar data protection and privacy rights, as well as rights over intellectual property and business secrets, can also be exercised in meaningful ways when data is used to build AI and when AI is being used by individuals in their private and professional lives.
- *Data empowerment* means putting AI capabilities to the service of people in a truly personal way that they can trust and therefore benefit from increased gains in efficiency, data-informed decision-making, and overall quality of life.
- *Open ecosystems* ensure on the macro level that no single company or organisation can control the entire AI stack and its entire value networks. Openness enables meaningful ways to exercise human oversight over technical, legal, and business practices around AI ecosystems.

- *Human-centric control* means human oversight and the ability to effect changes in how data about people is used by AI systems.
- *Portability, access, and reuse* become increasingly meaningful now that people can now use personal AI to interact with data about themselves in an intuitive and accessible way.
- *Transparency and accountability* become critically important principles that we must demand that AI companies, and companies using AI, implement. They safeguard against malicious and unintentionally harmful practices and allow their detection and correction.
- *Interoperability* becomes significantly easier with current AI capabilities. Data format and semantics transformation abilities of AI are alleviating some of the traditional needs for strictly observed standards, ontologies, and their mappings.

3.1.2. Future of democracies

Problem analysis. The current information environment, shaped by social media platforms and content streaming services and their underlying algorithms, fundamentally impacts democratic societies' core functions and participatory principles. This manifests through multiple interconnected challenges: the exploitation of individuals' data for micro-targeted political advertising online, the proliferation of mis- and disinformation in social media platforms, and algorithmic systems optimised for both for holding our attention for as long as possible at a demonstrable cost to our overall wellbeing and for emotionally charged engagement rather than democratic discourse. Digital divides have widened as services become increasingly data-driven, creating new forms of exclusion for those lacking digital access or literacy.

MyData perspective. The MyData approach considers people in all their roles, not only as consumers, users, business owners, or workers. Empowering people also as citizens is an important part of the MyData mission. Emerging solutions similar to the MyData operator model, such as data trusts, cooperatives, and commons, as well as other collective governance models, demonstrate potential pathways for placing the power of collective data in the service of the people and communities about whom it's collected, though their success depends on addressing both technical and social barriers to ensure democratic participation remains accessible to all.

Relevant MyData shifts and principles

- *Data empowerment* means freedom from undue influence on human agency, whether that is perpetrated by algorithmic designs by platform companies, deliberate disinformation campaigns by governmental and other actors, or other digitally exclusionary social practices.
- *Open ecosystems* allow people to have a real choice between good alternatives to current social media and content streaming services without being locked in by undesirable network effects.
- *Human-centric control* and the individual as the point of integration can be implemented and supported by emerging technical solutions for digital identity wallets that allow individuals to control their identities and what is shared of themselves online and technically enforce certain aspects of trust online.
- *Transparency and accountability* mean that platforms are open about their practices regarding fact-checking and content moderation, and allow people to make informed choices of what kind of environments they choose to participate in.

3.1.3. Global economy

Problem analysis. Data has emerged as a critical force shaping economic success and competitive dynamics across all scales of the modern economy. At the macro level, the concentration of data power in the hands of a few dominant platform companies based in the US and China is fundamentally reshaping the competitive landscape between nations and regions. These companies have consolidated their position through vertical integration throughout the digital stack, including expansion into essential digital infrastructure, and powerful network effects that create significant barriers to entry for challengers and alternatives.

At the micro level, this data concentration directly impacts the competitive capabilities of individual businesses, particularly smaller organisations that struggle to compete against data-driven giants or comply with complex regulations. The result is a distorted marketplace where people's choice as consumers but also as citizens, patients, business owners, parents, and so on, is increasingly limited. In addition, innovation is stifled by the incumbents' anti-competitive tactics, and alternative services that might better serve people's needs, wishes, and privacy preferences struggle to emerge.

