Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific Prosperity

Public-Private Dialogue (PPD) on Personal Data Protection and Utilization in the Asia-Pacific Region: Challenges and Opportunities

APEC Digital Economy Steering Group

April 2021

APEC Project: ECSG 02 2019A – Public-Private Dialogue (PPD) on Personal Data Protection and Utilization in the Asia-Pacific Region: Challenges and Opportunities

Produced by:
Choong-nyoung Lee (Mr)
Ministry of Trade, Industry and Energy
Government Complex-Sejong, 402, Hannuri-daero, Sejong-si
Republic of Korea
E-mail: young121@korea.kr

Prepared for:
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#221-CT-01.5

Acknowledgement

This project was guided by APEC Division, the Ministry of Industry, Trade and Energy, Korea. It was developed under closer collaboration with APEC Electronic Commerce Steering Group (ECSG) and honourable speakers from Australia; Chile; Japan; Korea; the US; other non-member economies such as UK; Finland; Belgium, and genuinely supportive co-sponsor economies namely Australia; Chile; Indonesia; Papua New Guinea; Peru; Philippines; and Chinese Taipei. This report consists of two parts: Summary of the Dialogue (starting from page 1) and Research paper (starting from page 13). The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official policy or opinion of all APEC member economies.

Table of Contents

Part I. Summary of the Dialogue

Part II. Research Paper

List of Tables

List of Figures

Part I. Summary of the Dialogue

1 Executive Summary

1.1 Overview

The Public-Private Dialogue (PPD) was held in a hybrid mode due to the COVID-19 pandemic on 25 November 2020. This PPD discussed two main points : (1) sharing experiences and business practices of MyData ; (2) discussing future tasks in terms of technical, institutional and cooperational aspects. All 21 APEC member economies are invited to attend and participate in the PPD. More specifically, APEC government officials and policymakers in charge of data protection are very much encouraged to take active part in the event to exchange views and experience on government policies and measures. Also, private representatives from Meeco in Australia, Lifesemantics in Korea, NTT in Japan participated in PPD as well.

The main objective for this PPD is threefold. Firstly, PPD will increase knowledge and understanding of policy framework for APEC economies, particularly policy makers, regulators and experts, to promote personal data protection and utilization. Second, PPD will draw valuable inputs for economies to consider policy approach that is less trade-restrictive and more conducive to open exchange and utilization of personal data while robust and effective safeguarding of privacy. Finally, PPD will establish momentum for continued discussion on personal data protection and utilization through relevant fora in the APEC. The meeting was held in through Zoom Virtual Meetings platform. Speakers and participants were gathered in that platform with two sessions of dialogue. The meeting was held successfully. Participants have been actively involved in dialogue and questions answers sessions with the speakers.

1.2 Event Details

The event was organized as follows:

1) **Opening Remarks**
2) **Keynote Speech**
3) **Session 1:** Case Studies of MyData Utilization
4) **Session 2:** Cooperation Tasks for Global MyData
5) **Closing Remarks**

The Policy Dialogue was attended by 45 people from all 9 APEC member economies, including 10 speakers and 4 discussants from Australia; Chile; Japan; Korea; The US; other non-member economies such as Finland and Belgium. The details of the speakers are as follows:

- Mr Chang, Sung-Gil, Director of the Ministry of Trade, Industry and Energy, Korea

- Ms Bojana Bellamy, President of Centre for Implementation Policy Leadership, UK

- Ms Viivi Lahteenoja, MyData Global, Finland
- Mr Pablo Trigo Kramcsak, the Council for Transparency of Chile, Chile
- Mr Dong-Bum Kim, Director of LifeSemantics Corp, Korea
- Mr Masahiro Hanatani, Senior Manager, Digital Strategy Section, Business Strategy Department, Financial Segment, NTT DATA Corp, Japan
- Ms Katryna Dow, CEO of Meeco, Australia
- Mr Christopher Lee, Director General of MyData Korea Hub, Korea
- Mr Adrian Gropper, CTO of Patient Privacy Right, US
- Mr Akio Shimono, Manager of Fujitsu Ltd, Japan
- Mr Jae Hoon Lee, Research Fellow of Korea Institute of S&T Evaluation and Planning, Korea
- Paul Olivier Dehaye, Personnal Data IO, Begium
- Ms Hyo Young Lee, Korea National Diplomatic Academy, Korea

2 Background

Securing the free flow of data while respecting applicable domestic laws and regulations, that avoid imposing discriminatory or unnecessary restrictions on transfers of information and data, is important for developing innovative business models and promoting digital economy. However, there is also a clear need for effective safeguarding of privacy and personal data, while ensuring legitimate policy objectives and public welfare. The APEC Internet and Digital Economy Roadmap (AIDER) suggested securing privacy on one hand and flow and utilization of data on the other at the same time. Also, the APEC Privacy Framework (2015) promotes privacy and personal information protection while ensuring the free flow of data. But, how can an individual government and APEC as a whole realize such goals? Perhaps, this is a problem that affects many APEC economies as they share common purpose of developing digital economy and pursue this purpose with many creative ideas and solutions.

