European Strategy for Data

A Meeco Review of the European Strategy for Data Communication from the European Commission on February 19th, 2020

Forward

January 2020 marked the beginning of another decade deeper into the Information Age and further from the Industrial Revolution. New market forces were competing for dominance in our borderless digital society, alongside increasing tensions over physical borders and the environment.

And then, the impossible happened. A domino effect starting in China and circling the globe, shutting down borders and economies in its wake. Clearing the skies of pollution and wiping out stock market gains.

Three clear strategies have been amplified in the physical world in a bid to manage the pandemic curve: the power of the State, the rights of the Citizen and the naked forces of the Market. Each with its unique approach to health services, population management and contact tracing.

An obvious advantage of the connected world is the vast amount of data to help model, plan and sense make through the chaos. The options to increase surveillance, foster a democratic society or allow market forces to dominate will all depend on the data strategy adopted by each jurisdiction.

Coincidently or with perfect timing, The European Union published "A European Strategy for Data" on February 19th, 2020 outlining its vision for a connected single digital market where the benefits of the digital economy could enhance the lives of its citizens, residents and trade partners.

However, we now find ourselves at a very real crossroad. This is not a drill. A post-pandemic world will be a new type of normal. Amidst the tragic loss of lives there have been breakthroughs in science, new ways of working, new digital tools embraced and a chance for our planet to breath.

Personal data linked to identity, fuelled by AI sits at the centre of three competing digital strategies; the tensions between the rights of the EU citizen, the power of the State in China and the commercial market forces of the USA present new ethical, technical and societal challenges.

We are at the beginning of a new design and architectural phase where just because technology can, doesn't mean it should. Where we go from here depends on how the European Union successfully strikes a balance between the competing data strategies.

At Meeco we believe that enabling citizens, students, patients, passengers and consumers to more equitably join the value chains fuelled by data will ultimately lead to greater trust and personalisation, resulting in a more prosperous society. However, this will require new commercial models, enforceable regulation and the digital tools to transform our connected society.

It is our hope that the European Union's Data Strategy is a force in contributing to this transformation.

Katryna Dow

CEO & Founder, Meeco

Contents

For the reader

This document has been written to give the reader a snapshot of the new European Union (EU) Strategy for Data published as an EU communication on February 19th, 2020. In this document the authors express their opinion by way of commentary on the topic of personal data management and analysis of the strategy that the EU will adopt.

Meeco's review points the reader to some of the most important elements of the EU's position on various data issues, as well as the key elements of its strategy. We have taken care to include all direct excerpts between quotation marks and to reference them clearly back to the original communication document, by way of footnotes.

We have also taken the opportunity by way of Case Studies, to highlight leading examples of personal data management, and how their approach to personal data management fits in with the European strategy for data. The Case Studies comprise five key perspectives: Business, Legal, Technology, Barriers and Catalysts. Through this lens we have addressed the commercial opportunities enabled through new technologies designed to meet regulatory compliance. We also explore the barriers that exist to build scale, together with the strategies that can accelerate adoption.

Part I – Executive Summary

Europe fully intends to be a major actor in the new Data Economy, holding its own against other world powers.

This is the headline announcement in the EU's latest communication on the European Strategy for Data. This paper published in February 2020 lays out a coherent vision for common data spaces in Europe and a single data market in the European Union. It recognises that Europe is not where it should be today and that there remain considerable risks and barriers to achieving its vision. The European Commission further comments that there is much work to be done and many investments to be made, often as a catch-up on other more data-agile economies and societies.

But the tone of the document is upbeat and purposeful, it lays out clearly and in a reasonable manner what Europe intends to achieve over the next 10 years. It outlines specifically what the European authorities will do to create the best environment for Europe to carry its own weight in the developing Data Economy.

For those in the private and public sectors who may not be as well-advanced in thinking about the future of data, this European Strategy for Data should serve as a wake-up call. In this very fast evolving environment, there remains a huge amount to be done, and rapidly, if the EU is to compete with the two other data superpowers; China and the United States.

The EU is committing to build a supportive environment in Europe from a regulatory and legal perspective. It will participate alongside Member States and private enterprise to build next generation technology and infrastructure solutions such as Cloud at the Edge Computing, Quantum Computing. The other relevant area of important development is of course Blockchain.

It will continue to push for greater data interoperability and re-use of data amongst actors in the same sector and across different sectors as well, both B2B and B2G. It will continue to place the individual citizen at the centre of the data equation and even reinforce the individual data rights for privacy and consent that are already enshrined in the General Data Protection Regulation (GDPR). It calls for the data economy to be human-centric.

Another strong sign of action on the EU's behalf is the plan to establish Common European Data Spaces in strategic areas and domains of public interest, including:

- Industrial (manufacturing)
- Green Deal
- Mobility
- Health
- Financial
- Energy
- Agriculture
- Public Administration
- Skills

The EU will develop these data spaces and their use in the appropriate regulatory and legal framework to ensure that data rights are fully respected. It will also ensure that the right standards for data sharing and data interoperability are present, as well as the technical tools and infrastructures necessary to use and exchange data, as well as appropriate governance mechanisms.

These measures should render the collection, management and use of this vast amount of common European data as efficient as possible.

They will be further complemented by policies that stimulate the use of data and demand for services enriched with data. It is expected that the availability of these pan-EU data pools will significantly enhance the use of data that can positively and systemically impact the entire ecosystem, including Europe's citizens.

One can well imagine the significantly improved position Europe would find itself in today in the face of the Coronavirus pandemic, if instead of dealing piecemeal with top down health data, it could rely on a range of verified data sources, including personal health data directly from citizens and residents, with privacy and data protection as pre-requisites. Collectively, the power of the public sector, industry and people could better help us to rise to challenges such as contact tracing, identifying antibodies and the approval of vaccines faster and more efficiently.

It is the EU's intention to put us all - individuals, enterprises, organisations and public authorities - in a position to gain as much as possible from the economic and societal benefits that vastly enhanced use of data can bring.

How those benefits are achieved is, however, where one sees the least progress, the least effort and the least investment from the stakeholders that stand to benefit from them. Here we are talking about the concrete means of collecting and storing personal and non-personal data, how the data is organised and how it is made available upon demand. We are also looking for societal value from new products and services derived from better ways of using data.

The most blatant example of this is indeed true data interoperability and data reusability, as opposed to straight forward data portability in the sense of service provider switching.

Just consider the cost involved, for the individual to manually input personal data every time it is required for onboarding or periodic review, such as is the case for example in Know Your Customer (KYC) for financial institutions. Consider the cost for banks to collect, store and manage this same data, when potentially it could easily be obtained with the individual's consent from a trusted 3rd party who already holds the same data, can verify provenance and authenticity and is prepared to issue a Verifiable Credential

If Europeans are enabled to leverage the information that they have provided to trusted 3rd parties (once), together with the technological means to make it reusable, then significant access and efficiencies could be gained. Add to this the opportunities for trusted 3rd parties to form transparent marketplaces of Verified Credentials (government, financial institutions, telecommunications) and a range of new services and commercial opportunities emerge.

These are the sort of day-to-day use cases that need to be rethought and remedied and that will create immediate and tangible value for all stakeholders. This is what the private and public sectors need to be working on, with a greater sense of purpose.

Beyond the obvious use cases, Europeans also need to engage in blue sky thinking and develop the future business models that will succeed and that leverage the availability of accurate and timely personal data. This is where the greatest potential for value creation lies, but how many organisations have the courage and the ability to think beyond their well-tried and tested, yet declining business models?

The reality is that most likely, only those enterprises whose business is data have thought through the regulatory risks and future potential for enhanced value creation. And yet in today's digital economy, how many organisations can say that the data that they need to manage every day on behalf of individual customers does not increasingly drive their business and their revenues?

Image Source: Meeco Human Centric approach to data management and consent.

The key to the Data Economy is personalisation of data and this requires trust on the part of individuals vis-à-vis the enterprises and organisations that collect and use their data.

Part of this ecosystem of trust is understanding and controlling what happens to our data when used by others. The other part is exercising our right to consent to sharing data, which includes our inalienable right to revoke our consent as well.

This is no longer about the obsolete notion of an enterprise owning a customer, nor is it about individuals claiming complete ownership over data that has been mutually created. Rather, it is about individuals exercising their data rights and being able to control the impact that the use of their data has on them.

At the end of the day, the best way for an individual to control this impact is by choosing whom to buy products and services from, as well as when and how to buy them. If an individual ignores the other actors who use his or her data without consent, then ultimately the data becomes worthless to those operators. In the same light, this also places the emphasis on the quality of data used by enterprises and organisations. Clearly the best source for the personalisation of services is the individual, as they bring two valuable additions to accurate and timely data: context and intent.

So, within this supportive environment that the EU is prepared to build for us, we need to take on the responsibility to create more value out of data management. This in turn requires safe and secure technology, cost efficiency and flexibility around organising data. It also requires products and services that create more value than today and that afford the individual the opportunity for a greater share in this value creation.

