October 2024

An Innovation for the Digital Economy Architecture

GLOBAL INITIATIVE FOR DIGITAL EMPOWERMENT

GIDE Global Initiative for Digital Empowerment
HUMAN-CENTERED DIGITAL GOVERNANCE

TABLE OF CONTENTS

An Innovation for the Digital Economy Architecture (IDEA)

Over the last five years, most countries around the globe have enacted norms and rules that are fundamental to the evolution of a human-focused single data market. Building on data protection legislation, they have created critical rights and protections: putting in place, *inter alia*, enhanced privacy and data control rights, protection of minors, improved competition rules, data intermediaries and fiduciary obligations, improved data sharing rules, increased transparency and accountability of platforms, enhanced data accessibility and interoperability, fair data value allocation, and ethical AI frameworks.

Now there is an opportunity to put in place an additional market mechanism and incentives to fully exploit these legislative pillars to practically build a consumer driven data market and unleash widespread innovation in the digital economy and society. Evolving from the established rights and protections, now is the time to further practically empower digital citizens in their digital lives by giving them control over the accuracy and source of their personal data and how it is processed, who has access to it, and on what terms, and to empower them with skilled advisers who can help them effectively negotiate and benefit from the modern digital economy.

Now is the time for an Innovation for a Digital Economy framework.

The objectives of the proposed Innovation for the Digital Economy Architecture (IDEA) are to:

1. Ensure all digital citizens have real control over the accuracy and source of their personal data, total transparency, and choice as to who and how processes it, has access to it, and from where and, through collective representation, negotiate the terms under which personal data is processed.

2. Rebalance the economic and social power structure in the digital economy by establishing an industry model of expert fiduciary professionals to advise digital citizens and negotiate on their behalf with entities seeking their personal data, how personal data about them can and should be used, and under what terms.

3. Unleash a widespread wave of innovation and renewed competition through the creation of a new market, driven by new companies and business units of existing businesses, that delivers personal digital advisory services and new models for the use of personal data in the single market, where the needs and purposes of digital users drive digital services rather than the other way around.

4. Reduce fraud and improve efficiency by requiring residents to ensure Key Personal Data[1] is accurate and verified by trusted parties[2] and require the residents' unique data repository to deliver to interacting entities the residents' personal data, use preferences and negotiated terms through uniquely encrypted machine-readable data protocols.

5. Achieve greater data sovereignty and literacy in a global online ecosystem by giving residents greater personal expert advice and control over where their personal data is processed.

A Digital Economy Innovation Architecture could have as significant an impact on the digital economy as the other big reforms of the last centuries, which empowered residents as economic actors. The collective representation of workers changed the labour markets, and fiduciary agents transformed the financial service and pension markets. Together, they delivered the middle-class economy. Empowered residents as active consumers will transform the 21st-century digital economy.

In the following sections, we explain

- why we need a new digital economy innovation regime
- how reform in data governance can drive innovation and growth
- what needs to be included in the new digital economy innovation regime
- who will benefit
- how existing legislation supports the proposed IDEA

We close with a call to action. Annex I provides initial wording for the proposed IDEA in the context of the European Union.

Why We Need a Digital Economy Innovation regime

The present digital data system may work on a superficial level. But the reality is that the misalignment between digital consumers and those who collect and monetise personal data has led to a wide variety of serious problems:

- Individuals/citizens do not have access to the skills, bargaining power or tools to participate in the digital economy effectively; they have legitimate interests over their data but not the means to implement.
- They are exposed to a far-ranging manipulation of attention, thought, feeling, and behaviour. Fundamental human rights are threatened, and the cohesion of our societies is being degraded.
- The existing system erodes appreciation for objective notions of truth, undermining our democratic processes.

[1] As outlined below, a subset of Personal Identifiable Information.

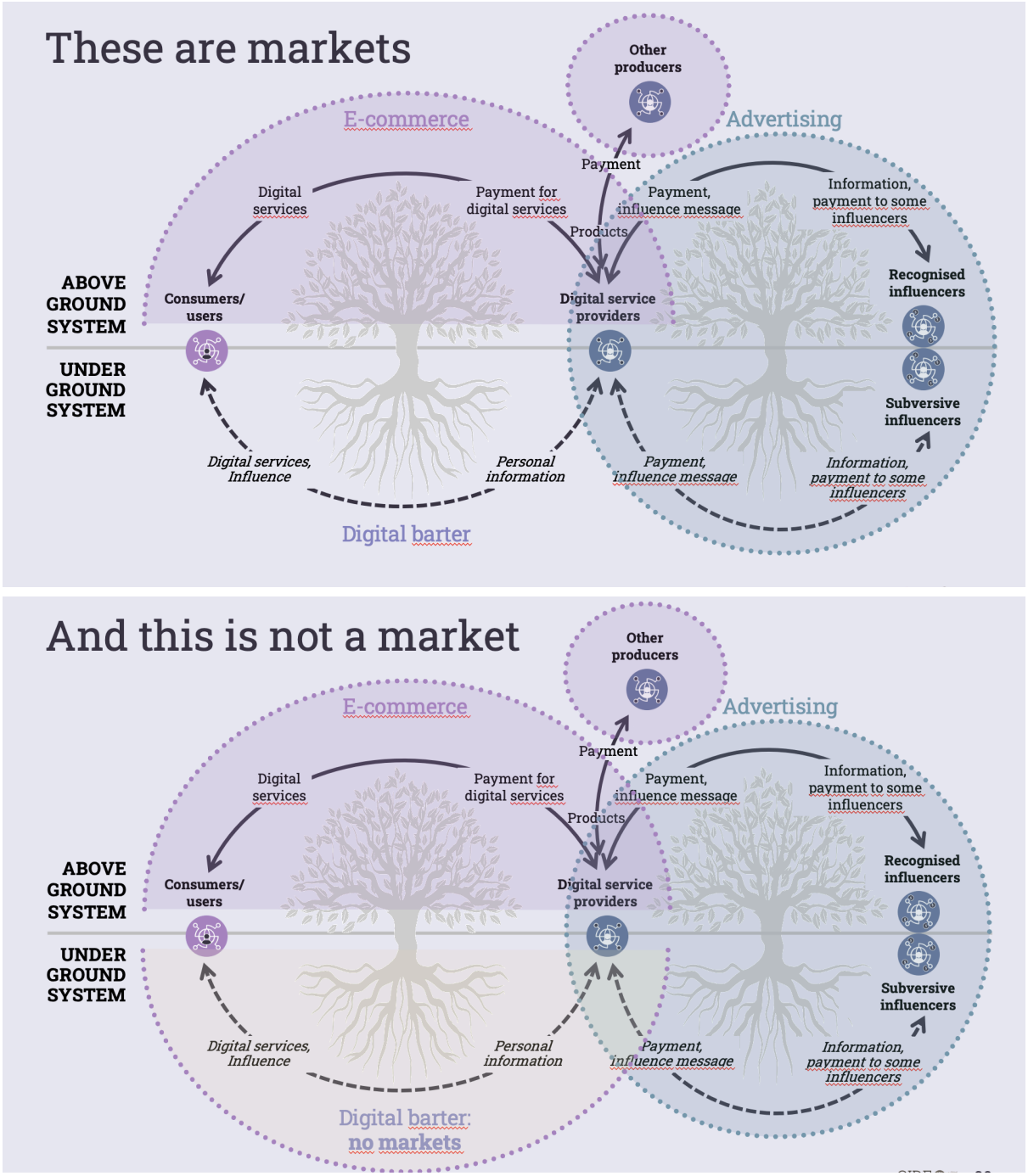
[2] To be developed country by country. For example, in Europe: the European Digital Identity Regulation (Regulation (EU) 2024/1183), also known as eIDAS 2.0

- The mental health of many individuals is weakened in many different ways[3].
- The functioning of our economic market system is undermined. The near-invisible harvesting of vast amounts of individuals' information has been in response to only one incentive—advertising—and has established a closed market between monopolistic digital service providers/data aggregators and those who seek to influence users. Consumers and the community are unable to reap the total economic and social value of personal data because of a lack of alternative incentives and negotiating power.
- Innovation in the digital economy is stalled when a lack of transparency and one-sided control over the key resource – personal data – rewards only one set of actors, the digital service providers/ data aggregators.
- The current system exposes consumers, businesses, and governments to widespread fraud and cybersecurity threats; a risk which, unless addressed, will only compound with the aid Artificial Intelligence (AI) ;

These problems emerge not so much from the visible digital trade (e-commerce, etc.) as the invisible digital trade in information and influence. As Figure 1 below shows this latter trade may work with normal market conditions for the influencers, but it is not a functioning market for consumers.