This project seeks to explore the ways for personal data protection and utilization, and examine diverse approaches within the region. The project will also explore how personal data protection and utilization can contribute to the implementation of the AIDER.

3 Event Summary

3.1 Opening Remarks

In the opening remarks, Mr Chang Sung-Gil, Director General of the Ministry of Trade, Industry and Energy, Republic of Korea, emphasized the importance of data utilization and protection in the current era of digital transformation and explained the role of APEC and the Korean government in the discussion of digital issues and the development of related frameworks. He said that over several years, we have witnessed a rapid digital transformation across the entire globe and how the ongoing COVID-19 pandemic has accelerated an avoidable trend. The digital transformation will bring tremendous changes to trade and the economy. Over the ensuing decades, the proportion of the economic value created based on digitally enabled platforms will increase sevenfold

APEC has served as a key channel for discussing digitalization since the establishment of ECSG in 1999, which led to successful implementation of the APEC CBPR. The adoption of the APEC Internet and Digital Economy Roadmap in 2017, the creation of the Digital Economy Steering Group in 2019, and the Kuala Lumpur Declaration adopted in November 2020 have ushered in a new era of regional cooperation on the digital economy. The Republic of Korea is already a key supporter of APEC cooperation when it comes to digital issues; President Moon suggested launching an APEC digital innovation sub-fund, which was then established in 2018, through which the dialogue is funded. In the Kuala Lumpur declaration, APEC leaders highlighted the importance of cooperation in facilitating the flow of data and strengthening consumer and business trust in digital transactions. This declaration requires economies to find a sort of balance between digital data utilization and protection. And this is what the dialogue intends to contribute to. One of the most useful tools for sustaining balance between the two values is MyData ecosystem. MyData helps people using personal data for their own purposes or sharing it in a secure manner. The MyData ecosystem is a prominent and safe method for facilitating flows of data, meaning that it allows people to use their data with great flexibility and freedom all while ensuring privacy and security of the data. In this regard, Mr. Chang emphasizes that the dialogue will be beneficial and timely in better understanding the MyData ecosystem.

3.2 Keynote Speech

This session describes the importance of the data economy and MyData for the remainder of the dialogue. It was comprised of three presentations, each lasting 15 minutes. The expert presenters were:

- Ms Bojana Bellamy
  President, Centre for Implementation Policy Leadership, UK

- Ms Viivi Lahteenoja (originally, the presenter was Mr Teemu Ropponen, but for personal reasons, Ms Viivi was replaced) MyData Global, Finland

- Mr Pablo Trigo Kramcsak
  The Council for Transparency of Chile

3.2.1 Presentation by Ms Bojana Bellamy

Ms Bojana Bellamy explained the data economy. The Fourth Industrial Revolution (also known by the acronym 4IR and the term Industry 4.0) has led to the advent of an era marked by technological revolution that is blurring the lines between the physical, digital and biological spheres. Furthermore, COVID-19 has accelerated this revolution.

According to a KPMG report published in 2020, 64 percent of CEOs report that the pandemic has accelerated the creation of new digital business models and revenue streams. And at the heart of the Fourth Industrial Revolution sits data: data serves as a driver of the economy and innovation and as an asset for businesses and governments. Also, global data flows increase value for consumers and lead to economic growth. However, there exist several challenges related to data, such as privacy and security problems, the trust deficit and sensitivities about the use of data, and inconsistencies with traditional laws and regulations. Therefore, a data framework for the trusted digital age should be established based on blocks which consist of organizational accountability, empowered individuals and smart regulations and regulators.

3.2.2 Presentation by Ms Viivi Lahttenoja

Ms Viivi Lahteenoja of MyData Global described the general features of MyData. MyData refers to the use of personal data as a resource that individuals can access and control. It represents a paradigm shift in personal data management and processing in seeking to transform the current organization-centric system to a human-centric system. There is more personal data being collected now than ever before.

There is great potential for service users to make use of their own personal datasets. Many services already provide options for downloading personal data. But there are currently no industry standards or best practices. In this respect, sharing practices and discussing future orientations for establishing related frameworks and policies is important. From the demand side, the ethical use of data is always the most attractive option, and from the supply side, people get value from their data and set the agenda on how it is used.

3.2.3 Presentation by Mr Fablo Trigo Kramcsak

Mr Pablo Trigo Kramcsak introduced Chile's data protection regulatory framework and the challenges it faces. Chile is renowned for its commercial openness and high economic integration with the world, with an important network of agreements to promote trade and investments. Chile is becoming Latin

America's data center hub. But as the Chilean Data Protection law has been evaluated to be insufficient and outdated in addressing the digital transformation, there has recently been introduced a bill that seeks to amend the CDL. The bill establishes a single independent supervisory authority for the public and the private sector, the Chilean Transparency Council, which would assess effective and dissuasive fines and sanctions for specific data protection violations. Moreover, the bill regulates the international transfer of personal data.

3.3 Session 1: Case Studies of MyData Utilization

In this section, Mr Chul Chung, Senior Fellow of the Korea Institute for International Economics Policy, Korea, played the role of moderator.