It requires that European citizens, enterprises and organisations take up the banner and deliver on the vision of the EU, but also for example on the far-reaching vision of pioneers such as KuppingerCole and its early work on the topic of life management platforms.[1]

In short, it requires investment in developing new data tools and services that bridge the enterprise and the organisation of today, with genuine participation in the value chain from citizens, patients, students, consumers and employees. This is our focus at Meeco, developing the means for everyone in the data-chain to achieve equity and value through transparent participation.

Europe fully intends to be a major actor in the new Data Economy, holding its own against other world powers. In Part II of this review, we take a closer look at what the communication “A European Strategy for Data” tells us about how the EU plans to achieve this.

[1] KuppingerCole (Germany) 2012 Advisory Note on “Life Management Platforms: Control and Privacy for Personal Data”.

Part II – A closer look at The European Strategy for Data

For the easy reference of the reader, the structure of this part of the document follows the same order of topics that are presented in the source EU Strategy for Data communication document. All direct quotes from the EU Strategy document are highlighted in blue and referenced via footnotes.

1. Introduction

The introduction kicks off with a very general statement, but one that hits the nail on the head:

"Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans. Data is at the centre of this transformation and more is to come."[2]

The implication is that data is central to all economic and societal transformation and development for the foreseeable future. As such, it should be a focal point of strategic importance for all stakeholders, whether individuals, enterprises or governments.

[2] European Strategy for Data, 2020 – page 1

“Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans. Data is at the centre of this transformation and more is to come.”

– European Strategy for Data, 2020 – page 1

A second fundamental point is then raised, with regards to the paramount importance of the respect for data rights of individuals in Europe. Only if those rights are respected, will the individuals trust new products and services born of this data revolution.

The EU further states that Europe's citizens should be empowered to make better decisions based on this data, both personal and non-personal. On the back of this, the document lays out a far-reaching ambition: to become a role model for a data-empowered society.

The principal conditions of success that need to be met for this to happen are a robust legal framework for data, in all its aspects, and a market framework that supports organisations across all industrial segments. The benefits that will accrue to Europe's citizens are both economic and societal, including health and well-being, the environment, transparent government and improved public services.

"In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules."[3]

The key here is that there is an incredible potential for data-enabled innovation, provided individuals are prepared to supply the resource – personal data – that will drive more personalisation of products and services. In the current personal data environment, trust on the part of data subjects is in very short supply.

This is an issue that needs to resolved first, before individuals can be convinced to share their personal data with enterprises, organisations and 3rd parties. The following case study shows how Meeco's API-of-Me platform was designed to be human-centric and developed to support a trusted eco-system of actors that can fulfil data driven services.

Value is derived through the combination of data "from me" together with data "about me". This may comprise personal, social, public, enterprise and derived data. This approach enables individuals to fully participate in the value chain. However, it equally requires strong, clear value propositions that are mutual and transparent in order to win and maintain trust.

[3] European Strategy for Data, 2020 – page 1

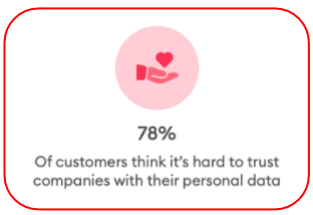
Case Study 1.

Building Trust and the API-of-Me

For decades enterprise and governments have benefited from the technological integrations between their infrastructure and their B2B partners. We accept this as common place for supply chain management, access and authorisation of services and settlements. This is largely achieved through industry standard APIs (Application Programming Interfaces).

APIs enable value chains across industry sectors, such as financial services for faster credit assessment and provision, as well as across adjacent industries such as healthcare and insurance.

Up until now the power to capture, analyse and profit from personal data has resided with business, government and social networks. What if you and I had the same power? **Enter the API-of-Me**. The same tried, tested and trusted technology that can now enable individuals to directly exchange personal data with the people and organisations they trust. Privately, securely and always with explicit consent.



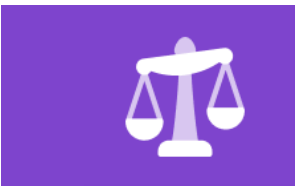
As individuals gain the legal rights to manage and control their data, businesses need to re-think how they collect, store and exchange customer information. Data breaches, identity theft and data malpractice have taken trust to an all-time low. As a result, people are now calling for a new social contract with respect to how their data can be used. Meeco's API-of-Me platform is specifically designed to provide individuals and enterprise the necessary tools to accelerate a more integrated and transparent data economy.

From a **business perspective**, the adoption of human-centric data solutions, such as Meeco's API-of-Me Platform open new digital economy opportunities, including new business models and improved operational efficiencies.

Specifically, the ability to develop more integrated digital experiences, reduce on-boarding friction and offer more personalised customer experiences. Integrating consent and personal data access can reduce form filling and decrease time to decision. Implementing Verified Claims reduces data collection and storage, increases data accuracy, provenance and trust.

The increase of operational efficiencies provides a basis for investing in new digital tools for customers that use industry standard data schemas, protocols (APIs) and market enablers, such as PSD2 (Payment Services Directive Two) and Open Banking.

These changes pave the way towards new commercial offers and business models that focus on service outcomes and personalisation. Results may include greater value derived from the transparent use of personal data and more mutual value across all stakeholders.



From a **legal perspective**, individuals' data protection rights are already established through the General Data Protection Regulation (GDPR). However, cost and compliance implementation has been the focus since its introduction in May 2018. Activity has focussed on the avoidance of fines rather than the acceleration of data innovation.

Design methods such as "Privacy by Design" consider both the rights of the individual and compliance requirements, from ideation to implementation of solutions. This approach dramatically reduces the burden of compliance as an external monitor, by bringing audit and revocation (Right to Erasure) directly into the digital service.

Furthermore, capabilities such as Meeco's "Progressive Disclosure" minimise data collection by limiting the amount of data to that which forms a lawful basis as set out in Article 6 of the GDPR. Progressive disclosure supports the increase in data shared commensurate with the service provision value proposition.

From a **technology perspective**, human-centric tools are a step change for the digital economy. Personal data platforms like Meeco provide both back-end (services) and front-end (applications) that can easily be integrated with existing enterprise technology.

By way of example, Meeco provides a "secure data enclave" such as a vault or wallet which can be deployed as either a cloud or on-premise solution in the European Union. However, neither Meeco nor the enterprise have direct access to the personal data, as it is protected by end-to-end encryption.

Data is stored on a "per attribute" basis which enables business use cases, such as progressive disclosure. Each attribute is managed through a Consent Engine which allows individuals to decide on the Permissions including duration (minutes, hours, date), together with whether the data can be on-shared or used for loyalty tracking or monetisation. Data can be added to the secure data enclave in three ways;

1. API Push - data shared from the enterprise
2. API Pull - data from third party services such as financial, social, IoT and health
3. Self-Asserted – converting form filling to re-usable data.

The Personal Event Ledger function tracks access to devices, authorised connections and sharing of data, thus establishing an immutable audit trail that is unique to the individual user.

The **barriers** to the adoption of human-centric technology include:

- Market awareness, lack of understanding and exploration of new business models
- Entrenched data practices and business models, despite fines and flat growth
- Lack of investment in digital transformation and technology
- Compliance squeezes out innovation as a response to data regulation
- Competition from American and Chinese data platforms

Catalysts for EU adoption and scaling of human-centric technology include:

1. Clear Data Strategy for European Union
2. Regulatory incentives for adoption of privacy and human-centric solutions
3. Investment in European alternatives to existing social and surveillance economy platforms
4. Investment in European data infrastructure.

Specific examples of these new human-centric products and services are featured in each of the following Case Studies.

“Data is the lifeblood of economic development: it is the basis for many new products and services, driving productivity and resource efficiency gains across all sectors of the economy, allowing for more personalised products and services and enabling better policy making and upgrading government services.”

– European Strategy for Data, 2020 – page 2

2. What is at stake?

One of the fundamental changes that is taking place is the shift in data production from data centres and centralised computing centres, to smart connected objects and in-computing facilities closer to the user (edge computing). This implies that we will all produce much more data than in the past.

This is already evident over the past few years with the emergence of the Internet of Things (IoT), with an explosion of data being produced by us around the clock. The EU identifies this as an opportunity, and perhaps also a necessity, to develop new tools that will give individuals more control over the data that they produce.

The opportunities are exponential, given that data fuels innovation in new products and services, boosts revenue opportunities and is fundamental to efficiency gains. It also allows for performance by the Executive branch in formulating policy and improving services to Europe's citizens. Many of the modern challenges that we face in Europe's societies today can be better solved if we are prepared to use shared data in a more effective manner. The EU makes specific reference to:

"Moreover, making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges, contributing to healthier, more prosperous and more sustainable societies."[4]

But the key to this happening is to achieve a better distribution of data across all actors and sectors in Europe and its single market, instead of the concentration of data in the hands of a few big tech firms as is the case today.