MyData perspective. Mastery over data collection, analysis, and deployment will likely continue to determine both national and regional economic competitiveness and individual business success in

the global marketplace. This is why the MyData approach is essential if we are to make progress towards more equitable data economies both on the macro and micro levels. Placing this mastery over data throughout its lifecycle into the hands of the people, not a few global corporations, promises to democratise, legitimise, and redistribute the value from data collection, analysis and deployment.

Relevant MyData shifts and principles

- *Open ecosystems* are key to fending off current and guarding against future monopolistic and anti-competitive behaviour. When ecosystems are accessible to organisations of different sizes, real competition between good alternatives can emerge and the playing field is more level and people better served.
- *Human-centric control* is the antidote to current, organisation-centric models that treat data as something that belongs to the company capturing it, rather than the people from whom it originates. This colonialist logic is at the heart of the exploitative practices that concentrate data, and therefore power, in the hands of the few only.
- *Data portability, access, and re-use* mean that data can move freely wherever people go online. It means data isn't stuck or locked within the systems or ecosystem of a single company or organisation, but can be used by people and services they trust. Together with interoperability, this principle undoes some of the undesirable network effects that dictate the business logic of today's global economy and can disrupt the prevalent incentive structures for data hoarding.
- *Interoperability* is the requirement for data to be useful outside the system into which it was originally captured. It is an alternative to proprietary formats and walled gardens that prop up the current data economy's oligopolistic practices.
- *Transparency and accountability* about real data practices, shining a light on what actually goes on in the globally dominant companies today, can raise general awareness of the unethical and undesirable ways in which they operate. Awareness is key to empowering people to vote with their feet and choose better alternatives.

3.1.4. Geopolitical tensions

Problem analysis. The fragmentation of the global internet has been complemented by the emergence of competing market and regulatory systems for data sharing and reuse. Common distinctions are drawn between the European, US, and Chinese regulatory environments, their comparative potential for competing globally and generating va-

lue, and the normative values on which they are based. These distinctions are accentuated by geopolitical tensions surrounding access and control of rare earth minerals and the production of semiconductors. They have been particularly salient to the European discourse on data sovereignty and strategic autonomy, in which reliance on US-based hyperscalers for cloud computing and storage services raises concerns about vulnerabilities down the technology stake and the insufficiency of GDPR protections to protect European data.[13] These concerns have gained increasing attention in the wake of recent changes in the US political leadership and global policy. Against this background, ongoing debates about appropriate regulatory frameworks to facilitate trusted data sharing across borders and services continue, with regulators in developing economies considering the challenges and advantages of aligning national policy with EU regulations or other regulatory frameworks, such as the Japanese-led initiative for Data Free Flow with Trust (DFFT).[14]

MyData perspective. Data services and platforms that operationalise the MyData principles, such as the operator model, often provide users with direct control over data about them, including the ability to limit the access of third parties to that data. The use of federated and edge-based data storage and governance models structurally embeds individual data sovereignty into the global data economy for those individuals who use such services. If scaled, this could represent a significant contribution to protecting the digital autonomy and data sovereignty of nations and regions. Providing individuals with meaningful and understandable agency over their own data also facilitates data sharing based on trust, and provides individual benchmarks for considering and comparing different regulatory regimes for data sharing.

Relevant MyData shifts and principles

- *Human-centric control* means that individuals are able to manage and control access to the data about them, and can include the ability to store that data on their devices or on federated or encrypted platforms that provide them with individual data sovereignty.
- *Individual as the point of integration* means that individuals have a full overview and access to the relevant data about them, so that they can make informed decisions about which data they want to control access to.

13 Pencho Kuzev, Cadenabbia Memorandum on the European Cloud Policy (Berlin: Konrad-Adenauer-Stiftung, 2022), accessed March 22, 2025, https://www.kas.de/de/monitor/detail/-/content/cadenabbia-memorandum-on-the-european-cloud-policy.

14 Digital Agency of Japan, Data Free Flow with Trust (n.d.), accessed March 22, 2025, https://www.digital.go.jp/en/policies/dfft.

- *Transparency and accountability* about who has access to data and how it is used is essential for building the trust required to facilitate the improved flow of high quality data to support innovation and value creation in the marketplace.