[3] For example, European policymakers have expressed concern that addictive online services can have harmful effects on people, especially children, such as increased pressure, stress, poor sleep, information overload, leading to lower self-esteem, general anxiety disorder, social anxiety disorder, depression, intentional self-harm and suicide. See for instance: European Parliament's Report on *Addictive Design of Online Services and Consumer Protection in the EU Single Market* (Report - A9-0340/2023) and *Report on Mental Health* (Report - A9-0367/2023). This has reflected researchers' concerns. The social psychologist Jonathan Haidt's, *The Anxious Generation*, explores global data on how social media and smart phone interactions has contributing to a Generation Z's mental health crisis. These concerns are also reflected in European research, for instance a 1923 Norwegian nationwide study on time spent on social media and self-harm among adolescents. https://www.nature.com/articles/s41598-023-46370-y

Figure 1



Digital policies are doomed to remain inadequate as long as the consumers of digital services have artificially restricted choices, such as the choice between revealing large amounts of personal data (by agreeing to the terms and conditions of digital services) and being excluded from most economic and social interactions in this increasingly digitalised world. To ensure that consumers do not face artificially restricted choices, giving them control over access to, and the terms of use of, the data about themselves, individually and collectively, is necessary.

Rather than just expecting governments to continue shouldering an onerous burden of trying to regularly update consumer protection/privacy regulation to keep up with technological and commercial changes among data aggregators and influencers, the IDEA moves forcefully to gain the benefits of a properly functioning market through ensuring that residents are active economic participants. Giving consumers the ability to control access, and on what terms, to their data, provides incentives throughout the value chain for economic resources to be allocated in their most productive uses in satisfying consumers' needs. Similarly, promoting such control gives individuals the ability to express social and political views and choices free from a non- transparent environment of implicit manipulation.

This is the basis for true "digital citizenship," in two senses: first, empowering digital consumers to shape their digital experience in accordance with their own objectives and, second, enabling the economic markets to work in an effective and humane and human-centric way in meeting digital consumers' objectives at minimum resource cost. The sense of control over their data and how it is used is also likely to result in improved confidence by people in market, social and political institutions seeking to use such data. This is a political and democratic benefit.

A point of nomenclature

In this paper, we refer to the citizenship and consumer benefits of the IDEA proposals. But to be consistent most legislations, we will refer to people the IDEA applies to as residents (rather than limited to citizens). And to make clear that we seek a significant change in their economic power, we do not refer to people as users but as consumers.

Data governance reform will drive innovation and growth

The proposed IDEA will attract unprecedented economic activity to the digital economy, locally and globally. The reason is simple. The current digital governance system is driven by a large number of data aggregators, and those seeking to exercise economic, psychological, political, and social influence on digital users. The interests of these actors are poorly aligned with those of digital users. The current digital experience creates many problems, from data privacy and security digital surveillance and manipulation to information and market power inequities.

The present digital governance system undermines the workings of economic markets since digital users receive many free (or underpriced) digital services in return for vast amounts of free information about themselves, usually extracted without informed consent and knowledge. This digital barter is financed by economic, social, psychological, and political influencers who seek to exploit digital users' experiences.

Even if processing personal data in targeted advertising is at risk of regulatory action, data, particularly inferred data, is still used by a large number of actors who hardly ever have a direct relationship with consumers. These include financial institutions, healthcare providers, retail and e-commerce, automotive companies, and technology and AI companies. Many of these companies also participate in the contextual advertisement market.

Digital users have become distrustful, disempowered, and politically and socially divided as a result. Furthermore, they need the right incentives to promote the further development of the digital economy. They remain engaged in the digital economy due to the gains from digital connectedness. Still, they have no choice but to accept the terms of digital service providers in return.

The proposed IDEA empowers digital users to exchange information about themselves on terms that they, via their representatives, have chosen. It creates new market structures that will enable innovation driven by the interests of digital users. Such a fundamental rebalancing will generate unprecedented flows of economic activity, as the countries will create the market structures to allow the needs and purposes of digital users drive digital services rather than the other way around.

Figure 2

The Value of Data Ecosystems

A recent UN study has affirmed the value of encouraging data ecosystems[4]. These benefits range across four inter-related categories:

Economic Benefits: Data creates real value through new economic and impact opportunities, and cost savings through everything from process efficiencies to reduced corruption; analysis of past investments has shown an average return of USD 32 for every dollar invested.

Social Benefits: Data can save lives and enhance the quality and equity of living standards by increasing the effectiveness of social programs; for example, data fosters stronger and more effective health systems, higher rates of attendance and performance in schools, more proactive and anticipatory action to climate or humanitarian emergencies, and much more.

Environmental Benefits: Data can bolster the transition to sustainable development, shedding light on the drivers, rates of change, and impacts of environmental issues.

Institutional Benefits: Public data systems support evidence-based decision making and provide the information needed to hold institutions accountable.

[4] *Investment Case: Multiplying progress through data ecosystems.* A Data With Purpose publication, United Nations and Global Partnership for Sustainable Development Data https://www.data4sdgs.org/sites/default/files/file_uploads/Investment%2Bcase_Multiplying%2Bprogress%2Bthrough%2Bdata%2Becosystems_vFINAL.pdf

The monopolistic power of giant data aggregators based on massive data lakes of personal information will be diminished when start-ups and smaller businesses can make propositions to large numbers of potential consumers through their skilled representatives The ability of start-ups and smaller businesses to connect with large numbers of potential consumers through skilled representatives will enhance competitions. This will empower these businesses to thrive, while creating a more balanced digital markets.

Moreover, as the proposed IDEA enables consumers to shape their online experience, it will raise the level of transparency and agency to help consumers keep pace with rapid technological change, also bringing vast benefits to businesses by ensuring accurate and first-hand customer information, reducing the likelihood of fraud. The resulting digital market dynamics, driven by consumer choice about personal data use, would fuel innovation and new business creation to meet the newly revealed consumer demands. In markets with consumers empowered by expert advisors, information about products and services, their true price in terms of demanded personal data, and quality becomes more transparent.

The resulting rise in economic activity would provide new incentives for R&D and influence the adoption of new technologies and AI systems. Companies will be driven to greater customisation and personalisation of their products and services. However, this would now be driven by consumer choice rather than by the profit opportunities of digital service providers. New business models would evolve, including novel approaches to better meet consumer needs.

Governments and multilateral organisations have a role in protecting consumers through evolving rights built on a foundation of consumer protection reforms. However, rather than having to play catch-up after several electoral cycles, governments will be able to have confidence that the negotiations on behalf of consumers will resolve many of the consumer's concerns.

Implementing the IDEA will provide an impetus for more countries and regions to follow suit or suffer competitive disadvantage in digital service markets.

In the long run, the IDEA would make all digital market participants – on both the demand and the supply sides – better off since all would benefit from the surge in economic activity. In the short run, however, it is plausible to expect resistance to the IDEA from digital gatekeepers powerhouses since it would strengthen the market power of digital consumers via their representatives relative to these digital service providers. These providers characteristically argue that the value of individual personal data is negligible. In contrast, the lion’s share of the value lies in how this data is used to provide digital services. In response, it is worth noting that the same may be said of global value chains: the value of an individual worker’s input is negligible but instead resides in the value chains themselves. But just as this argument is not used to justify not paying workers their wages, it should not imply that digital users should not be compensated for their data, in money or kind, if they see fit. Some of this compensation will be economic; many may not be.

A well-structured framework within the IDEA can better protect human rights and the welfare of individuals by ensuring that data is managed with a focus on their particular interests and desires. By embedding these principles into the core of the digital economy, our framework can safeguard personal freedoms and enhance the overall well-being of

consumers. This commitment to human rights and welfare establishes a foundation of trust, which is crucial for fostering a secure and transparent digital environment.

What should be in a digital economy innovation regime?