This can be achieved through technological change in areas in which Europe is strong. This could somewhat reshuffle the cards, in a manner that could change those actors that currently dominate the Data Economy in Europe. In order not to miss out on these opportunities, the EU needs to act promptly. It recognises this very openly, by stating the fundamental importance of data across many facets of the economy and society:

"Data is the lifeblood of economic development: it is the basis for many new products and services, driving productivity and resource efficiency gains across all sectors of the economy, allowing for more personalised products and services and enabling better policy making and upgrading government services. It is an essential resource for start-ups and small and medium-sized enterprises (SMEs) in developing products and services. The availability of data is essential for training artificial intelligence systems, with products and services rapidly moving from pattern recognition and insight generation to more sophisticated forecasting techniques and, thus, better decisions".[5]

Few services require more personalisation than financial advisory. Financial advice requires very detailed personal data and information about individual clients - their assets, liabilities, affordability and cash flow. Of equal importance is understanding their goals, aspirations and lifestyle.

In the next case study, we explore the benefits of access to real-time personal financial and lifestyle data, including the benefits of such solutions amidst the impact of COVID-19.

[4] European Strategy for Data, 2020 – page 3
[5] European Strategy for Data, 2020 – page 2

Case Study 2.

Financial Advice Nexia Wealth Connect

Nexia International is a leading worldwide network of independent accounting and consulting firms with 671 offices in over 122 countries. According to the latest International Accounting Bulletin (IAB) World Survey, the network has risen to become the 9th largest global accounting network.

The Nexia Australia and New Zealand network services clients from small to medium enterprises, large private company groups, not-for-profits, subsidiaries of international companies, publicly listed companies and high net worth individuals. The breadth of services offered highlights the importance of understanding the range of "roles" individuals assume with respect to their financial obligations, as they move between the personal and professional implications of financial decisions.

In order to provide personalised advice, wealth advisers and clients alike require access to their personal financial data and information in a wholistic way. Apart from reducing the potential for errors, it both optimises the advisory process and reduces the cost of compliance.

In 2017, Nexia Sydney implemented Meeco's Secure Value Exchange (SVX) personal data management products within their Digital Client platform Nexia Wealth Connect. SVX is designed for wealth advisory and provides a secure collaboration portal for clients and their trusted advisors (accounting, legal, tax, insurance) to have real-time and secure shared access to financial data and documents.

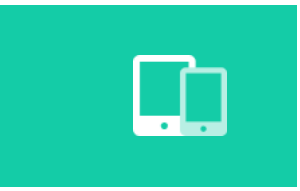
From a **business perspective**, the Wealth Connect Platform enables advisors and clients to have real-time access in order to digitally collaborate. For Nexia Sydney, this proved to be invaluable in moving to a virtual office within days of the COVID-19 crisis. Such initiatives underscored the resilience of their business continuity whilst continuing to provide remote personalised services to their clients.

Personal financial management requires a human-centric approach. The burdens of compliance, tax regulation and personal circumstance must all be taken into account and balanced in order to offer advice. The effort to access and review the relevant data and information has a bearing on the cost and timeliness of the advice. Enabling clients to be transaction ready and significantly decreasing the time-to-value are some of the major benefits of secure financial data collaboration. Reducing the risk of fraud and identity theft through secure management and exchange of encrypted data is another business differentiator in building trust and providing clients with service transparency.

From a **legal perspective**, compliance is the key consideration in the provision of any financial advice. Audit and referenceable documentation are equally critical to the adviser and client. Recommendations must clearly demonstrate the assumptions and inputs considered.

Initiatives such as the Personal Services Directive 2 (PSD2) and Open Banking are aimed at providing greater transparency, and access to personal financial data and to better enable

individuals to compare products and services. However, whilst there is a move to automate many of these options through the rise of FinTech solutions, the underlying requirements to comply with the legal, tax and jurisdictional requirements remain in force. Collaborative platforms such as SVX provide for the necessary balance between minimising data collection and maximises data driven decisions.



From a **technology perspective** the platform provides an integrated and consolidated view of a client's real-time financial position.

Supported by automated bank feeds, superannuation (pension), accounting, property, share portfolio, and even loyalty data. SVX provides three important dashboards: Adviser, Personal and Business.

1. The Adviser Dashboard helps advisers understand the live and real-time portfolio of clients and manage their commitments in order to be pro-active in delivering timely services.

2. The Personal Dashboard provides individuals with a full view of their real-time financial position.

3. The Business Dashboard provides clients with a full view of their business' financial position, risks, opportunities and provides customized alerts to individual by role as a group.

The platform integrates 3rd party enterprise applications and data feeds through industry standard APIs, along with providing functionality for document verification, digital signature and video conferencing.

There are a number of **barriers** to the widespread adoption of personal financial platforms such as SVX including:

- On-boarding - often, individuals only become motivated to put in the effort when triggered by a life event, such as inheritance, illness, marriage, retrenchment, promotion or tax audit.

- Time-to-Value – the effort required to bring all information together can be overwhelming. For this reason, timely decisions are delayed and more importantly opportunities are missed.

- Digital literacy – the rise of FinTech is helping to educate a younger European population, however given increased longevity and the size of assets held by Baby Boomers, digital adoption needs to be intergenerational.

Catalysts for EU adoption and scaling of more access to financial advice and better financial decisions include:

- Data access - enabling Europeans to have timely access to machine readable financial data from trusted sources (bank, financial institutions and government)

- Streamlining automation – providing secure access to private, public, tax and financial digital services

- Digital regulation – ensuring Europeans have the necessary protections in place to access, exchange and secure their personal and financial data.

- Digital Security – given the rise in fraud and identity theft, ensure data management, encryption and identity verification provide adequate consumer protection.

“The Commission’s vision stems from European values and fundamental rights and the conviction that the human being is and should remain at the centre. The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions. It is all the more compelling to seize the opportunity presented by data for social and economic good, as data – unlike most economic resources – can be replicated at close to zero cost and its use by one person or organisation does not prevent the simultaneous use by another person or organisation. That potential should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage.”

– European Strategy for Data, 2020 – page 4

3. The vision

Data is a vital resource that can be used simultaneously by several parties to create value, with a cost of replication and reuse close to zero. This implies that it can significantly contribute to value creation and growth if used in a productive manner. This represents an opportunity that could benefit all stakeholders in Europe. The EU cautions however that taking advantage of this opportunity can only be achieved with better access to data and its responsible usage. Over the past two decades we have witnessed wide-spread data abuse, and the implementation of surveillance capitalism which increases asymmetry in digital participation for Europeans.

Europe will ensure that its share of the data economy by 2030 is at least of the same order as its economic weight. In order to further support the usefulness of data, the EU states that it will look to create a single European data space in the form of a single market for data in Europe. This will be a space where EU law will prevail to its fullest extent and where all data-driven products and services are fully compliant with Europe's data regulations. These common data spaces should in turn foster an ecosystem including all stakeholders, that will drive the creation of new products and services based on improved accessibility and use of data.

The correct functioning of the European data space requires Europe to invest in next generation technologies and new infrastructures and to boost digital competences such as data literacy, where it lags more data-agile actors elsewhere in the world. The results of this investment would be the existence of European data pools, feeding big data analytics and data-enabled ecosystems.

"The Commission's vision stems from European values and fundamental rights and the conviction that the human being is and should remain at the centre. The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions. It is all the more compelling to seize the opportunity presented by data for social and economic good, as data – unlike most economic resources – can be replicated at close to zero cost and its use by one person or organisation does not prevent the simultaneous use by another person or organisation. That potential should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage."[6]

Better access to personal data requires actors that are prepared to make the necessary investments, in order to provide individuals with the means of storing and sharing their personal data, information and documents. This must be done in a secure and private manner, fully compliant with GDPR.

These very same actors then become data operators in the wider data-enabled European economy. As for more responsible usage of personal data, this goes both ways. On the one hand, these data operators must always respect the privacy and data rights of the individual and only use his or her data after obtaining explicit consent. On the other hand, it is important that these data operators also impose minimum standards and rules as to what type of data, information or documents can be stored in personal data vaults or safes and what can be shared across any specific platform. Sharing inappropriate material would ultimately be to the detriment of all stakeholders, which is why strong user verification, such as some form of Know Your Customer (KYC) is best practice.

The following Case Study features a human-centric implementation from KBC, a leading Belgian bank and insurer. The KBC digital safe, serves to illustrate how trusted financial services, amongst others, can help their customers create personal value and utility from their personal data whilst guaranteeing privacy and adhering to EU data regulation.

[6] European Strategy for Data, 2020 – page 4

Case Study 3.
KBC Bank
The Digital Safe

KBC Bank, is one of the leading retail banks in Belgium and was voted Best Digital Bank in the 2019 Spaargids.be bank Awards. It serves 3.5 million customers. With a focus on building a trusted eco-system of third-party services KBC embarked on the strategic goal to deliver a Privacy-by-Design digital safe for its mobile banking customers.