3.2. Inhibiting factors and trends

MyData's potential to contribute to the problem spaces presented above is frustrated by systemic contextual factors, which have continued to develop since the MyData vision was first articulated, and which must be confronted if the potential of the MyData approach is to be realised.

Technical and security vulnerabilities. The acceleration of technological innovation has outpaced our ability to secure personal data and ensure meaningful human oversight. Complex, opaque data practices severely limit user understanding and agency, creating exploitable security gaps and undermining trust. Meanwhile, the advent of quantum computing threatens to render current encryption standards obsolete, potentially exposing vast repositories of sensitive information.

The technical complexity of modern data systems has created a fundamental imbalance—individuals are expected to manage increasingly sophisticated data relationships with tools that remain rudimentary and fragmented, while their data is scattered across hundreds of organisations. This asymmetry between the sophistication of data collection and the primitiveness of user control mechanisms represents a systemic vulnerability that undermines both individual rights and collective security.

The economics of power concentration. The economics of data accumulation continue to favor concentration over distribution. Network effects, data network effects, and economies of scale create powerful incentives for centralisation that make it extraordinarily difficult for alternative, more distributed models to gain traction. This concentration directly impacts the competitive capabilities of individual businesses, particularly smaller organisations that struggle to compete against data-driven giants.

The result is a distorted marketplace where consumer choice is increasingly limited, innovation is stifled, and alternative services that might better serve individual needs or privacy preferences struggle to emerge. Traditional antitrust approaches have proven insufficient to address these dynamics, as data advantages often operate through mechanisms that existing competition frameworks were not designed to regulate.

The intractable data self. Beyond the practical challenges of data ma-

nagement lies a deeper philosophical problem—what might be called the "Intractable Data Self."[15] Modern data systems create persistent, partial representations of individuals that increasingly determine their opportunities and experiences, yet remain largely invisible and uncontrollable.

These data shadows are often incomplete, inaccurate, or unfairly constructed, leading to significant harms ranging from economic exclusion to algorithmic discrimination. Yet individuals typically lack both awareness of these data representations and effective means to correct or contextualise them. This disconnect between lived identity and data identity represents a fundamental threat to human dignity and self-determination in digital society.

The digital literacy gap. Despite growing public awareness of data issues, a profound digital literacy gap persists that undermines individuals' ability to meaningfully engage with their data rights. People cannot begin to take control until they have visibility and understanding of what data exists and how it is being used. Complex privacy policies, technical jargon, and deliberately obscure user interfaces create substantial barriers to informed decision-making, even for motivated and educated users.

This literacy gap is not evenly distributed, with already marginalised communities often facing the greatest challenges in understanding and exercising data rights. The result is a data economy where meaningful consent remains more theoretical than practical for large segments of the population, undermining the legitimacy of current data practices.

3.3. Enabling factors and trends

There have also been several contextual developments that can significantly enable and amplify the development of the MyData approach. Reviewing recent developments across regulation, technology, business and society highlights several trends and developments that can support the application of MyData principles, and and suggest an emergent collective of initiatives that can be mutually reinforcing in the effort to achieve the MyData vision.

Regulatory evolution beyond compliance. The global regulatory landscape has progressed significantly beyond GDPR's foundational framework, with new approaches that incorporate increasingly sophisticated human-centric principles:

- Data fiduciary models: Legal frameworks establishing formal trust responsibilities for organisations handling personal data, shifting from mere compliance to affirmative duties of care.
- Collective enforcement mechanisms: Systems enabling groups of affected individuals to collectively challenge data practices, addressing the fundamental power imbalance between individuals and data controllers.

15 Alex Bowyer, Understanding and Improving Human Data Relations (PhD thesis, Newcastle University, 2023), accessed March 22, 2025, https://theses.ncl.ac.uk/jspui/handle/10443/5973.

- Interoperability mandates: Requirements for dominant platforms to enable meaningful data portability and service interoperability, directly countering the lock-in effects that sustain digital monopolies.