With support from more than 70 researchers, policy experts, civil society advocates, digital trade, and internet technical and security experts from 24 countries, GIDE launched in 2022 the report *Empowering Digital Citizens: Making Humane Markets Work in the Digital Age*[5]. Building on existing digital legislation and the progress of national e-identity systems, and following a broad consultation among stakeholders, our proposals have evolved into a regulatory framework, the IDEA, that will deliver the following outcomes:

Envisaged Outcomes

- All personal data seeking entities will initially only access Key Personal Data (verified by trusted parties) from consumer-controlled sources and ensure that all entity customer records are auditably derived from such sourced data;
- Consumers will have greater understanding and confidence in the companies with whom they interact, as they have authorisation, access, and control of what data they share, with whom, and under what conditions;
- Both users and companies will have reasonable expectations that Key Personal Data collected is dedicated to its specific purpose and is verified by trusted third parties, certified, up-to-date, and auditable;
- Skilled agents will help educate consumers about how their interests can be better balanced. In return, consumers will ensure trusted third parties verify their data;
- Confirmed rights of association and representation will enable skilled agents to negotiate on behalf of millions of individuals for equal use and financial and other terms with large data holders. Collective representation contributes to economic competition and the kind of market segmentation that fosters innovation;
- Companies, associations and civil society organisations will be able to build on traditional skills in personal professional advice to build significant skilled agent businesses;
- No organisation will hold Key Personal Data on an individual without that person's knowledge and consent unless as prescribed by law and for clear exceptions, such as public security, law enforcement, and national security;
- Attempts to influence online experience will be aligned with users' decisions about the balancing of their interests and consequent negotiated terms;
- Efforts at disguised economic, social, psychological, or political manipulation will be in breach of contract and the proposed IDEA. It shall also be auditable;
- Entities that infer information about an individual from data that the consumer does not create will be bound by new fiduciary rules and will be allow to only process data in the best interests of the data subject;
- The opening up of access to and control of data to the many will support a renewed flourishing of innovation and scientific development;

[5] https://thegide.org/empowering-digital-citizen-report/

- Online markets will enjoy enriched competition when start-ups and smaller businesses can make propositions to large numbers of potential consumers through their skilled agents;
- Similarly, the mechanisms for establishing various data commons will be simpler as proponents have a simpler path to approach millions of potential members through their skilled advisers/agents;
- Renewed oversight and audit rules will be in place for data aggregators and large business end-users to ensure compliance;
- Further help enforce existent data protection measures to safeguard personal information and prevent misuse. This will help build confidence among users and stakeholders, encouraging greater participation in the digital economy and improved human rights compliance via consumer controlled data sharing.

Putting the components in place

Building on the rights established in a series of recent digital legislations, the IDEA will establish:

- Requirements which will transform users into active economic consumers who have the ability to control how their data is used in return for terms they value;
- Renewed rights of association and representation of consumers for their being able to take advantage of both expert advice and economies of scale; and
- Regulatory frameworks to incentivise an industry structure where power shifts to the consumer while ensuring a large scale, speedy and accurate interactions for business and public entities.

Ensuring users are empowered consumers

Key Personal Data

To avoid conflicts with the broad definition of personal data, it is crucial to include a comprehensive list of data requiring trusted-party verification – "Key Personal Data". A definitive list will emerge from consultation. The data categories managed in digital wallet frameworks can inform this list, but are not exhaustive of categories. One guide would be data normally required for entering into a contract or satisfying governmental or major identity requirements. This is a subset of what is commonly understood as Personally Identifiable Information. The following could be examples of Key Personal Data:

- Name: full name, maiden name, mother's maiden name, or alias;
- Personal identification numbers: social security number (SSN), passport number, driver's licence number, taxpayer identification number, patient identification number, financial account number, or credit card number;
- Personal address information: street address or email address;
- Geolocation;
- Personal telephone numbers;
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting;

- Biometric data: retina scans, voice signatures, or facial geometry;
- Information identifying personally owned property: VIN or title number;
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person.

Consumer-controlled Sole Source of Key Personal Data for Processing Purposes

A digital economy innovation regime requires that all entities access Key Personal Data from authenticated user-controlled sources. The appropriate offline analogy is the use of an ID card, for which agents (such as hotels) are legally required to collect the data verified on the card only from this authoritative source. Similarly, in most cases, a passport is required to cross a border. The data on the passport could be sourced by the receiving immigration officers from any other source, but to ensure the integrity of the broader system, the law requires it to be sourced only from an authoritatively issued passport.

The key is that, legally, consumer-controlled records, verified by trusted parties and held in trusted data repositories, are the single source to be used by those who want to process Key Personal Data. This mechanism enables individuals to restrict data aggregators to using only Key Personal Data obtained from a source that is under the individual's control and according to approved terms.

Why does the single source matter? Because it provides the system with a unique legal representation of the individual (not the vast number of versions of the individual which exist with rough functional equivalence in the present ecosystem, many of which the individual does not know exist). And uniqueness means that not only is control of access more easily achieved, but it also bolsters the leverage of the individual – or her agent – to negotiate with companies the financial and use terms for access to this data. It is the fulcrum on which the power between the data aggregator and the individual can be adjusted.

Important public equities

No organisation will hold Key Personal Data on an individual without that person's knowledge and consent unless as prescribed by law and for clear exceptions, such as public security, law enforcement, and national security.

Importantly, the IDEA proposal is silent on the concept of individual ownership of personal data. What it seeks to establish is the right for the individual’s control over who has access to Key Personal Data on and under what terms.

Key Personal Data Authentication

The IDEA will establish rules requiring consumers to authenticate Key Personal Data and the process and types of trusted third parties on which consumers can rely. These guidelines will also standardise practices for encrypting data, preventing unauthorised access, and maintaining data integrity throughout the processing lifecycle.

Best Interest of the Data Subject

The IDEA also foresees that actors who process personal data about individuals that is not Key Personal Data, such as data inferred from IoT data, must do so in the best interest of the data subject. Governments should extend the offline fiduciary obligation to act in the best

interest of data subjects which is applied to doctors, teachers, lawyers, or government agencies to digital service providers and ensure data is processed in the best interest of the data subject. It is essential to include fiduciary duties for data controllers and processors explicitly, aligning their actions to uphold data subjects' fundamental rights and interests. An objective test, grounded in human rights law, should ensure that interpreting the "best interest of the data subject" is not open to differing interpretations. An audit requirement should be added to existing to corporate and public entity audit regimes to ensure that such data is controlled and/or processed within the defined duty of care.

Protecting Vulnerable Populations

The requirement to process personal data in the best interest of the data subject should be expansively applied to vulnerable populations, such as children, elders, displaced and homeless people and immigrants. The proposal below for fiduciary representatives to help consumers is particularly important for these populations where the required expertise will be both in the social circumstance of these populations and the personal data markets.

Establishing Effective Rights and Incentives for Representation and Collective Association

A digital economy innovation regime foresees skilled entities representing users' interests in proposing and negotiating data-sharing and benefit-sharing options in return for access to users' Key Personal Data. This is important if handling consumers' Key Personal Data is to shift from digital husbandry to a more properly operating market in which the users are participants. Those with skills in data aggregation, analytics, and online advertising presently overwhelmingly serve data aggregators and influencers. It is not feasible that each user should ascertain this knowledge – hence the benefit of collective representatives who can bring similar skills to the interests of consumers. Establishing empowered consumers with a market structure for skilled advisors, incentivises people with these skills to move across to serve consumers.

The process of negotiating the terms of authorisation – who has the right to access an individual's Key Personal Data records and on what conditions – is the crux of re-empowering consumers. This ensures that they are aware of who is collecting data on them and to set directly, or through an agent or collective bargaining, the terms on which they allow such data to be collected and used – including the right to refuse such collection. This is a principle which builds on the existing data protection and privacy rights for an individual to be informed about the collection and use of the individual's personal data.

The consumer, through the advice of an expert agent/representative, could set the terms under which he or she receives and approves/denies requests from companies/entities to access and use the consumer's Key Personal Data records. Such an agent principle reflects the rights of association and of collective representation. It also rewards scale or specialisation by expert agent/representatives in negotiating the best/most tailored terms with various types of data collectors. Some of these terms will be financial, many may not be. [6]

[6] For instance, financial benefits could come from decision enablement for both the consumer and a data seeking services provider which could result in significant cost reductions for the services provider and be rewarded through discounts, increased buying power, lower interest rates, carbon offset, loyalty rewards etc.

It is not feasible for each user to ascertain enough knowledge to negotiate individually with data aggregators, especially if the user is of a vulnerable group. Collective representation and transparent data practices help individuals understand how their data is processed, fostering trust and confidence in digital services.

Nobel Prize-winning economist George Akerlof famously pointed out how information asymmetries undermine markets. Skilled people are essential to getting information to both sides of a properly operating digital market. In this way, we envisage that some lessons from the last 200 years of how collective representation of workers changed the labour markets and how fiduciary agents transformed the financial service and pension markets will be instructive in the personal data market of the twenty-first century.

Possible Individuals' Skilled Advisor/Representatives

Companies, associations and civil society organisations should be able to build on existing customer relations, billing systems to support value exchange and traditional skills in personal professional advice to build significant skilled agent businesses. Some entities which could be well positioned to play the skilled advisor/representative role include:

- Telcos
- Regional banks
- Co-operatives
- Professional associations
- Accounting and legal firms
- Industry associations
- Banking, Insurance and financial service fiduciaries
- Unions
- Civil society organisations
- Collection agencies
- Domain name registrar
- Regulated agents with existing fiduciary duty (e.g. health entities).
- Industry-based independent advisory agents (e.g. auto and mobility)
- Existing or start-up companies focused on data management and protection.