"The distinction between customers and non-customers is becoming increasingly blurred. Consumers are looking for the fastest and easiest way to meet a particular need and they only want to see information and services that are relevant and tailored to the way they organise their lives. They expect to have access to a much wider and more attractive package of services, which they want to be able to activate quickly and easily from a single central app, without fuss or having to download 10 different apps. KBC will focus on this heavily in the years ahead. We're going to develop KBC Mobile into an open platform that is readily accessible to every consumer and adds genuine financial value."
– Karin Van Hoecke, General Manager Digital Transformation & Data

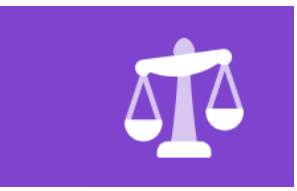
KBC is leading the way in the provision of value-added services for their mobile customers. Taking the eco-system approach, KBC provides customers with direct access to a range of vital every-day services including, public transport (STIB, SNCB, De Lijn), bike rentals (Blue-bike, Mobit, Velo) Olympus Mobility, parking (Q-Park, 4411), Brussels Airport (Fast Lane & Lounge access), service vouchers (Sodexo), vouchers (Monizze) payments (Payconiq, PayPal), government documents (eBox), registered email (IPEX) and the KBC Digital Safe. KBC will add more third-party services through 2020.

The unique feature of KBC's Digital Safe is an extension of a physical bank safe: key management and access. Whilst the Digital Safe is accessible through mobile banking, the security architecture and customer access is designed so that only the customer has complete control of the data and documents within the Digital Safe. Not only is the solution Privacy-by-Design, it is also Security-by-Design.

From a **business perspective**, this strategy is very customer centric. It demonstrates the value of the bank for digital services beyond banking. It also provides for multiple touch points daily.

Leveraging brand trust and bank security helps to overcome the concerns associated with the collection, access and control of sensitive personal data. Just in the same way, physical bank vaults were used to hold important assets and documents.

The Separation of Concerns architecture is a great foundation to enabling customers to have privacy and control, whilst developing a range of value-added services. In the context of PSD2 and Open Banking, KBC is well positioned to extend the Digital Safe to a range of use cases which would enable the customer to participate directly by making their personal data and consent available real-time.



From a **legal perspective**, this is a great customer initiative that allows KBC to be a step ahead of privacy regulation. As individual data protection rights are embedded in GDPR, KBC has provided customers with the means to both protect their data and exercise their digital rights. The Digital Safe includes a data download service, option for data deletion (right of erasure) and the file format supports data portability.

Given the focus in the EU Data Strategy on the rights of EU citizens and the need for technologies, such as the Digital Safe, KBC is ahead of the data regulation curve and well positioned to extend services in line with the use-cases described to foster a single digital market.

From a **technology perspective**, there are four unique aspects to the implementation:

1. Provision of a secure data enclave, totally compliant with European data and privacy regulation, together with convenience of mobile access.

2. Leverage the bank's identity, authentication and authorisation services to access the Digital Safe, whilst not having direct access to the data.

3. Implementing Meeco's Zero Value Knowledge data model, which ensures all attributes are fully encrypted, however labels are available to support the implementation of use-cases such as attribute request and exchange.

4. Secure storage and sharing capabilities for personal data and documents.

The front-end application was custom developed for KBC, whilst all back-end services are powered by Meeco's API Platform. This enabled the bank to launch the first version within five months, including design, development, compliance, legal and go-live. This provides the foundation to extend services from a features perspective (technical), legal perspective (compliance) and business perspective (value-added services).

The **barriers** to enterprise solutions for personal data management include:

1. Many business managers do not yet fully appreciate the business opportunities that personal data management offers.

2. Implementing such solutions requires upfront investment, which requires clear business and technical roadmaps to ensure customers gain value along the way.

3. Viewing regulations such as GDPR as a compliance constraint versus innovation opportunity.

4. Customers increasingly have high expectations of digital services; they need to see benefits from using personal data beyond storage and sharing of personal data alone. This requires education and demonstrating to customers how they can benefit from personalised services that reduce friction.

The **catalysts** to support the wider adoption of customer-centric personal data:

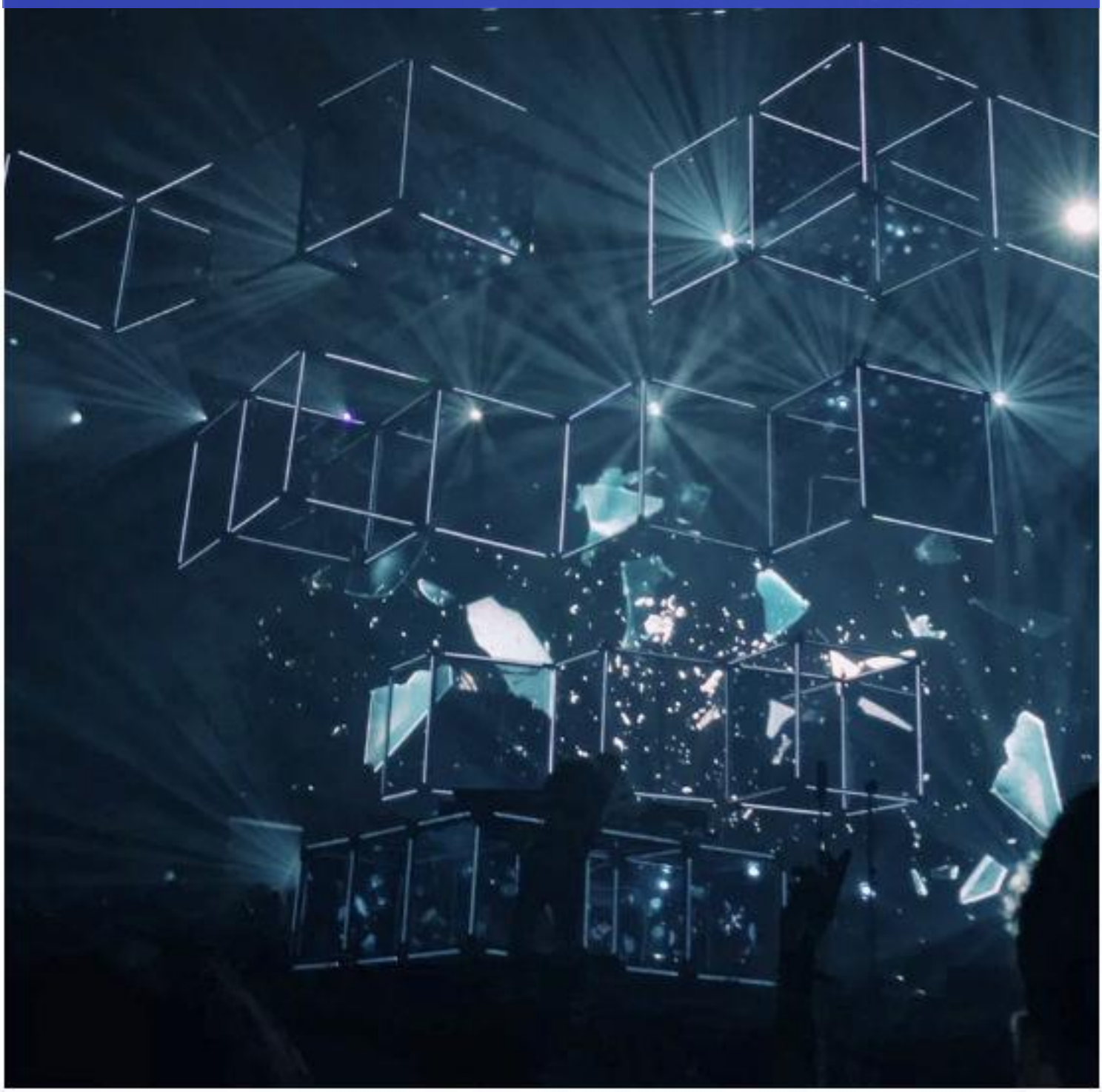
- Adoption of EU Data Strategy to further inform business and enterprise on where to focus customer and digital innovation.

- Regulatory and policy protections for European initiatives which protect and increase customer's digital rights.

- Tax and financial incentives for European enterprises that adopt human-centric technologies and contribute to the success of the EU Data Strategy.

“The high degree of market power resulting from the ‘data advantage’ can enable large players to set the rules on the platform and unilaterally impose conditions for access and use of data or, indeed, allow leveraging of such ‘power advantage’ when developing new services and expanding towards new markets.”

– European Strategy for Data, 2020 – page 8



4. The problems

Several issues are holding the EU back from realising its potential in the data economy. The main contextual element here is the emerging fragmentation between Member States who individually are more or less advanced in adapting national legal frameworks to the realities of the myriad issues involved in data management in Europe. The EU sees this as reinforcing the need for coordinated action amongst its Members.