These regulatory innovations are increasingly converging around principles that align with MyData, creating a more supportive environment for human-centric data practices. However, their success ultimately depends on robust enforcement and the development of simplified compliance pathways, particularly for smaller organisations.

Technical infrastructure for digital sovereignty. The technical foundations for implementing MyData principles at scale continue to mature:

- Self-Sovereign identity systems: Decentralised identity solutions enabling individuals to manage their digital identities without dependence on platform gatekeepers, creating the foundation for genuine digital autonomy.
- Personal data stores: User-controlled repositories allowing individuals to aggregate their fragmented digital presence while maintaining granular, dynamic access controls across services.
- Privacy-preserving computation: Advanced cryptographic techniques enabling data utilisation without compromising privacy, resolving the false dichotomy between data protection and innovation.

These technological building blocks have moved from theoretical possibilities to production-ready systems, removing previous barriers to MyData implementation while preserving functionality and usability.

Market transformation through trust economics. Economic incentives are gradually shifting toward models that reward human-centric data practices:

- Trust as competitive advantage: Organisations demonstrating respect for individual data rights increasingly outperform peers in customer acquisition and retention, creating market pressure for improved practices.
- Data cooperatives and trusts: Collectively governed structures allowing individuals to pool their data while maintaining democratic control over its use, creating counterweights to corporate data power.
- Value exchange networks: Infrastructures enabling fair compensation for data contribution, creating economic incentives for individual participation in data ecosystems without commoditising privacy.

These market developments suggest human-centric approaches can be economically sustainable and competitively advantageous when the right incentives and governance structures are established. The challenge lies in creating sustainable economic models that fairly distribute both costs and benefits across the ecosystem.

Social infrastructure for collective agency. Beyond technology and regulation, vital social infrastructure is emerging to support human-centric data practices:

- Data rights service organisations: Specialised intermediaries helping individuals exercise their data rights effectively, addressing the fundamental knowledge and power asymmetries in current data relationships.
- Community governance models: Participatory frameworks enabling collective decision-making about shared data resources, particularly for non-personal but collectively impactful data.
- Digital literacy initiatives: Educational programs building individual and community capacity to understand and navigate increasingly complex data environments with agency and discernment.

This social infrastructure is essential for translating technical capabilities and regulatory rights into meaningful agency for individuals across diverse contexts and capabilities. The most sophisticated technology will fail without corresponding social structures that make it accessible and meaningful to ordinary people.

These developments in regulation, technology, markets and social infrastructure suggest new allies, resources, ideas and initiatives that can help to drive the elaboration and application of the MyData approach. Engaging with these dynamics and finding ways to complement and amplify the work of other initiatives that contribute to the MyData vision will be an important aspect of elaborating MyData in 2025.

4. Future directions

This chapter offers a provocation on how to understand MyData's relevance and potential in the context of 2025. It does so on the basis of the key developments, challenges, and enabling trends described above, and poses critical questions to the MyData community and beyond.

This is a call to action: it's time to take stock and evaluate what we have, and to ensure it serves us in the futures we're facing. We firmly believe that the MyData approach is more valid and necessary today than it has ever been, but that we need to re-interrogate how.

To do so, this chapter asks a series of questions in the spirit of productive interrogation: how can we further strengthen the MyData approach given what we've learned and what is happening around us today?

4.1. Interrogating the MyData vision

The MyData vision has been in the past articulated as "**a fair, sustainable, and prosperous digital society through human-centric use of personal data**". It is time to flesh out this vision statement in 2025: what do fairness, sustainability, and prosperity mean for digital society today? And is there just one digital society, or should we rather speak of digital societies as many? Is the term "human-centric" still the right one to convey what MyData is? Is the scoping to "personal" data still relevant?

Fairness and **prosperity** have in recent decades become understood as having a causal relationship, not only a correlation.[16] Stable and fair institutions, like those in democracies, cause economic prosperity, not just coincide with it.