The IDEA will establish a regime for accreditation of such consumer advisor/representatives which will operate in a competitive market to attract consumers. Drawing on the experience of other fiduciary regimes, the IDEA will set rules on disclosure, transparency, fiduciary standards, conflicts of interest and fair dealing with clients. Through either public regulators, or a professional association of advisor/representatives, continuing professional education will be required and offered to agents, as well as materials for consumer education awareness.[7] Similarly, public regulators or the professional association will coordinate a complaints and complaint resolutions mechanism.

[7] Such training will need to adapt as advising evolves to be AI enabled, at least partly automated and be based on being able, with permission, to access various data sources to provide integrated and informed decision guidance.

The IDEA will also establish rights of association and representation to ensure that groups of digital consumers can establish digital customer associations to play these roles - digital-data manifestations of fundamental international standards on freedom of association and collective bargaining. Some lessons could be drawn from how collective representation of workers changed the labour markets in the nineteenth and twentieth centuries and how the International Labor Organization's Conventions provide discretion for such associations to constitute their rules and procedures and protect them from State interference. Presumably digital consumers' associations would themselves predominantly operate on a digital basis. They could be organised according to a provider (e.g. "Provider X's Consumers' Association") but ideally would be organised and bargain with main digital service providers and associations of smaller digital service providers.

Obligation to negotiate in good faith

If an accredited advisor/representative provider has indicated an intention to bargain on behalf of its consumer members/clients for access to their Key Personal Data, a responsible digital service provider and the accredited advisor/representative provider must negotiate in good faith. Breaches of this requirement should be subject to a significant civil penalty.

Advisor/representatives organisations shall be able to form groups to collectively bargain with the digital service providers. Smaller digital service providers shall also be able to form groups to negotiate with advisor/representatives.

A process for ensuring that negotiations close without distortion by power asymmetries will need to be put in place. For instance, international models have emerged for negotiations to proceed for some months, and if inconclusive, then proceed to meditation and then binding "final offer" arbitration.[8]

Industry Structure

The IDEA foresees a business ecosystem to implement these proposals which would likely have a market structure similar to other very large scale Business to Business to Consumer industries. Some examples include the mature Domain Name System (DNS), the credit card processing industry, the travel booking system, and some countries' retirement income systems. The consumer is likely to engage a consumer-facing expert advisor/representative services enterprise that manages the details of consumer preferences and negotiates terms on behalf of and consumers. These advisor/representative enterprises will recruit consumers and producing various degrees of specialisation and services in negotiating terms for the use of that data. Such specialisation will also aid to the development of consumer needs-based segmentation, and hence various different terms and agreements between consumers and digital service providers. The consumer-facing enterprise would pass the registration of the consumers details to a specialist, secure data registry, which would manage the requests for the consumer's data from the myriad of entities with whom the consumer interacts according to the terms set by the consumer.

A relevant analogy is the Domain Name System (DNS) – the Internet's backbone "look-up table". Using a hierarchical and distributed set of databases, including data supplied by

[8] One such model the Australian rules is for negotiations between platforms and media companies for media content

Internet companies and consumers, enables billions of requests from people and Internet of Things devices to be resolved – resulting in data being transferred and websites being presented. Consider that loading one page of an e-commerce website can result in more than 50 DNS requests – all of which resolve in a fraction of a second. And that process takes place billions of times daily as the world surfs the web. This gives a sense of the scale and robustness of the DNS.

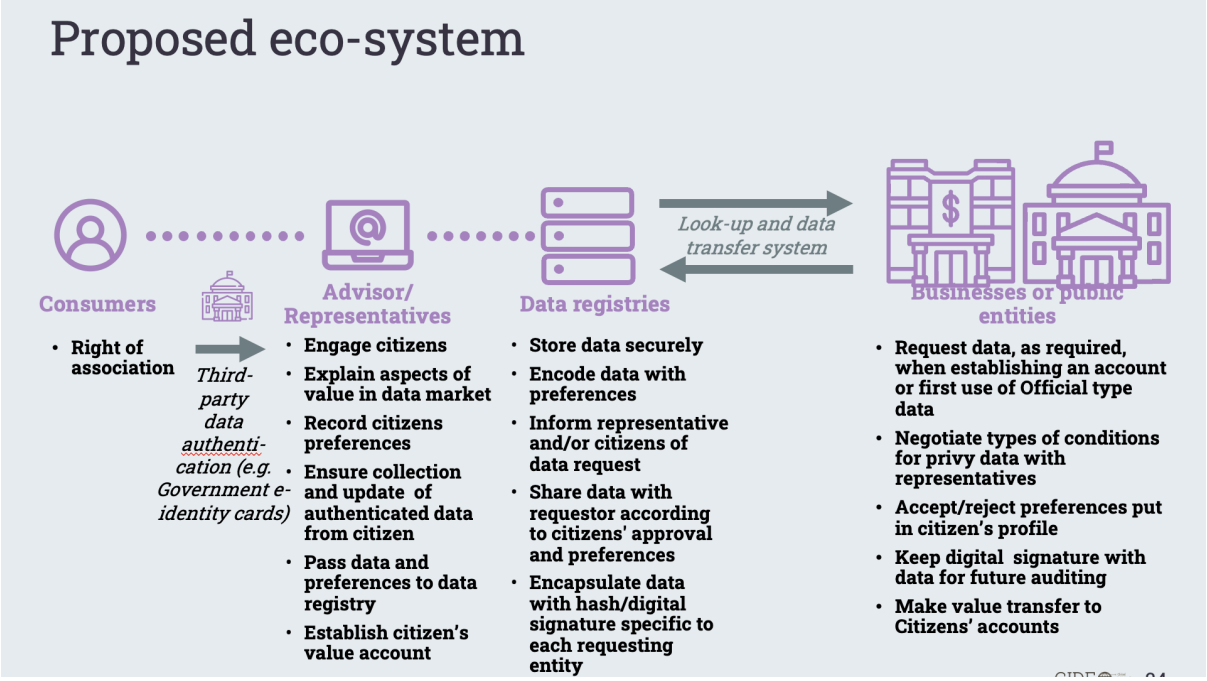
Many registrars run the customer-facing service, while a smaller number of registries handle the storage of the core DNS data and the management of high-speed resolution of queries to that DNS data. The resolution process is very quick and highly scalable. The DNS also supports the encryption of data queries.

The registry function, including storing the records and maintaining the security of the data at rest, could also draw lessons from the current Payment Card Industry Data Security Standard model in North America. After several notorious data hacks of credit card data from retailers, the industry changed the structure so that stores no longer maintain credit card information. Instead, once the customer supplies her credit card information, the seller passes it to another specialist provider who maintains all the information about the customer's credit card. The credit card processor is responsible for data transmission and security; it processes the payment and returns the confirmation to the store.

Credit card processors' security standards are detailed and now world-leading. A similar approach could be taken for the storage of Key Personal Data. While the Internet's Domain Name System is a useful model for the distributed, high-speed resolution of queries for authoritative data, other technologies and processes can also be used.

This industry structure is outlined in Figure 3

Figure 3



The components of the proposed system are:

- authentication and hosting of the collated Key Personal Data;
- a legal obligation for all companies/entities to source official type data only from the consumer-controlled record;
- the advice to consumers from their expert advices and the negotiation of terms with digital service providers by the same representatives
- the placing of consumer preferences and negotiated terms in machine readable code
- authorisation for access according to negotiated terms;
- businesses or public entities implementing their initial Key Personal Data request;
- businesses or public entities ensuring up-to-date upgrades to the data; and
- the auditing of businesses or public entities to ensure the use of Key Personal Data is consistent with the regime set out above.

Role of expert advisor/representatives and specialist data registries

The markets for expert advisor/representatives and data registries will be competitive and require clear rules for data transfer for consumer roll-overs. Operators in both parts of the market will be agents for the consumer – the IDEA will set out the fiduciary obligations of the operators, drawing from the accumulated lessons from financial services and similar industries. It is likely that there will be structural separation of ownership between expert advisor/representatives and data registries. For the purpose of GDPR, the advisors/representatives will work with residents and will be data controllers. They will also be data processors. Data registries will be data processors under the GDPR and data holders under the Data Act. The data registries will also be informed by the current data intermediation service provider provisions of the Digital Governance Act.

As in the other large scale markets, the consumer-facing advisor/representatives will pay fees to specialist data registry operators for each individual's data registered through their service. The details of the consumers Key Personal Data and related terms for access and access rules would be passed to the secure data-holding registry for hosting and for managing the authorisation process when a data requester wants the consumer's personal data.[9]

The advisor/representatives will be responsible for assisting the consumers to fulfill their obligation to ensure that the consumers' data is accurate and up to date and the data registry will ensure that requesting entities have access to up-to-date upgrades to the data.

The advisor/representative provider will provide the consumer with pathways to draw authentication for each piece of data from the appropriate layer of government, educational institutions or other recognised bodies. (Indeed these entities may provide verified data directly.) This authentication would be in the form of a digitally signed document with a digital certificate issued by the authenticating body or a variable credential as part of country based digital wallet specifications. The data can then also be signed with a digital certificate issued by the service provider. These signatures ensure a digital "paper trail" as to the authenticity of the records and where the authentic copy is stored.