The EU communication document enumerates 8 major current and potential impediments that need to be addressed if Europe is to fulfil its vision and ambitions for a data economy worthy of its position in the world. These are detailed below:

1. **Availability of data** must improve in order to boost the creation of value from its use and reuse. Innovative reuse of data, such as in artificial intelligence requires more data than is currently available.

2. **Imbalances in market power**, with a small number of large on-line platforms able to exploit the quasi-exclusive access they have to vast quantities of data and to drive significant competitive advantage through data usage. The ability of these large on-line platforms to derive deep insight based on the quality and variety of the data pools places them ahead of competition, particularly smaller enterprises, and represents an unfair advantage that is not conducive to the more widespread access and usage of data by all actors in the European economy.

3. **Data interoperability and quality** are key to allowing actors in specific industries and across different sectors to exploit data in a beneficial manner. This requires a more standardised approach to collecting, managing and using or re-using data. All actors need to be confident that the data that they obtain from different sources has the same meaning for all stakeholders and meets minimum standards of quality and compatibility. This can and should be encouraged through the rolling plan for ICT standardisation and a strengthened European Interoperability Framework.

4. **Data governance** needs further definition and application of organisational approaches and structures (both public and private) that enable data-driven innovation based on the existing legal framework.

5. **Data infrastructures and technologies** basically need to be developed much more towards cloud infrastructure and services, as there has been a low uptake of cloud services in Europe to date. This would also help reduce Europe's dependency on external providers of these services and in doing so would lessen the risk that European citizens become subject to the legal frameworks of other countries, which often differ from the European data standards.

6. **Empowering individuals to exercise their rights** under GDPR and ePrivacy legislation is essential. However, the tools and standards are lacking that would otherwise simplify and ease the exercise of their rights. In principle, says the EU, Article 20 of the GDPR should enable novel data flows and foster competition.

   In fact, its practical application is still somewhat limited by the fact that it was designed to favour switching of service providers rather than prioritising and supporting data reuse. This is partly what the Payment Services Directive has sought to remedy in its inclusion of provisions on data access and reuse. Here the EU goes on further to recognise the importance and potential for the right tools to bring real economic and societal advantages to European citizens. These tools include consent services, personal data management platforms to support personal data sharing, blockchain solutions and novel neutral data operators.

7. **Skills and data literacy** remain too low with big data and analytics at the top of the list of skills shortages. These are important issues that need to be addressed if Europe's citizens are to benefit fully from the data economy and society.

8. **Cyber security** will need to evolve in order to adapt to the shift in data processing and storage from data centres to computing closer to the user 'at the edge'. The EU tells us that preserving data security when data are being exchanged is essential in building trust in data sharing. Distributed ledger technology will help to establish the right environment for data security.

One fundamental change that will occur in the area of cybersecurity is the idea of key management. Just as children in the past have been taught the value of taking care of the physical keys to the house – the current generation will be schooled in the importance of taking care of their digital keys – which will determine access and consent together with an audit log.

Another fundamental issue that touches on several of the problems enumerated above is how individuals can use physical documents (in the context of a digital service) in a way that is cryptographically secure, privacy respecting, and machine verifiable.

These documents may include government-issued identity documents such as passports and driving licences or university diplomas, all of which may be required for an on-boarding process, in order to complete an e-commerce transaction or simply to access, authorise or authenticate a given service.

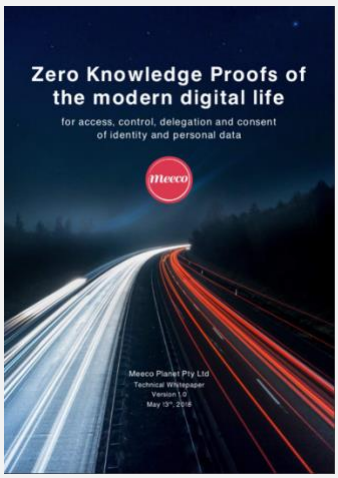
What is now required in order to enable digital trust in these previously physical artefacts, is provenance traceability, verification of authenticity, and governance of how data is used, tracked and logged.

"New decentralised digital technologies such as blockchain offer a further possibility for both individuals and companies to manage data flows and usage, based on individual free choice and self-determination. Such technologies will make dynamic data portability in real time possible for individuals and companies, along with various compensation models." [7]

A good example of blockchain and distributed ledger technology with practical applications is Verifiable Credentials. The following case study looks at how the W3C and Decentralised Identity Foundation (DIF) are working to create business, legal and technology value by developing standards in the area of Digital Identity and Verifiable Credentials.

For a more in-depth look into blockchain and its application on the world of personal data management, the reader is invited to consult the Meeco Whitepaper on this subject matter:

https://www.meeco.me/meeco-whitepaper



[7] European Strategy for Data, 2020 – page 11

Case Study 4.

Verifiable Credentials

Companies, governments and people make claims about different types of information, as part of their everyday activities (e.g., about their share price, citizenship, location, accomplishments, assets). If these claims can be supported by evidence that verifies the provenance and authenticity of the record, then these claims can be embedded in a credential issued by a trusted authority, enterprise or organisation.

In the physical world, typically these credentials are documents like audited tax returns, passports, driver's license, diplomas, degrees, birth and marriage certificates. These are all used as proofs of our claims, such as nationality, profession, marital status or place and time of birth.

Increasingly, these physical documents have digital twins, with both versions usually issued and managed in a federated or centralised architecture, i.e. single points of control. In this model the identity provider plays a central role as the issuer and verifier of the credential in a closed eco-system. This means, in order for a service provider to benefit from trusting the credentials, they must first be permissioned by the identity provider, or become part of the closed eco-system.

In the physical world it is a common practice to use a passport or driver's license for reasons other than travel or driving. For example, identity documents are often used to enter a building or prove your age to buy alcohol. This process is usually a match between the photo ID and the person. However, it is not possible beyond doubt to determine whether either the document or the data is valid. Indeed, fake documents are everywhere and the user of the document is not always its real owner.

In the digital world the weakness and vulnerability of this traditional model is even more acute. Simply uploading a passport and taking a selfie does not provide a high level of assurance to the relying party, without validating the provenance and the validity of the document. This is an expensive process, and it usually means that the issuer is aware that the identity document is being used. It also means that the end-user (identity subject) is prohibited from digitally sharing his or her credentials outside of the closed eco-system that is required in order to trust the credential. As a further consideration, this whole process may also violate an individual's privacy, as the identity provider will know for which service the credential is being authenticated.

Verifiable Credentials and blockchain technology constitute a paradigm shift that brings the identity subject into the centre of the eco-system. This is also referred to as human-centric technology, self-sovereign or self-managed identity. The core premise is that once a credential is issued by a trusted source, then this enables individuals to manage their credentials and reuse them on multiple occasions and with 3rd parties. It also means that the credentials can be shared independently of the credential issuer, thus providing greater privacy and control for the individual.

Developing and issuing credentials against an agreed standard and combined with non-repudiation, enables individuals to use credentials in both closed and open eco-systems. This approach results in

reduced cost and increased utility. However, developing an open eco-system and interoperability requires standardisation.

Two bodies dedicated to this global task are the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation (DIF). The mission of the Verifiable Credentials (formerly known as Verifiable Claims) Working Group (VCWG) is to make the issuance and the exchange of credentials that have been verified by a third party easier and more secure on the Web.

Likewise, DIF is developing the foundational components of an open, standards-based, decentralised identity ecosystem for people, organisations, apps and devices. These combined efforts are focussed on technical specifications, reference implementations and industry coordination. Enablers such as protocols and implementations then enable creation, resolution and discovery of decentralised identifiers and names across decentralised systems, like blockchains and distributed ledgers.

The main goal of this uniform approach is to enable credentials to be universally shared with any local or foreign entity. A holder of such a Decentralized Identifier (DID) can issue credentials independently to support the validity of claim of another DID holder, subject to a standard known as Verifiable Credentials.

From a **business perspective**, these open identity ecosystems will enable companies to optimize their current business models. Especially processes that involve collaboration between different actors in the supply chain process or where traceability of goods is a legal requirement. It is also an accelerant to moving from physical documents to trusted digital credentials, which in turn can remove friction and reduce time and cost in the delivery of digital services.

From a **legal perspective**, in Europe this could be supported by an extension of the scope of the eiDAS regulation and the framework of trust that it has created, to include identity proof via verified claims. It is equally important to establish through a legal framework the responsibility, obligations and legal remedies for individuals issuing claims, those verifying them and those relying upon them.

Using blockchain technology and Verifiable Credentials, goods, suppliers and buyers can easily be identified and verified on their issued credentials throughout the whole flow. Issuing of these credentials can be done separate from each other, thus enabling single claims (data attribute) to be shared (e.g. over 18 years old) or grouped together (presentation) to support progressive disclosure of claims.