It might therefore be justified to focus efforts on bringing about more egalitarian institutions into our digital societies, as those will lead also to the prosperity and economic well-being for these societies. Fairness in the institutions of digital societies, on the other hand, must also include planetary justice and the promotion of **sustainable** ecological as well as social practices.

The single, global **digital society** may not always be the most helpful level of abstraction, or of action. The splintering of the internet has already been in progress with Russian and Chinese governments essentially segregating their peoples from the rest of the internet into their own digital societies. Certain European initiatives calling for, e.g., data localisation and restricting third-country data processing can also be seen as following an isolationist trend. A single digital society is not reality, nor is it entirely clear that it's wholly desirable as opposed to, for example, a more mosaic-like configuration of interconnected digital societies built by and for the people that populate them.

16 Daron Acemoglu and James A. Robinson, Why Nations Fail: The Origins of Power, Prosperity, and Poverty (New York: Crown Publishing Group, 2012).

The term "**human-centric**" is increasingly both inflated and criticised. In some contexts, just about anything can be called "human-centric" without any real ethical meaning or commitment to back it up. Other criticisms blame it for anthropocentrism and failing to address the needs, rights, and duties associated with the planet we live on. MyData does not hold monopoly on the term human-centric, and it may well be good time to let it go and focus on rather defining the term MyData to stand for the ethical commitments and inclusive scope, also of humans as biological beings in a biosphere in crisis.

Finally, it may well be time to shift focus away from the too often too narrowly defined **personal data**. The inclusive scope of MyData also touches on data that is not being used in a context that makes it personal data, but nevertheless either impacts people, directly or indirectly, or could be used by people to improve their quality of life.

4.2. Interrogating the MyData shifts

What do the three shifts, defined in the MyData Declaration of 2017, mean today? How might we update them to reflect the realities of 2025 and beyond? This section describes some considerations.

4.2.1. From formal to actionable rights

What if there are no formal rights? Thanks to "the Brussels effect" of GDPR-like laws becoming increasingly popular around the world, most of the world's population is today covered by some kind of data protection law. Still, over 20% of people in the world, some 1.67 billion of us, do not have this right to digital privacy recognised by their national legislation.[17] Further, group rights are an area of mainly international law, where their status is not firmly established. So how could this shift be rethought to account for contexts where even formal rights are lacking?

What about other than data subject rights? Data protection and privacy laws are not the only ones that establish formal rights to people. Copyright and intellectual property, consumer affairs, regulations on matters of health and medicine, freedom of information, labour laws, and other types of legislation also grant individuals formal rights related to data. In addition to these, also international human rights law recognises rights of all individuals. How could this shift more explicitly incorporate these considerations?

More than merely technical actionability? Legal rights must be not only technically actionable but people must also be aware of them, understand their importance and relevance to their lives, and willing to take action when something goes wrong. How might this shift account also for this kind of social and cultural actionability?

17 Aly Apacible-Bernardo and Luke Fischer, "Identifying Global Privacy Laws, Relevant DPAs," International Association of Privacy Professionals, March 19, 2024, accessed March 22, 2025, https://iapp.org/news/a/identifying-global-privacy-laws-relevant-dpas

What about the burden on ethical businesses? An important part of making formal laws actionable is also the adequate resourcing and political backing for enforcement actions by public authorities. Formally recognised rights cannot be made actionable without being actively enforced. At the same time, it is important to recognise that the overall regulatory burden on law-abiding businesses and other organisations should be fit for purpose and not amount to a barrier to their success. Is there a way to account for striking this balance in this shift?

4.2.2. From data protection to data empowerment

Who should be empowered? Data about people exists on the individual, group, and societal levels. In addition to individuals being empowered with data, how can this shift account also for group and community empowerment, such as indigenous data sovereignty, or societal empowerment, meaning general attitudes to data recognising the potential of its benefits to democracies and societal cohesion as well as the competitiveness of economies?

What does this mean for public bodies and societies at large? How can this shift account for the plurality and diversity of legitimate opinions of how much protection is enough and how much empowerment is still too little? In other words, how does this shift understand the culturally relative understanding of the appropriate point between extreme protection and extreme liberties?