As an added protection against possible political manipulation of authorisation in a sub-jurisdiction, a governmental body could also establish an institution to sign the government certificates (and implicitly audit the certificate authorities at the sub-jurisdictional level).

The specialist data registry will be responsible for enabling requestors to receive authorisation and then the sharing of Key Personal Data and associated negotiated terms of use in machine readable format.

The digitally signed data would be transferred to the requesting company from the data holding provider together with a machine readable summary of the permissions agreed by the user. These could take the form of an attached transaction-specific electronic contract certificate outlining the terms of contract agreed for the use of the data. Such electronic contact certificates are already used in the real estate, trading and labour services markets.

The data service provider would also attach a tag/electronic certificate to at least part of the data being shared saying "this is Key Personal Data." Using similar technology to existing digital rights management, this tagging will enable receiving servers to determine if it is the sort of data their users can access, or to decide if this is data which should not be received. In this respect it would be similar to the classified document regimes used by governments which only allow delivery depending on the classification of the material.

Another benefit of attaching digital signatures/hashes to the transaction-related holdings of an individual's Key Personal Data by an enterprise is that stealing a company's database of customer records would be far less valuable to criminals than it is today. Unlike now, such

[9] One of the most effective means of meeting the request may be micro-transactions or API calls which are scalable and very cost effective, therefore the requesting entitles are not paying for the "data" they are exchanging value for the immediacy of accurate, real-time, verified, in-context data to complete a specific outcome, e.g. approve a mortgage.

records would not be fungible – but specific only to that company and the transaction. The value of the database to other criminals for other uses, such as phishing, would be considerably diminished.

Any payment from an entity seeking personal data (according to terms set out in the agreement with the consumer) would take place at the time of data transfer. It would be collected by the data registry and transferred to the advisor/representatives who will maintain a value account for the consumer. Such an account may keep a record of all monetary and non-monetary benefits the consumer has achieved through the sharing of Key Personal Data, and from whom.

Specific rules for lawfulness of processing personal data

Consumers must embed their preferences into machine readable code before giving consent, ensuring that consent is effectively informed and reflective of the individual's preferences. Automating consent processes enhances the autonomy and control of data subjects over personal data. It also reduces the time required for individuals to manage their preferences across various platforms.

Specific rules must be established depending on the lawful basis for processing data. For consent-based processing, lawful processing should be presumed when business or public entities adjust their processing, (including websites or platforms) to reflect consumers' embedded preferences. For contract-based processing, lawful processing should be presumed if a consumer's advisor/representative negotiates the terms with the data aggregator, with the agreement of the consumer, and they are reflected in machine readable code processed by the data registry.

Technology

The IDEA will not pick a technology to implement these policies. The Framework will encourage an industry standard development or in the failure of such, promote technological competition providing there is full interoperability.

The IDEA proposals recognise the extensive work among the standards community for the last decade that has provided clarity on protocols, credentials, signing, schemas, interoperability, scalability etc.

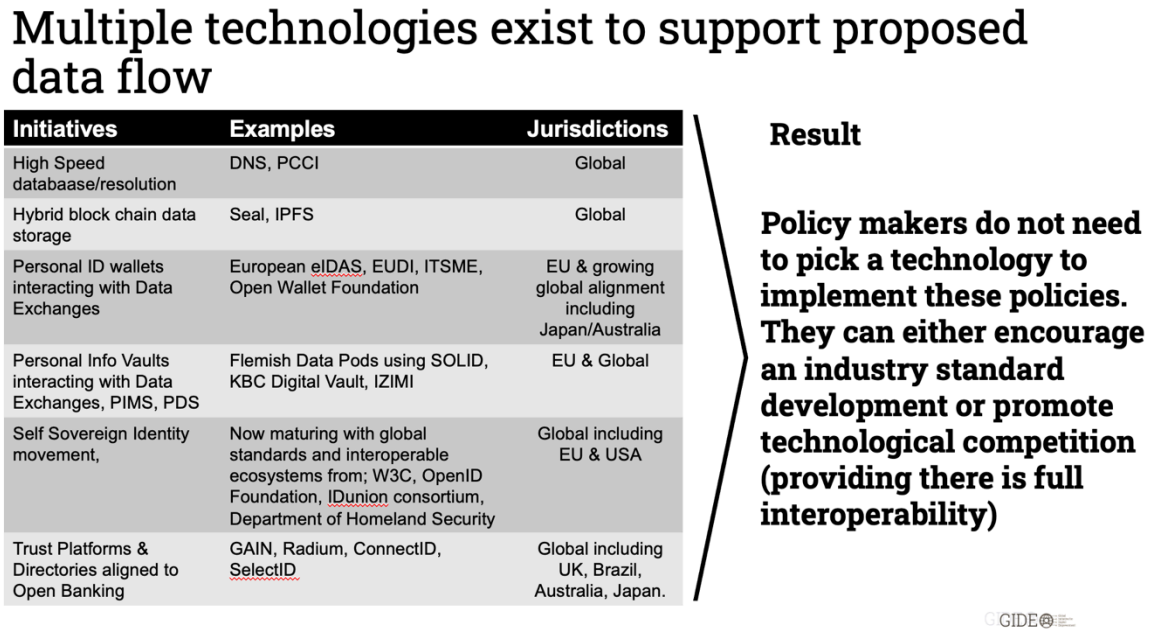
Digital Identity Wallets are designed to support verifiable credentials which are designed to be tamper proof and can support machine readable rules as described in the IDEA.

The implementation of the recommendations could also draw on the lessons of Personal Information Management Systems (PIMS), and the related Personal Data Stores (PDS), which have been implemented on a modest scale to improve the portability and interoperability of systems using personal data. One of the value of PIMS and PDSs is that are flexible and can enable a range of data formats; documents, attributes, photographs etc.

However, for Key Personal Data it will be important that its typical attributes be verified and able to be requested in a specific schema in order to complete a transaction.

Whatever the outcome, the system(s) selected will need to be very large scale and ensure very little latency in what will be a very high level of transactions.

Figure 4



Costs

Considering the huge scale of covering all consumers, and drawing from the experience of the DNS, we expect that the per record operational cost of the data registry function could be in single digit euros per year. There would be significant capital costs in establishing such a registry, but existing large-scale data processors would be in a strong position to establish a sister registry business. The cost of the advisor/representative function would vary according to scale achieved by each enterprise and the resources they dedicate to negotiating terms for consumers. Only in agreement with their member consumers, advisor/representatives could receive payment from third parties to present digital service opportunities (e.g. joining a medical research data commons). The DNS registrar market has shown that the customer facing service provider can also develop other offerings of value to their consumers while still be consistent with their primary advisor/representative purpose. Indeed competition over time has driven down prices for both core and supplementary offerings from the registrars. Overall, it is feasible that once the IDEA regime is established the annual cost to supply these services could be similar to that of a take-away coffee. We do note pricing in competitive markets varies above costs and will change according to the value offered by the advisor/representative.

Start-up Incentives

Several incentives should be implemented to encourage participation in both parts of the market and ensure effective representation. Financial support to help meet start-up costs for entities seeking to be either Advisor/Representatives and specialist Data Registries would

provide a tangible reward for their efforts, making establishment of the market more likely and sustainable. Access to specialised training and information resources would also further empower advisor/representatives, equipping them with the necessary skills and knowledge to perform their duties effectively.

It will also be important to similarly incentivise the verifying parties to put in place the assets and processes to swiftly verify data so that the parties that will be able to rely on the data.

An important short term goal on the new digital economy innovation regime will be to ensure rapid consumer adoption. This will be largely driven by the requirement for businesses and public entities to access Key Personal Data only from the consumer-controlled source in the Data Registries. But to also accelerate the education of consumers of their role in this new market, it would also be useful offer an initial small subsidy per Resident to fund transition as a customer of the of Advisor/Representatives and specialist Data Registries. This subsidy could be for each consumer to help them pay any initial fees. Over time it is expected that the value the consumer will receive more value (including financial value) from the new market dynamics than the price to them.

Such a consumer subsidy would be similar to effort countries are making to sway consumer interest towards funding the transition to more renewable sources of energy and transport.

Businesses or public entities seeking Key Personal Data

The initial implementation of gaining authorisation to consumer Key Personal Data by most businesses or public entities will be straightforward. Similar to what the European Union did during the GDPR implementation period, business will email or otherwise message their customers asking them to nominate their data service providers and seek permission for accessing the Key Personal Data. Or when they were engaging a customer for the first time, they would request the Key Personal Data fields to be completed from the customer's nominated Data Registry. This process will also result in the download of the consumer's standard preferences about the use or the data or generate a request by the consumer's advisor/representatives to negotiate terms for use.