IBM and Chainyard offer a blockchain network, called “Trust Your Supplier” to optimize the supply chain process. They predict that the use of the network can reduce the on-boarding time of new suppliers up to 70-80 percent, with a potential 50 percent reduction in administrative costs.

Likely, the greatest **barrier** is the effort required to help organisations and individuals to understand blockchain and distributed technology. This may be further weighed down by the negative reputation of cryptocurrencies, which the public most frequently associate with blockchain. The lack of clarity for legal frameworks around the designation and certification of trusted 3rd parties will also slow the development of Verified Credentials.

Catalysts to accelerate the wider adoption and scaling of Verified Credentials include official (EU and Member State) support for the establishment of a governance framework accurately describing the roles of the issuer, the recipient and the verifier (or trusted 3rd party). In parallel, the population at large, including individuals and organisations require standards for interoperability so that everyone knows how to read, use and revoke Verifiable Credentials.

“Europe’s data strategy relies on a thriving ecosystem of private actors to create economic and societal value from data. Start-ups and scale-ups will play a key role in developing and growing disruptive new business models that fully take advantage of the data revolution. Europe should offer an environment that supports data-driven innovation and stimulates demand for products and services that rely on data as an important factor of production.”

– European Strategy for Data, 2020 – page 15

5. The Strategy

In the face of the vision and ambition that Europe has given itself to build a single market for data, common data spaces and a data economy and society worthy of its name, the EU has built a coherent strategy based on policy measures and funding.

The policy measures include the governance framework for the data economy, which will allow for orderly access and usage of data and the creation of Common European Data Spaces. The policy framework will also serve to support data-driven innovation and to stimulate demand for new data-enabled products and services.

The Digital Europe programme will look to support the development of personal data spaces and the EU will ensure that rules govern the providers of these personal data spaces to guarantee their neutrality. The all-important issue of data portability and enhanced control by individuals over their data will be strengthened by reinforcing Article 20 of the GDPR.

In terms of funding measures, one of the main targets of investment will be to entrench Europe's technological sovereignty for the data economy. This includes a High Impact project on European data spaces, covering data architecture, next-generation infrastructure, standards setting, tool development and best practices collection on how to deal with personal data (especially around pseudonymization).

The Digital Europe programme will also actively contribute funding for closing the skills gap, particularly in the areas of analytics and big data and the deployment of the latest technologies.

The communication document sets out the strategy based on the four following pillars:

A cross-sectoral governance framework for data access and use

The priority for the EU will be to establish a unique European legislative framework for the governance of common data spaces to be put in place in Q4'20. It will span different sectors and Member States, whose specificities may nonetheless weigh in during its elaboration. This will determine contextual data usage, standards of interoperability across sectors and facilitate cross-border data usage. The EU recognizes the need to proceed with an open mind, as it does not hold all answers as to how the journey to the data economy will unfold. As such it prefers to provide frameworks that provide a context, but still allow ecosystems to develop in a dynamic manner.

Second, the EU will work on the procedure for the adoption of an Implementing Act on High-Value Data Sets in Q1'21 under the Open Data Directive, making high quality public-sector data sets available across the EU for free and for reuse in innovation.

Third, the EU will explore, as part of the Data Act in 2021, how best to incentivise actors in the data-agile economy to engage in horizontal data sharing across sectors. In doing so, the EU recognises the need to provide guidance as to how data sharing and pooling arrangements will be impacted by EU Competition Law through an update to the Horizontal Cooperation Guidelines. In the same spirit, but outside the Data Act, the EU will consider how to address systemic issues related to data accumulation in vast quantities by platforms and Big Tech companies, including possible legislation to ensure fair competition across all markets and actors.

Last, the EU pledges to lead by example, in improving the organisation and usage of its data and by making available the data that it produces and funds.

Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability

The EU will build an environment that will foster innovation and the development of data-enabled products and services. Start-ups and scale-ups are expected to play an important role in this development of the data economy.

This environment will be supported by an ambitious investment programme in the form of the High Impact project on European data spaces to finance next-generation infrastructure and services for data processing by means of cloud computing in data centres and highly distributed and smart data processing at the edge.

It will also fund data sharing architectures such as standard setting, tool development and collating best personal data management practices, as well as governance mechanisms. In total, this should involve combined investments of €4-6 billion, of which the EU could invest up to €2 billion. The first implementation phase is foreseen for 2022. This is part of wider strategic investments in new technologies that the EU will make as part of its industrial strategy.

In order to further advance its technical sovereignty, the EU will Sign Memoranda of Understanding with Member States on cloud federation in Q3 2020 with a view to fostering pan-European cloud participation and capacity to scale. It will create an EU (self-)regulatory cloud rulebook in Q2 2022 and it will launch a European cloud services marketplace, integrating the full stack of cloud service offering in Q4 2022.

In terms of data interoperability, the EU will fund the establishment of EU-wide common, interoperable data spaces in strategic sectors, to overcome legal and technical barriers to data sharing and address issues of trust, by way of common rules developed for the space. Funding will also support authorities in the Member States in making high value data sets available for reuse in the different common data spaces.

Competences: Empowering individuals, investing in skills and in SMEs

First, the EU wants to strengthen the control that individuals have over the usage of their data through the establishment of personal data spaces. This will likely be done through a combination of reinforcing the data portability rights under Article 20 of GDPR, consideration of rules on the neutrality of data operators in the forthcoming Data Act and through the Digital Europe programme in terms of the development and roll-out of personal data spaces.

The Digital Europe programme will also fund the development of skills for a pool of 250.000 people to narrow the gap in terms of big data and analytics capacities. This will enhance capacity to deploy the latest data technologies in businesses throughout the EU. In terms of general data literacy, the Reinforced Skills agenda will set a pathway to increase the proportion of the EU population with basic digital skills, from the current 57% to 65% by 2025.[8]

Start-ups and scale-ups are seen as important actors for the future of Europe's data economy. In its upcoming SME strategy, the EU will define measures to build capacity for SMEs and start-ups, since their development based on data is not very capital intensive. The Horizon Europe and Digital Europe programmes will create opportunities for SMEs in the data economy, to have better access to data and to develop new services and applications based on data.

[8] European Strategy for Data, 2020 – page 20

Common European data spaces in strategic sectors and domains of public interest

In addition to the measures, programmes and key actions enumerated in the previous 3 points, the EU will develop common European data spaces to facilitate the sharing and usage of data that can have a systemic impact on Europe, its citizens, enterprises and organisations. This means that substantial pools of data will be available to fuel the data economy and society. Infrastructure, technical tools and governance mechanisms will facilitate access and usage of the data in these common European data spaces.

As key actions the EU will propose a legislative framework for the governance of common European data spaces, Q4'20, it will adopt an implementing act on high-value data-sets, Q1'21, it will propose, as appropriate, a Data Act, 2021 and it will analyse the importance of data in the digital economy (e.g. through the Observatory of the Online Platform Economy), and review of the existing policy framework in the context of the Digital Services Act package in Q4'20.

The nine common European data spaces are listed below:

1. Industrial (manufacturing) data space
2. Green Deal data space
3. Mobility data space
4. Health data space
5. Financial data space
6. Energy data space
7. Agricultural data space
8. Public Administration
9. Skills data space

The key to this all coming together, with data sharing and usage working in a fluid and useful manner is interoperability. If Party A cannot easily read and reuse the data that Party B is sharing, then there is absolutely no point in sharing the data in the first place. For this, the EU requires an enabling legislative framework that will help to:

"strengthen the governance mechanisms at EU level and in the Member States relevant for cross-sector data use and for data use in the common sectoral data spaces, involving both private and public players. This could include a mechanism to prioritise standardisation activities [36] and to work towards a more harmonised description and overview of datasets, data objects and identifiers to foster data interoperability (i.e. their usability at a technical level[37]) between sectors and, where relevant, within sectors[38]. This can be done in line with the principles on Findability, Accessibility, Interoperability and Reusability (FAIR) of data taking into account the developments and decisions of sector-specific authorities" [9]

The following Case Study illustrates examples of emerging standards and global initiatives that underpin data interoperability and data reusability, which are so necessary to realise the societal value of common European data spaces.

[9] European Strategy for Data, 2020 – page 12

Case Study 5.

Data Interoperability and Reusability

Cross sector personal data use requires data interoperability and data reusability. It also requires governance as a strong foundation. Bodies such as MyData.org[10] and The Kantara Initiative are examples of organisations dedicated to shaping thought leadership and developing standards across key aspects of Human-Centric personal data management and data audit.

The purpose of MyData Global is to **empower individuals by improving their right to self-determination regarding their personal data,** based on the MyData Declaration. MyData Global has 90+ organisation members and over 600 individual members from over 40 countries, on six continents, facilitating a 2000+ strong global community working on the ethical use of personal data. This global movement formed from the seminal MyData White Paper first published in Finland in 2014.