What data should empower people? How does this shift account for data other than what is considered personal data about a specific individual? The world is full of data that can be used by people to lead better lives. How can this shift capture the wealth of kinds of data empowerment that is possible with other than a person's own data?

Should we share more data about ourselves? How can this shift consider models whereby the individual signals out the kinds of services or products they are after, or their intent to make a decision, and lets the data come to them? Can this shift somehow promote reversing the consumer relationships so that people aren't data in companies' CRM (customer relationship management) systems, but rather companies are data in people's VRM (vendor relationship management) systems, enriched with personal preferences?

4.2.3. From closed to open ecosystems

Do all ecosystems have to be open? Monopolistic and oligopolistic market behaviours are unacceptable from a MyData perspective, but is the alternative exclusively open ecosystems? There are some business models and data governance frameworks that appear to pursue the MyData vision by providing individuals with control over their own closed systems. How might this shift account for the busi-

ness realities of needs for exclusive and confidential arrangements without compromising its core meaning?

4.2.4. What else needs to shift?

The 2017 shifts stand the test of time, and each is timely still in 2025. Our collective understanding of the complexity of the MyData landscape has meanwhile deepened, and there may be other shifts we may as a community choose to lift up alongside the originals. Below are collected some candidates for new or newly phrased shifts for inspiration.

- The shift from static to contextual definition of people's data
- The shift from data exploitation to ethically sustainable data practices
- The shift from global concentration of data power to data sovereign societies (without falling into splintered tribalism)
- The shift from binary 'personal' or 'non-personal' data to plurality of data 'with human impact'
- The shift from optimisation for maximum transaction quantity to optimisation for maximum relationships quality
- The shift from corporate profiteering from data to people flourishing with data
- The shift from state dictatorship and industry self-regulation towards participatory, democratic governance of data

4.3. Interrogating the MyData principles

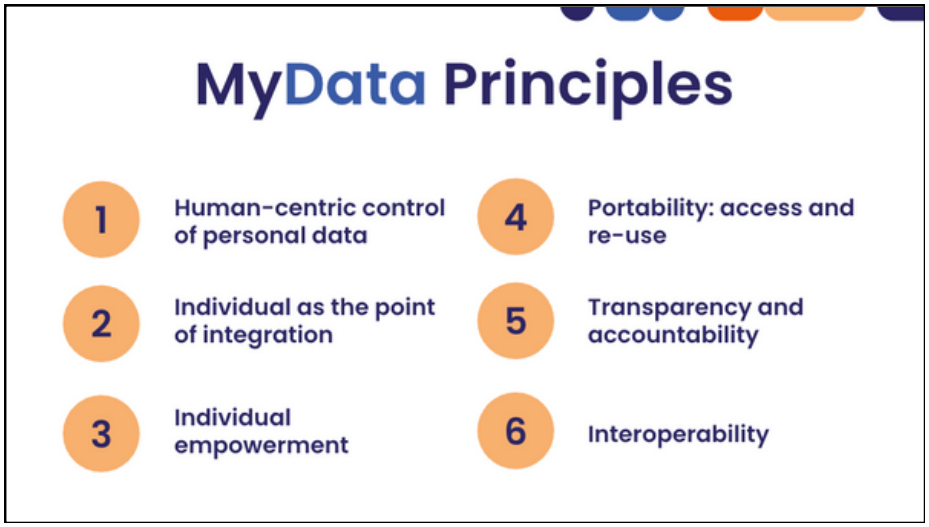

FIGURE 4. The MyData Principles as articulated in the MyData Declaration

The MyData principles of 2017 (see Figure 4) continue to resonate in 2025, but there may be new considerations we as the MyData community will want to elevate at this moment. Below are collected some candidates for new or newly phrased principles for inspiration.

- **Literacy and awareness**: People should understand from an early age what data is and what it can be used to do to impact their lives, communities, and environments.