The IDEA will also call on advisor/representative providers to form a group(s) to draft a common set of minimal terms for use which is to serve as a recommended template for terms presented to Small and Medium Enterprises. Such templates require review and approval by an appointed arbitration body.

As explained above, to ensure that companies are able to prove to auditors that they have sourced the Key Personal Data only from the authenticated records held by the individual's data registry, it will be necessary for that registry to digitally watermark or fingerprint the record to say from where the record has come. This provision is additional to the layers of digital certification outlined above. The legal structure to support this obligation will also require entities which receive Key Personal Data from another source not to use it and to report the source to authorities (similar to the regime concerning receiving stolen property).
The watermarking/hashing of the Key Personal Data transferred for a specific agreement provides an easy mechanism for auditors to check if such types of data held by a business or public entity is in accordance with the IDEA.

Application to AI actors

Acknowledging the risks and benefits brought by the development of artificial intelligence (AI), the provisions of the *IDEA* will also apply to the application of AI systems to personal data and also to the collection and use of Key Personal Data in machine learning datasets.

It is important to ensure that AI providers embed fiduciary rules into their AI processes and tools. These rules will create a legal and ethical obligation for AI providers to act in the best interest of data subjects, and/or under the terms negotiated with consumer representatives. We have already seen examples of the benefits of collective representation, for instance, in how the Writers Guild of America successfully negotiated contracts featuring strong guard rails on how AI can be used in the US film and television industry.

Accelerating a humane personal data markets

We would argue for two pillars to a humane digital market: the rules and empowerment to ensure that individuals and businesses (in various combinations of demand and supply) operate effectively as balanced parts of a market; and the rules to protect the vulnerable and ignorant from being exploited in such a market. Over the last Commission, the European Union put in place both important rights to establish a single data market and also important protections for individuals.

The IDEA regime puts in place an additional market mechanism and incentives to practically build a consumer driven data market and unleash widespread innovation in the digital economy and society. Importantly, the role of skilled advisers/representatives also creates a resident-serving mechanism for educating residents and helping them proactively defend the critical rights passed in the five foundational pieces of legislation. IDEA also extends the protection for individuals by calling for actors who process personal data about individuals that is not Key Personal Data is done so in the best interest of the data subject.

Who benefits?

The IDEA's proposed reforms will ensure fairer and more transparent participation in the digital economy by consumers and businesses. Further they will drive a new wave of innovation and growth driven by more participation and choice by consumers as to how their data is used and rewarded. The IDEA will constitute an important step towards promoting market efficiency, reducing manipulation and inequalities, enhancing protection of privacy, driving diminished fraud and improving cybersecurity. Importantly, the proposals aim to mitigate the digital husbandry of residents and thereby promote the fundamental liberties, solidarity, and personal agency that are essential for human wellbeing in empowering and socially cohesive communities.

The direct beneficiaries of the IDEA changes are: the economy as whole, consumers, enterprises, start-ups and small and medium-sized businesses, data commons/public benefit data analysts, new participants in the expert advice/representation function, data centres and registries, and even digital service providers.

Economy as a whole

By incentivising companies to share benefits with consumers in return for negotiating access to more of their Key Personal Data, the IDEA should be a significant driver of product and service innovation as well as fueling competition. The IDEA will also achieve greater data sovereignty and literacy in a global online ecosystem by giving each resident more expert advice and greater control over where their personal data is processed.

As noted above, the present digital governance system is driven by a large number of data aggregators, and their influencer customers seeking to exercise economic, psychological, political, and social influence on digital users. The interests of these actors are poorly aligned with those of digital users, overwhelmingly relying on the creation of services driven by advertising and on-selling users' data. The current digital governance system spawns a range of problems, from poorly appreciated digital surveillance, a loss of privacy and widespread manipulation to disinformation and market power inequities. Digital users have become distrustful, disempowered, and politically and socially divided as a result.

The new market structures proposed by the IDEA will generate a wave of innovation and renewed competition that promotes the interests of digital users. It will attract unprecedented flows of economic activity as the countries will create the market structures to allow the needs and purposes of digital users drive digital services rather than the other way around. This market process will also incentivise companies to provide innovative services while also offering the individuals clearly defined and mutually agreed benefits.[10] Unsolicited Key Personal Data collection on individuals would no longer be incentivised.

Two new market forces will drive new growth and innovation:

- a new market, driven by new companies and business units of existing businesses, that delivers personal digital-life advisory services; and consequently

---

[10] One international practitioner points out that outcomes made possible through establishing trust and enabling personalisation and better decision making, result in at least two important business models:

1. Net New Value: Enabling digital trust through mediation, verification and risk mitigation services. Typically, a trusted party pursuing this business model will be able to:
    - Verify data at source
    - Prove provenance or data integrity
    - Manage risk
    - Mitigate fraud
    - Connect and authenticate parties in a trusted ecosystem
    - Provide infrastructure, governance and/or business rules
    - Enable audit and dispute resolution

    2. Time to Value: Enabling higher productivity through reduction in costs and time to value across digital channels. Typically, a trusted party pursuing this business model will be able to:
    - Reduce time and friction when onboarding to a service
    - Provide service orchestration reducing the need for over collection of data
    - Improve customer experience and reduce back-office processes
    - Manage data consent and compliance
    - Enable compliant access to data for pricing and personalisation
    - Connect network actors under a common business framework and/or scheme
    - Incentivise, reward and protect data subjects including decision enablement.

See https://www.meeco.me/resources/business-models

- a spawning of new models for the use of personal data in the single market, where the needs and purposes of digital users drive digital services rather than the other way around.

These will incentivise for new players to enter the digital markets. Able to swiftly access authenticated Key Personal Data on their customers, new companies shall be able to offer new services aligned with consumers negotiated preferences for use. This, to a significant extent, will undermine the moats that existing data aggregators have built around their companies through unsolicited data collection.

Such innovation will not just be for consumers' financial interests, but also for their social benefit. A new market structure will lower the barriers to entry for a broad range of data commons and public-good use of personal data. Promoters of data commons will have a streamlined mechanism through the advisors/representatives to recruit consumers to share their data for the public good.

Consumers

The IDEA will ensure residents have real control over the accuracy and source of their personal data, total transparency, and choice as to who and how processes it, has access to it, how it is processed. Through collective action, consumers will negotiate the terms under which personal data is processed. As outlined above, consumers will reap the benefits of having their own advisors and representatives to help them navigate a burgeoning digital life. They will also benefit from the new products and services which seek to meet their needs.

The IDEA requires the creation of a secure, authoritative record of individuals' data. But this is amounts to much less than the present circumstances in which every company, government agency or charity can establish its own avatar of an individual without that person knowing or ensuring that the information is accurate. Requiring that this consumer-controlled authoritative record be used by companies and others significantly reduces the incentive for the continued creation of such avatars. It also ensures both a universal compliance and a competitive focus on the security of collection and storage of such data, which is lacking today.

A single, verified source of Key Personal Data will result in a significant reduction of duplication – both for consumers and for businesses. The second-order effect of this is that the consumer burden of continuous update across an ever-increasing number of providers is reduced, retention of out-of-date data is reduced, and resultant errors or disclosures are also reduced. For consumers it will also promote more convenient switching between digital products and providers.

Enterprises

The proposals above establish for businesses a single point of confirmation for authenticated Key Personal Data about an individual – controlled by the individual but verified by trusted parties. This diminishes the risk of an individual lying about their data. It reduces the risk of fraud from customers, vendors and employee candidates.

Accessing an individual's Key Personal Data, use preferences and negotiated terms through uniquely encrypted machine-readable data protocols from their unique data repository improves efficiency and data security for business and public entities.

For businesses, it will reduce the costs of maintaining accurate data on consumers. Further, products and services should speak for themselves to the consumers, rather than relying on hidden manipulation of consumer behaviour. Consumer data success will depend more on meeting the needs of consumers, negotiated by their representatives, rather than surreptitiously accumulating vast amounts of data about the consumer.

The ability to negotiate directly with expertly advised consumers will also empower important sectors of the economy seeking more control over their own data value chain, (e.g. the automotive industry, finance institutions, etc.)

Start-ups and small and medium sized businesses

The monopolistic power of giant data aggregators based on massive data lakes of personal information will be diminished when start-ups and smaller businesses can make innovative propositions to large numbers of potential consumers through their skilled representatives. They will not be forced to rely on existing digital advertising as the sole mechanism to seek customers or funding.

Small and medium businesses will also enjoy the benefits of reduced fraud and improved security outlined for enterprises above.