The Kantara Initiative is also a member based not-for-profit, offering conformity assessments and assurance, granting Trust Marks against Standards under its Trust Framework program. In parallel, Kantara develops specifications to transform the state of Consent and Information Sharing, Consent Management Solutions and Identity Relationship Management. In particular, the set of standardized OAuth extensions known as User Managed Access (UMA) and Consent Receipt.[11]

Indeed, one of the greatest benefits to be had from the advent of the data economy is the systematic reuse of the same data across multiple applications and amongst multiple organisations. As the EU communication states, data is one of those rare commodities that can be used again and again at little or no additional cost. However, reuse of data can only be done in a fluid and efficient manner if the data is interoperable i.e. it does not require translation or transformation when used by different recipients in different data models.

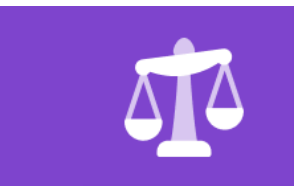
From a **business perspective**, the Kantara Initiative Consent & Information Sharing Workgroup provides a standard for an interoperable Consent Receipt, in the area of personal data sharing and usage. The specification includes the corresponding JSON field names and types (necessary for interoperable data exchange and processing).

The need for the Consent Receipt Standard arose because individuals are asked all the time for their consent to allow enterprises and organisations to collect, use and disclose personal information about them, principally in the process of these individuals accessing their on-line services, websites or platforms.

To date, there has been no universally accepted standard for Consent Receipt, and this means that there can be no common consent practices, consent management interoperability and standardised

[10] European Strategy for Data, 2020 – page 10
[11] Example in Annex B of DIS ISO/IEC 29184Online privacy notices and consent and ISO/IEC 27560 Consent record information structure

proof of consent. This standard for consent records allows both organisations and individuals to maintain and manage permissions for personal information.



From a **legal perspective**, the business advantages of standardised consent receipt management are the reassurance for all stakeholders that an individual's personal data is interpreted in the same way between different actors in the same sector, between actors in different sectors and also across borders.

This also provides legal proof that consent has been given for the access and use of personal data and an audit trail of any subsequent modification or revocation. This can also serve to drive reusability of data, which in turn can bring phenomenal efficiency to processes such as onboarding clients including Know Your Customer (KYC).

From a **technology perspective**, MyData.org is driving the agenda for a human-centric approach to the development of personal data management technology. Specifically, MyData provides a set of guiding technical principles to help individuals gain better control over their personal data disseminated throughout the digital world.

1. Human-Centric Control of Personal Data
2. Individual as The Point of Integration
3. Individual Empowerment
4. Portability, Access and Re-Use
5. Transparency and Accountability
6. Interoperability

The latest initiative from MyData.org is the publication of a new white paper: Understanding MyData Operators[12]. The paper describes the techno/legal role of an Operator responsible for operating infrastructure and providing tools for the person in a human-centric system of personal data exchange. Enabling people to securely access, manage and use personal data about themselves, as well as to control the flow of personal data with, and between, data sources and data using digital services.

Barriers to interoperability and reusability of EU data will continue to exist if:

- Standards remain different across sectors and amongst Member States.
- Regulation does not allow for common trust frameworks that render personal data both trustworthy and interoperable.
- Enterprises and organizations continue to believe that customers belong to them, as well as the personal data they collect and store on individual customers.

The **catalysts** to drive scalability, interoperability and reusability of data include:

- Wider adoption of EU and global standards for data exchange and consent.
- Reinforced data portability rights under GDPR.
- Certification for data operators as neutral data platform providers.

[12] Understanding MyData Operators, White Paper published April 2020

In particular, the EU will look to ensure that any access to its citizens' personal data and to commercially sensitive data can only take place in full respect of Europe's legislative and regulatory frameworks.

6. An open, but proactive international approach

The EU is very clear in its strategy document that it intends to reach beyond its borders, in all matters that involve international data flows. This is important as European companies operate with global reach and their competitiveness is as dependent on data within Europe as it is outside its confines. The strategy states clearly that the EU is more than willing to cooperate hand-in-hand with regulators and authorities around the world as regards international data flows, but it will do so in an assertive manner that fully protects the interests of Europe and its citizens.

In particular, the EU will look to ensure that any access to its citizens' personal data and to commercially sensitive data can only take place in full respect of Europe's legislative and regulatory frameworks.

The EU also believes that it can take advantage of its effective data regulatory and policy framework to attract the storage and processing of data from other countries and regions, and to increase the high-value-added innovation that arises from these data spaces. This is something that Meeco has already experienced by locating systems and infrastructure within the EU.

As a key action, the EU will create a framework to measure data flows and estimate their economic value within Europe, as well as between Europe and the rest of the world, Q4 2021.

In terms of development of new business models in the data economy, it is likely that many of these models will operate on an international basis and possibly beyond the borders of the EU. This only reinforces the need for the EU to weigh in with its full might in terms of ensuring that individual's data rights are fully respected. Were the contrary to occur, then this could put at peril the adoption of these new business models.

"The Commission will be particularly vigilant to protect and assert the rights, obligations and interests of Europeans and companies, in particular as regards data protection, security and fair and trustworthy market practices. The Commission is convinced that international cooperation must be based on an approach that promotes the EU's fundamental values, including protection of privacy. The EU must ensure, therefore, that any access to EU citizen's personal data and European commercially sensitive data is in compliance with its values and legislative framework."[13]

The final case study involves just such an innovative and disruptive business model that could only operate on a cross-border basis if the sharing of individuals data rights under European standards and regulations were fully respected.

[13] European Strategy for Data, 2020 - Page 23

Case Study 6.

Disruptive Data Business Models

Once implemented, the EU Data Strategy has the potential to enable a range of new and disruptive data driven business models. Europe's competitive advantage is both the size of the single digital market and the clarity of a united strategy, regulatory and data privacy environment.

European economy and society could be positioned to leverage personal data more effectively, if individuals, enterprises and organisations establish enough mutual trust to exchange personal data on an ongoing basis. At both ends of the spectrum, there are fundamentally different business models:

1. A business model predicated on the monetisation of personal data by virtue of the transfer of control (voluntary or involuntary) from the data subject, or

2. A business model predicated on collaboration between the data subject and 3rd parties, which creates or results in equitable sharing of value, whilst preserving the data rights of the individual.

In Meeco's view, it is clear that the collaborative form of business model will generate more value, because this approach fosters greater transparency, increased trust and therefore results in better access to personal data. Additionally, it fosters the conditions for the optimal value of personal data to be derived through:

Accuracy + Timeliness + Context + Intent.

For example, the family that genuinely wants to buy a hybrid car today is worth so much more to a suitable car manufacturer than ad-click bots. Consider this example via a collaborative approach where the purchase intent is broadcast to a curated group of preferred car brands.

A disruptive new business model is one which would help individuals to generate value for themselves directly from their intent and qualified personal data without selling or monetising the data. Enabling a consent-driven, reverse enquiry marketplace, in which individuals choose to expose their data via a trusted data management platform to selected enterprises in order to obtain a personalised service.

From a **business perspective**, an individual intends to buy a car and wants to get offers from 3 favourite brands. The individual is prepared to share his or her life stage, affordability, family composition, profession and brand preferences. The individual may also choose to provide additional descriptive attributes, such as concern for his or her carbon footprint. Together, all this data and personal information will give a brand a better understanding of the prospect's persona, without having access to Personally Identifiable Information i.e. anonymity is preserved until the prospect chooses otherwise.

The individual can choose how much information to give at what stage of the enquiry and possible transaction. This option using Verifiable Credentials allows the car buyer to avoid disclosing all of his or her information up-front, just to subsequently discover that the car that appeared at first to be of interest

is in fact not suitable, affordable or simply that the offer is not right. The advantage of this "intentions" model is that the willingness to share more personal data with the brands will allow them to better model and understand the individual's lifetime value, on the assumption that through the delivery of genuine value, he or she becomes or continues to be a repeat customer.

This better understanding of the individual's profile and value should motivate brands to price the lifetime relationship, versus a one-off transaction. So, maybe one of the car brands is prepared to offer a 10% discount from the list price. If a deal is concluded the brand has successfully sold a car to a potential repeat customer. The customer has received a great deal on his or her dream car.

What is true of buying a car also works when taking out an insurance policy, contracting a loan, looking for a new advisor for an investment portfolio, buying a flight or booking a honeymoon. For enterprises offering their customers human-centric technology, they are set up to participate in this reverse enquiry model. It is a direct non mediated opportunity to get qualified traffic in the form of real prospects.

This is a service model that puts individuals in control of their personal data and it generates great value for them. For organisations, the benefits span better productivity, considerable cost efficiencies, nice revenue-sharing opportunities and a means of really boosting customer loyalty through innovation and truly useful service.