- **Do no harm/Non-malfeasance**: Data should not be used to harm people or the biosphere directly, and any indirect harm should be documented and demonstrably minimised.
- **Sense of agency and empowerment:** People should feel they can affect and control what is done with data about themselves and actively benefit from different kinds of data use.
- **Contextualisation and pluralism**: Moving beyond the binary of personal and non-personal data, data protection and use should always be evaluated in its specific context and its potential impact on people as individuals and groups.
- **Proportionality and reciprocity**: People should always receive a proportionate benefit from any value-generating use of data about themselves.
- **Availability and portability**: when data is collected about people, that data must always be put also and to the fullest extent of its utility at the disposal of those people.

4.4. Interrogating the MyData operators model

The MyData operators model is a crucial part of the MyData approach. It is a model for implementing the MyData principles in practice to progress the MyData shifts. It is also an evolving model that has been adapted and refined in iterations since it was first introduced in the early 2010s. This section asks the question: what's next for the operator model?

The MyData operators model is one where each individual has control over the portion of the digital economy and society in which they live that is directly related to themselves, as opposed to organisations having this control. This model is based on certain assumptions that tend to be made. Potential variations of the MyData operators model, as described earlier in this paper, may adjust one or more of the underlying assumptions of the basic model. Some of these are described below.

- **Direct exercise of decision-making power.** The operators model tends to assume a direct power relationship between the person and the organisation processing data about them. The relationship is intermediated by the operator, but the operator does not exercise power itself, if merely acts as a conduit for the will of the person towards the organisation. This model presupposes the capacity, capability, and willingness of the person to make a conscious, informed decision about each potential use of their data. Alternatives to this aspect of the operator model can involve, for example, the person assigning or choosing a representative, such as a personal AI agent or a community-maintained preference profile, to make detailed decisions while the person itself chooses the basic principles on which individual decisions should be taken on their behalf.

- **Only direct stakeholder involvement.** The operators model tends to assume that only direct stakeholders of given data need to be involved and empowered in the use of that data. Further, this direct stakeholdership is usually conceived in terms of the "identified or identifiable natural person" relating to some data in the spirit of the GDPR. Alternatives to this aspect of the model involve participatory governance mechanisms whereby the use of data that affects the lives of people is governed in a way that involves those people, whether or not "their" personal data is used or not.
- **Meaningfully exclusive rights over data.** The operators model tends to assume that it's always clear who is the direct rights holder for particular data and that they have meaningfully exclusive rights over that data. Alternatives to this aspect of the model involve the recognition that most data is subject to different rights by different parties, both human and organisational, and technical, legal, and societal mechanisms by which these rights, and their attendant duties, can be weighed against each other and fairly recognised and assigned.
- **Static conceptions of data as (non-)personal.** The operators model tends to assume that certain data can be definitively and permanently labelled as "personal" and as relating to a specific individual who has consequent rights over that data. Alternatives to this aspect of the model involve recognition of the fact that the same data becomes "personal" or "non-personal" depending on the context in which it is used. For example, anonymised and therefore non-personal data becomes personal (again) once it's placed in the context of another set of data that allows for the identification of individuals in that data that wasn't possible before.
- **Individual responsibility to care for oneself.** The operators model tends to assume that the individual is the only, the main, or the most appropriate, locus of responsibility over the care and wellbeing of that person. The political spectrum can be organised on its relation to this very principle and the extent to which it holds. On the one hand, extreme libertarianism focuses on the individual's sole freedom and responsibility to determine their own condition. On the one hand, we find either extreme communitarianism which places the utmost value on the flourishing of the collective (not the individual), or extreme paternalism, which places the primary freedom and responsibility for individuals' condition in the hands of the state (not the individual). Alternatives to this aspect of the model find their place in some other point on this spectrum.