Data commons/public benefit data analysts

In the recent round of legislation, many countries have put in place the right to establish a data commons. The market structure proposed in the IDEA puts in place the practical steps whereby individuals can generate, and be easily recruited to participate in, such data commons. To give an example, today if an endocrinologist wished to establish a long term data set to measure the effects of long COVID, the only practical ways to seek participants would be through coordination with patient touch points, such as hospital admissions or doctor visits; or seeking access through national health data records. Both are laborious tasks. But under the IDEA, the doctor could establish a data commons and then approach a range of advisor/representatives' bodies to ask, would any of your members be interested in participating in such a study? The advisor/representatives can conduct due diligence on the governance of the proposed data commons. If satisfied, they can then put to their members as to who would be interested in participating. If members are, they can coordinate directly the data commons. Under this simpler regime, the data commons coordinator only needs to coordinate with a limited number of advisor/representatives to achieve the necessary outreach.

Participants in the expert advice/representation role

The IDEA will rebalance the economic and social power structure in the digital economy by establishing an industry model of expert fiduciary professionals to advise all residents and, if

requested, negotiate on their behalf with requesting entities how Key Personal Data about them can and should be used, and under what terms. By recognising and formalising data expert representatives as a new professional field, the IDEA can help ensure that skilled professionals can assist individuals and organisations in managing their data effectively and ethically.

As pointed out above, national companies, associations and civil society organisations should be able to build on existing customer relations, billing systems to support value exchange and traditional skills in personal professional advice to build significant skilled agent businesses. Some potential participants could include:

- Telcos
- Regional banks
- Co-operatives
- Professional associations
- Accounting and legal firms
- Industry associations
- Banking, Insurance and financial service fiduciaries
- Unions
- Civil society organisations
- Collection agencies
- Domain name registrar
- Regulated agents with existing fiduciary duty (e.g. health entities).
- Industry-based independent advisory agents (e.g. auto and mobility)
- Existing or start-up companies focused on data management and protection.

While data representatives can work on federal level, it is important to recognise that each country has differences in infrastructure and varying levels of consumers' trust in private and public institutions. These differences will affect which data representatives can emerge where.

Data centres and registries

While the IDEA does not pick a technology to implement these policies, it does promote full interoperability. Further, the regime requires a very large scale and high speed data resolution relying on machine readable code to meet millions of requests per day.

Let us explore the European context to give more detail about data resolution could be managed. Europe has 32 country code operators within a single market. These operators alone could constitute an experienced platform of enterprises used to serving customers and resolving high- speed DNS queries. Europe also has experienced traditional and fintech data processors that could bring expertise to the new opportunities in holding securely personal data. For instance, the over 300 members of the GAIA-X ecosystem could be well positioned to service this need. As noted above, European technology leaders in digital wallets, Personal Information Management Systems (PIMS), and the related Personal Data Stores (PDS), could also benefit both in arranging data storage and/or helping others with portability and interoperability of data.

Digital service providers

The introduction of the IDEA would undoubtedly cause a significant change to the business models of many digital service providers. But importantly, it will also provide a market-based approach for these providers to evolve their businesses.

The IDEA does not seek to break up their businesses, unlike other international proposals. Furthermore it gives them a customer-focused approach, over which they would have significant agency, to address the widening sort of issues which are driving a growing demand for government intervention throughout the world. Not all consumers have the same needs for data privacy, expression, age-based protection, and usage parameters. Devising solutions for different segments may be release significant pressure points for increased sovereign risk.

Rather than relying on overarching, prescriptive legislative tests, our proposals prefer a market-based system – but where the individual is a properly empowered and represented market participant. And digital service providers can adopt a needs-based segmentation approach to tailor their services to consumers. Further, as full market participants, both consumers and digital service providers can amend their agreed terms as the market changes – taking the pressure off legislators to play catch-up through regulatory "Whack-A-Mole".

Like other businesses, digital service providers will reap the diminished fraud benefits of the single point of confirmation for authenticated Key Personal Data about an individual. Indeed for many data aggregators having a source of accurate, authenticated and updated Key Personal Data will be a significant boon to operations. Importantly, it offers a mechanism to reduce the lies behind the registration of many extremists, trolls and criminals.

Call to Action

Passing this legislation will establish the practical incentives and industry structure which will deliver much of the consumer empowerment and economic and social innovation envisaged in the suite of rights-establishing digital acts.

Unleashing consumer-driven market forces in the 21st century digital economy will drive the scale of societal and economic innovation and growth in the digital economy that we witnessed in the 19th and 20th centuries through labour-market reform.

Now is the time for a Digital Economy Innovation Architecture.

ANNEX I. A CASE STUDY OF HOW THESE PRINCIPLES COULD BE APPLIED IN EUROPE

How Existing European Legislation Supports the Proposed IDEA

The proposed IDEA aims to complement and strengthen, not replace, existing regulation. Considering the leading role the European Union plays in international digital governance, the proposed IDEA aligns well with principles and the objectives of the GDPR, DSA, DMA, DA, and DGA. Figure 6 shows specific legal provisions that support the goals of the IDEA. The following table proposes additional legislative actions which would fill in gaps in the existing legislative framework to help achieve the IDEA Architecture.

Figure 6. How Aspects Of Existing Eu Legislation Support The Goals Of The IDEA

GDPR	Digital Services Act	Digital Market Act	Digital Governance Act	Artificial Intelligence Act	Data Act
The Right to Information The Right of Access The Right to Rectification The Right to Erasure The Right to Restriction of Processing The Right to Data Portability The Right to Avoid Automated Decision-Making	Due diligence obligation for intermediary service providers (Chapter III): Point of contact and legal representatives (art. 10, 11) Obligation to include certain information in T&C (art. 12) Transparency reporting obligations (art. 14, 24) Prohibition of using black patterns (art. 26)	Obligations for gatekeepers (art. 5, 6): Data processing restrictions Business user independence and end user access Legal rights and complaints Data portability and interoperability	Intermediations services governance rules (Chapter III): Data processing restrictions (art. 11, 19) Commercial terms (art. 12) Use and security of data (art. 13, 14, 16, and 17) Transparency rules (art. 15)	Requirements for high-risk AI systems (Section 2) - Article 10	Data sharing restrictions and third-party obligations (art. 4(14)

Framework of
Innovation for the Digital Economy Act (IDEA)

Title I: Objectives and Definitions

Section 1: Objectives

The objectives of the Digital Economy Innovation Act (DEIA) are as follows:

1. Control and Transparency of Personal Data: To ensure that all European residents have comprehensive control over the accuracy and source of their Key Personal Data. This includes providing complete transparency and choice regarding who processes their data, how it is processed, who has access to it, and from where. Additionally, it empowers residents to negotiate the terms of data processing through collective representation.

2. Rebalancing Power in the Digital Economy: To rebalance the European digital economy's economic and social power structure. This will be achieved by establishing an industry model of expert fiduciary professionals who will advise all European residents and negotiate on their behalf with entities seeking their Key Personal Data. These professionals will determine how such personal data can and should be used and under what terms.

3. Fostering Innovation and Competition: To stimulate widespread innovation and competition by creating a new market. This market will be driven by new companies and business units within existing businesses, delivering personal digital advisory services and new models for the use of Key Personal Data in the single market. This approach ensures that the needs and purposes of digital users drive digital services rather than the reverse.

4. Reducing Fraud and Improving Efficiency: To reduce fraud and enhance efficiency by requiring European residents to ensure their Key Personal Data is accurate and authenticated by trusted third parties. Additionally, residents' unique data repositories must deliver their personal data, use preferences, and negotiated terms to interacting entities via uniquely encrypted machine-readable data protocols.

5. Enhancing Data Sovereignty and Literacy: To achieve greater European data sovereignty and literacy in the global online ecosystem by providing residents with superior personal expert advice and control over the processing locations of their Key Personal Data.

Section 2: Definitions

1. Best Interest Test/Threshold: A standard used to evaluate whether data processing activities align with the welfare and rights of the Resident. This test ensures that data controllers and processors act in the best interest of the Resident, adhering to their fiduciary duties, including the duty of care, loyalty, good faith, confidentiality, prudence, and disclosure.

2. Machine Readable Consent: A method of obtaining informed consent where a Resident's preferences about sharing Key Personal Data are embedded within machine-readable code processed by a Data Registry acting as the Resident's agent. This mechanism ensures that systems automatically recognize and enforce the Resident's preferences. When a Data Aggregator attempts to access or use Key Personal Data, the embedded code checks for compliance with the Resident's preferences. Consent is granted if the request aligns with the preset conditions; otherwise, access is denied or additional authorization is required.

3. Data Aggregator: An entity that collects, processes, and consolidates data from various sources.

4. Data Registries: Entities responsible for storing, maintaining, and securely sharing a Resident's Key Personal Data according to the Resident's preferences as conveyed to the Data Registry by the Data Registrar.

5. Fiduciary Duties: Obligations of data controllers and processors to act in the best interest of a Resident, ensuring ethical and responsible data handling. These duties include the duty of care, loyalty, good faith, confidentiality, prudence, and disclosure.