From a **legal perspective**, there are existing and emerging data regulations that support new business models. For example, the General Data Protection Regulation (GDPR) is focussed on minimising data collection whilst increasing individual (data subjects) rights. Likewise, the Consumer Data Right (CRD) in Australia is designed to enable individuals make better choices across financial services, telecommunications and utilities.

At the heart of these legal requirements is greater transparency, increased data rights, revocation and rights of erasure for individuals. If this is the new normal, business models must evolve to both build for legal compliance and flex to offer better customer outcomes.

From a **technology perspective**, there a number of ways these new models can both enable data compliance and provide greater data access. Adopting emerging standards such as Verifiable Credentials and human-centric technology support a simple three phase process, which can both reduce cost and design for solution personalisation. The steps are:

1. Drive By – minimum amount of data to enable assessment of purchase intent and customer value
2. Tell Me More – data request to model the personalisation, pricing or customisation of service
3. Transact – data required to lawfully complete the transaction, for example identity and affordability.

Barriers to this model include the slow uptake and implementation of human-centric tools to collaborate directly with enterprise and government services. As these tools become more widespread, as advocated in the EU Data Strategy, direct and peer-2-peer connections between enterprise and customers will enable these new business models to emerge. Furthermore, this approach will enable organisations to refine their offers in collaboration with their customers, based on better quality and more timely data.

Catalysts to drive adoption and scalability of these new business models include:

- Offer and uptake of human-centric technology and digital tools.
- Adoption of EU Standards to enable Verified Credentials and data interoperability.
- Reduction in reliance on current platforms (social, advertising, retail) that monetise data versus surfacing intent insight that rewards individual participation.

“In order to secure its digital future, the EU must seize its window of opportunity in the data economy.”

– European Strategy for Data, 2020 – page 25

7. Conclusion

The EU's conclusion to the communication document on the European Strategy for Data once more states the vision and ambition for Europe to achieve a preeminent position amongst the data-agile economies of the world. But this, it cautions, will not come at the cost of European standards and values. Thus, it reads:

"This Communication puts forward a European data strategy whose ambition is to enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens. It enumerates a number of policy measures and investments needed to achieve this goal.

The stakes are high, since the EU's technological future depends on whether it manages to harness its strengths and seize the opportunities offered by the ever-increasing production and use of data. A European way for handling data will ensure that more data becomes available for addressing societal challenges and for use in the economy, while respecting and promoting our European shared values.

In order to secure its digital future, the EU must seize its window of opportunity in the data economy."[14]

The strategy itself is indeed coherent and seemingly complete, but the true question is whether it is sufficient to enthuse, motivate and incite all actors, whether private sector or public sector, whether individual citizens or society as a whole to act responsibly and take the actions that are called for. Indeed, the expression of goodwill alone will not be enough.

The consequences of inaction and complacency, were they to take root, would be dramatic for Europe's economy, its society and its citizens, at all levels. The role of all of us in Europe is therefore to inform and educate ourselves and those around us as to the importance of data and what we can do with it. Then we need to formulate our very own strategies and the roadmaps to implement them. It would be nice to see further concrete detail in the coming months and quarters on what the EU and Member States will do in practice to incite enterprises and individuals to jump onto the train and commence their data journey.

Now it is up to us, as citizens, as enterprises and as organisations to turn this strategy into reality. For this, we need to maintain the following building blocks and principles at the forefront of our minds:

- ✓ Personal data management in Europe must remain human-centric, always placing the individual at the centre.
- ✓ GDPR constitutes a strong regulatory framework, which sets out very clearly the data rights of European citizens and residents.
- ✓ Private persons have the right to understand and agree to the use of their data and to control the impact that such use may have on them.
- ✓ Technology, as regards personal data management, is only there to serve the best interests of the individuals and should not become an end unto itself.

[14] European Strategy for Data, 2020 – page 25

About Meeco

Meeco gives people and organisations the tools to access, control and create mutual value from personal data. Privately, securely and always with explicit consent.

Meeco provides the underlying technology to enable enterprises to become compliant MyData Operators, with interoperability across their B2B, B2B2C and Me2B services. Our technology always adheres to human-centric data management principles and privacy regulation.

Founded in Australia in 2012, Meeco has won five global awards and is independently acknowledged as a pioneer in the area of personal data management. Our end goal is to create a more level playing field between individuals, enterprises and government in order to generate more societal value. We believe that trusted and transparent data management can result in better health, education, financial and environmental outcomes for all.

This can be achieved by a combination of our patented technology, secure API platform and secure data enclaves. We combine this powerful technology with innovative use cases that can enhance existing and create exciting new data-enabled business models.

The organisation has grown from start-up to a global scale-up with operations in Australia, Belgium and the United Kingdom. Our infrastructure is hosted in the European Union, which means GDPR compliance is our base line.

Meeco strongly believes that the only way to reverse the adverse trends that have led to the improper use of personal data is to create a more symbiotic relationship between organisations gathering and using personal data and the data subjects themselves.

This is about individuals providing quality and up-to-date personal data and information on a pro-active basis to organisations, that in turn warrant that they will use it in a responsible manner.

This is about individuals giving consent for the access and use of their data.

This is about reducing the burden on individuals having to provide the same data on a recurring basis, because we should be able to re-use data already provided.

This is about organisations having access to personal data in a way that helps them to reduce their operating costs for processes such as onboarding, KYC or direct marketing.

This is about creating a balanced relationship in which individuals and organisations alike gain and share in the benefits and value generated by the transparent exchange of personal data.

With these last thoughts, we hope that this paper has been useful in exploring the “A European Strategy for Data”, as communicated by the EU on February 19th. At Meeco, we’re encouraged by what we read in the communication document, we are excited by the EU’s ownership of the issues and we strongly believe in many aspects of the data strategy that it has laid out. This is why at Meeco our vision is *“to create a place for everyone to get equity and value in exchange for the data they share”*[15].

Together, let’s make this a reality!

[15] Meeco Manifesto, 2012

Authors and Contributors

Lead Author
Charles McArthur, Global Head of Business Development, Meeco

Contributing Authors
Katryna Dow, CEO & Founder, Meeco
Jo Vercammen, CTO, Meeco

Digital Production
Mars El-Bougrini, Head of Design & UX, Meeco

Featured Case Studies
1. API-of-Me Platform, Meeco
2. Nexia Wealth Connect
3. KBC Bank
4. W3C and Distributed Identity Foundation (DIF) Verified Claims Standard Development
5. International Bodies Developing Human-Centric Data Solutions, MyData.org, Kantara Initiative
6. Disruptive Business Models for the Personal Data Economy – Meeco

For More Information

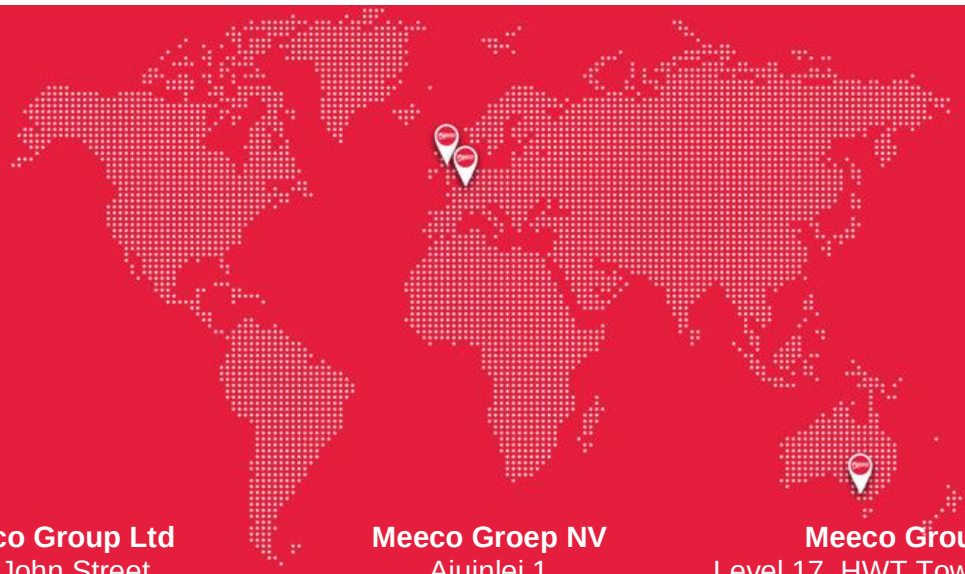
Visit our website: https://meeco.me

Enquiries: info@meeco.me

Demo: https://www.meeco.me/contact

Developer Portal: https://dev.meeco.me/

Data Strategy: https://meeco.me/data



Meeco Group Ltd
10 John Street
London WC1N 2EB
United Kingdom

Meeco Groep NV
Ajuinlei 1
9000 Gent
Belgium

Meeco Group Pty Ltd
Level 17, HWT Tower, 40 City Road,
Southbank VIC 3060
Australia