- **Operators have less power than other organisations.** The operator model tends to assume organisation-to-organisation relationships are symmetrical and this fact enables the operator (organisation) to effectively represent the individual among organisations that are data sources and data using services. Since operators merely act as conduits for the individual's will, some of the power asymmetry between individuals versus organisations remains intact even in the operator model. This recognition could be complemented with calls to design regulation that reinforces the operators' ability effectively to enforce the rights and preferences of the people whom they represent.
- **Data sources and data using services are not all equal.** The operator model tends to assume that organisations that are data sources or data using services are roughly equal to each other. The reality is, however, that there are only a handful of individual companies and other organisations that control the majority of the data related to, and affecting, the average person. The majority of organisations in the world, by contrast, are also victims of these powerful companies' anti-competitive practices and unethical data use. Alternatives to this aspect of the model call for specialised measures to mount credible defences and safeguards against the real and potential abuses by these specific major actors with the most power to impact the most people in the most profound ways. In doing so, we can also promote and benefit the majority of organisations, especially ethically minded data sources and data using services, who are unable to offer the kinds of services people want because they face huge barriers to entry and suffer from the undesirable network effects that benefit only the few.

4.5. Summary of provocative questions

Regarding the MyData vision

- Revise the vision of "a fair, sustainable, and prosperous digital society through human-centric use of personal data" ?
- Is "human-centric" the right term and concept?
- Is "personal data" still the focus?

Regarding the MyData shifts

- Regarding the shift "*From formal to actionable rights*", what if there are no formal rights? What about rights other than data subject rights? Should this be about more than merely technical actionability? What about the burden on ethical businesses?
- Regarding the shift "*From data protection to data empowerment*", who should be empowered? What does this mean for public bodies and societies at large? What data should empower people? Should we share more data about ourselves?
- Regarding the shift "From closed to open ecosystems", do all ecosystems have to be open?
- What else needs to shift?

Regarding the MyData principles, should we consider adding or revising principles related to:

- Literacy and awareness
- Do no harm/Non-malfeasance
- Sense of agency and empowerment
- Contextualisation and pluralism
- Proportionality and reciprocity
- Availability and portability

Regarding the MyData operators model

- Should the model accommodate indirect decision-making power
- Should operators have the power to enforce the rights and preferences of the people whom they represent?
- Should the model accommodate the interests of affected third-party individuals and stakeholders?
- How should the model accommodate complex allocation of data rights across different stakeholders?
- How should the model acknowledge contexts in which individuals are not the main or the only responsible party for individuals well-being?
- How should the model engage with power imbalances between organisations?

5. Concluding remarks

Unlike previous editions of the MyData White Paper, this edition takes a fundamental stock of the MyData vision and approach in the context of dramatic recent developments across technology, business, regulation and society. It does not assert a clear prescription, but asks challenging questions about what the MyData approach means and how it is relevant in our turbulent times.

This is in keeping with the ethos of the vision and the movement. The MyData approach has always been about more than technical infrastructure or regulatory compliance. It is a bet on a different future—one where dignity and thriving is designed into digital life, where the benefits of data are equitably shared, and where human agency and flourishing are not luxuries, but everyday realities.

If MyData is to remain not just relevant but transformative, we must be willing to question our own assumptions and ambitions. This white paper does not prescribe a single path forward. Instead, it invites everyone — technologists, policymakers, researchers, entrepreneurs, and everyday people — to co-create that path: rigorous in its ethics, inclusive in its vision, and bold in its imagination. The future of data is still unwritten. Let us write it, together.

About MyData Global

MyData Global is an award-winning international nonprofit. The purpose of MyData Global is to empower individuals by improving their right to self-determination regarding their personal data. MyData Global facilitates a global community of personal data professionals and enthusiasts, who share a vision of human-centric paradigm towards personal data. This paradigm is aimed at a fair, sustainable, and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationships between individuals and organisations.

Join MyData Global at mydata.org/participate/membership/
Email us at hello@mydata.org
Follow us on Bluesky @mydataorg.bsky.social
Visit us at mydata.org

About this publication

Authors: Alex Bowyer, Viivi Lähteenoja, Christopher Wilson

Design: Sille Sepp and Viivi Lähteenoja

Citation information: Bowyer, A., Lähteenoja V., and Wilson, C. (2025) MyData in Motion: Evolving Empowerment for 2025 and beyond.

Download this publication at https://mydata.org/publications