6. Freedom of Association: The right of Residents to group together or form or join associations and appoint Skilled Advisors and Representatives to collectively negotiate data processing terms on their behalf.

7. Key Personal Data: Information relating to an identified or identifiable Resident that is normally required for entering into a contract, including Data Aggregator terms and conditions, or satisfying governmental or major information system or identity requirements. Key Personal Data includes:
   (1)
   - Full name, maiden name, mother's maiden name, or alias;
   - Personal identification numbers: social security number (SSN), passport number, driver's licence number, taxpayer identification number, patient identification number, financial account number, or credit card number;
   - Personal address information: street address or email address;
   - Geolocation;
   - Personal telephone numbers;
   - Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting;
   - Biometric data: retina scans, voice signatures, or facial geometry;
   - Information identifying personally owned property: VIN or title number;
   - Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person.

(2) The Commission may update this list of Key Personal Data through delegated acts under specific conditions. Before adopting a delegated act, the Commission must consult experts designated by Member States. Once adopted, the act is notified to the European Parliament and the Council and will enter into force if no objection is raised within two months.

8. Resident: A real person resident of the European Union.

9. Skilled Advisor and Representative: A professional or entity authorized to act on behalf of a Resident to advise the Resident on the operation of the digital data ecosystem, including the use of Key Personal Data, and negotiate with Data Aggregators on behalf of the Resident the processing terms for the Resident's Key Personal Data and related data. They ensure the interests of the Resident are protected and advise the Resident on what access and processing preferences to set for each Data Aggregator.

10. Third-Party Authenticators: Trusted entities that verify the accuracy and authenticity of Key Personal Data.

Title II: Scope

Section 3: Material Scope

1. Personal data and, particularly, Key Personal Data.
2. Skilled Advisors and Representatives.
3. Data Aggregators, including gatekeepers and providers of artificial intelligence systems, especially those categorised as high-risk.
4. Data Registries and Third-Party Authenticators.

Section 4: Personal Scope

The IDEA applies to:

1. Residents of the European Union.
2. Data Aggregators operating in the EU, regardless of where the business or organisation is established.
3. Skilled Advisors and Representatives, Data Registries, and Third Party Authenticators.

Section 5: Territorial Scope

The IDEA applies to:

1. **Processing Activities within the EU:** All data processing activities conducted within the territory of the European Union.
2. **Entities Outside the EU:** Businesses and organisations established outside the EU that offer goods or services to, or monitor the behaviour of, EU Residents.
3. **Personal Data Transfers to Third Countries:** Cross-border data transfers, ensuring that adequate data protection measures are maintained.

Title III: Provisions

Section 6: Data Protection and Rights

1. **Data Collation:**
    - Authenticating and hosting of Key Personal Data including establishing an EU wide mechanism for establishing and recognising digital certification utilised by Third-Party Authenticators, consistent with eIDA regulations.
    - Prohibiting processing of Key Personal Data without verification from trusted Third-Party Authenticators.
    - Obligation on Resident to ensure Key Personal Data is accurate and authenticated and regularly updated and stored with Data Registry.

2. **Access, Consent and Data Representation:**
    - Obligation for all Data Aggregators to source Key Personal Data only from the Resident-controlled record and only under the terms the Resident has set. The record and terms to be accessed through the Resident's Data Registry.
    - No Data Aggregator will hold Key Personal Data on an individual without that person's knowledge and consent unless as prescribed by law and for clear exceptions, such as public security, law enforcement, and national security.
    - Establishing the advisory role to Residents from Skilled Advisor and Representative, including assisting Residents to collate and update authenticated Key Personal Data.
    - Right to negotiate Residents' terms and conditions of use through Skilled Advisor and Representative.
    - Mechanism for the placing of consumer preferences and negotiated terms in Machine Readable Code.
    - Consent to be obtained through Machine Readable Consent.
    - Terms of access and processing expressed in Machine Readable Consent are presumed to be in the best interest of the Resident.
    - Mechanism for the updating change of Key Personal Data and/or Resident preferences and negotiated terms to Data Aggregators via Machine Readable Code.
    - Encourage Data Aggregators to adopt operational rules that manage individual consent variations, respecting diverse Resident preferences.
    - Ensure non-Key Personal Data is processed in the best interest of the Resident.
    - Establish fiduciary duties for Data Aggregators to ensure their processing of Residents personal data actions upholds Residents fundamental rights and interests.
    - Establish an objective test, grounded in human rights law, to ensure that interpreting the "best interest of the data subject/Resident" is not open to differing interpretations.
    - Add an audit requirement to existing corporate and public entity audit regimes to ensure that such data is controlled and/or processed within the defined duty of care.

3. **Obligation to negotiate in good faith:**
    - Where an accredited advisor/representative provider has indicated an intention to bargain on behalf of its consumer members/clients for access to their Key Personal Data, a responsible digital service provider and the accredited advisor/representative provider must negotiate in good faith. Breaches of this requirement should be subject to a significant civil penalty.
    - Advisor/representatives organisations shall be able to form groups to collectively bargain with the digital service providers.
    - Smaller digital service providers shall also be able to form groups to negotiate with advisor/representatives.
    - Negotiation can proceed for four months and then proceed to meditation and then binding "final offer" arbitration.

4. **Compliance:**
    - Data Aggregators to prove to auditors that they have sourced Key Personal Data only from the authenticated records held by the Resident's Data Registry.
    - Establish a system to prove to the Data Registry to digitally watermark or fingerprint the record for each specific agreement or transfer and to say from where the record has been sourced.
    - Obligation on Data Aggregators which receive or are offered Key Personal Data from another source not to use it and to report the source to authorities (similar to the regime concerning receiving stolen property).
    - Auditors to check if such types of data held by a business or public entity is in accordance with the IDEA.

5. **Governance and Transparency:**
    - Provide clear operational guidelines for Skilled Advisors and Representatives, Third-Party Authenticators, and Data Registries.
    - [Recognize and regulate data commons as key components of the data-sharing ecosystem. (Isn't this laid out in the DGA?)]
    - Establish a regime for accreditation of each Advisor/Representatives and Data Registries.
    - Establish a fiduciary governance regime for each of Advisor/Representatives and Data Registries, including setting rules on disclosure, transparency, fiduciary standards, conflicts of interest and fair dealing with clients.
    - Commission either public regulators, or a professional association of Advisors/Representatives, to require continuing professional education to agents, as well as materials for consumer education awareness.
    - Commission public regulators or the professional association will coordinate a complaints and complaint resolutions mechanism, including civil penalties.

Section 7: **Market Fairness and Competition**

1. **Market Initiation Incentives:**

- Implement incentives to encourage participation in both parts of the market and ensure effective representation.
- Establish financial support to help meet start-up costs for entities seeking to be either Advisor/Representatives and specialist Data Registries.
- Fund access to specialised training and information resources to support nascent Advisor/Representatives achieve the necessary skills and knowledge to perform their duties effectively.
- Consider an initial small subsidy per Resident to fund transition of Europeans to the new role of empowered data consumer.

2. Competitive Markets

- Advisor/Representatives which will operate in competition to each other to attract and serve Residents.
- Data Registries will operate in competition to each other to attract Advisors/Representatives as channels to Residents. The end customer of the Data Registries will be Residents, but payment from Residents will be coordinated through Advisors/Representatives.

3 Competition Safeguards:

- Prohibit Advisors/Representatives and specialist Data Registries from using a Resident's Key Personal Data for any other purpose than as a fiduciary agent of the Resident for the purposes of this Act.
- Prohibit Advisors/Representatives and specialist Data Registries from using the Residents' Key Personal Data for any purpose in competition with or detriment to other Data Aggregators.
- [Should we have a carve out for online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms to prohibit them from being Advisors/Representatives and specialist Data Registries similar to the Digital Services Act?]

Section 8: Artificial Intelligence Regulation

- The provisions of this Act apply to the application of Artificial Intelligence systems and developers.
- The Act will apply to output of Key Personal Data from such systems and also to the collection and processing of Key Personal Data in machine learning datasets.
- The Commission is to coordinate with Artificial Intelligence developers a code for the transition of digitally watermarked or fingerprinted Key Personal Data for each specific agreement or transfer into machine learning data processing.

Conclusion

The IDEA integrates and builds upon existing European digital legislation to create a comprehensive framework that empowers consumers, protects data, ensures market fairness, and fosters innovation. This Act aims to contribute to Europe's dynamic and competitive digital economy.

The Global Initiative for Digital Empowerment (GIDE) is a non-partisan, international non-profit organization founded to give people a voice and control over how the data about them is collected, stored, and used. We advocate raising the values that prioritize the well-being and rights of people, both individuals and as representatives of communities and democracies, as the main drivers of the decision-making processes in the digital economy.