The first session aimed to share experiences and practices of MyData-related businesses centered on three main topics: Health, System and Personal Data Storage. The three experts were:

- Mr Dong-Bum Kim
  Director, LifeSemantics Corp. Korea

- Mr Masahiro Hanatani
  Senior Manager, Digital Strategy Section, Business Strategy Department, Financial Segment, NTT DATA Corp. Japan

- Ms Katryna Dow
  CEO, Meeco, Australia

3.3.1 Presentation by Mr Dong-Bum Kim

Mr Dong-Bum Kim, director of LifeSemantics, introduced the business model of his firm, called a PHR (Personal Health Record) platform and digital health service, which was established in 2012. Its services are based on medical information technology, big data, artificial intelligence, cloud computing blockchain. A PHR includes medical records and lab results generated by medical institutions, as well as activity data generated by an individual's smartphone, wearables or other personal health devices. The latter types of data differ from the data of medical institutions in that individuals themselves have ownership of the data. LifeSemantics also provides artificial intelligence, information management technology and a secure environment to store, analyze, and utilize personal health records. All services as a cloud service are needed for customers to have a stable business. With respect to data collection, the firms collects data by extracting data from existing health data platforms such as Samsung Health, Google Fitness and Apple Health, from hospital systems (which consist of push type and pull type data) and from devices and sensors such as 'efil'. For the security of digital health platforms, LifeSemantics

complies with international standards related to security, data exchange, and information processing such as ISO 27001 (verification of the information security management systems) ISO 27017 (verification of the cloud service personal information management system) and ISO 27799 (verification for the medical information protection management system).

3.3.2 Presentation by Mr. Masahiro Hanatani

Mr Masahiro Hanatani shared general knowledge about personal data and introduced the business model of Japanese firm NDD. Its personal data bank is a service to manage personal data based on entrusted agreements with individuals on the utilization of their data and to provide such data on behalf of the individuals to third parties in agreement with the instructions of those individuals or according to pre-specified conditions. Customers store and manage their personal data on servers provided by a PDS (personal data storage) company which provides a system for individuals to collect and control their personal data as they wish, returning direct and indirect benefits to the customer.

The Data economy an important agenda items for the Japanese government. Former leader Shinzo Abe emphasized the acceleration of innovation through the use of data and the free flow of data across borders at the Davos forum. In Japan, the personal data bank certification system, which was established in 2018, and reliable information banks have been certified since 2019. The certification system allows individuals to choose organizations where they can deposit data with confidence. Also, individuals can benefit not only from the financial benefits of positing data, but also from more personalized services. Consistent with the Japanese government's initiative on data exchange and data utilization, NTT Data argues that personal data can be used without being distributed, and people can control the use of own personal data. NTT Data proposes the introduction of two data consent tools, called My Information Tracer and Consent Wallet, as well as promoting data use without distribution. My Information Tracer is a platform for distributing personal data that will be released commercially in October 2020. By acting as a hub connecting businesses and providing basic functions necessary for personal data distribution, such as a unified authentication function using a common ID, the platform facilitates the coordination of personal data across businesses and promotes the personal data distribution business. Through the Consent Wallet tool, users that agree to terms of service through the platform can confirm and change what personal data provide, and to which companies. Consent Wallet provides the ability to automatically create TOS and visualizes the status of consent flows.

3.3.3 Presentation by Ms. Katryna Dow

The vision of Meeco is to give people and organizations the tools to access, control and create mutual value from personal data. Meeco allows customers to securely store personal data and access it across all devices, and automatically updates information after editing. The applicable sectors include travel preferences, insurance and finance, identity and health and fitness. Meeco has been at the forefront of

the emerging personal data economy since 2012, having developed a platform suite of APIs and a Consent Engine, which enables customers to aggregate personal data in all aspects of their lives, including identity, social, IoT, finance, health and lifestyle, and share it directly with the people and organizations they trust. For enterprises, Meeco enables trusted data ecosystems to develop through existing business to business relationships, where new business models can be developed in partnership with customers. Consistent with the regulatory change in Australia, Meeco has established an Open Banking Sandbox. This established testing and iteration environment is designed for financial institutions to trial new consent-based customer experiences. The objective is to help organizations design their service tools for increased customer trust, while meeting the compliance requirements of the proposed regulation.

3.3.4 Designated Discussion

Mr Akio Shimono of Fujitsu offered his take on MyData and shared Fujitsu's approach to MyData. He argued that the key essence of MyData is to empower people, or save them from "data slavery." For every person, digital empowerment should come with transparency and for companies, an open and secure data flow should be the basis of a healthy data economy. Fujitsu pursues MyData projects based on a goal-oriented and human-centric perspective. It operates an open source PDS project called Personium. The Personium PDS can be independently operated but still form a global network. Consumers can choose a provider and interoperability among providers exists.

Another designated discussant, Mr Jae Hoon Lee, mentioned the challenges Korea faces with MyData. In Korea, the National assembly has passed an amendment to three major privacy laws: the personal data protection law, the law on the promotion of information and communication networks, and the law regulating the utilization and protection of personal information and credit information. Specifically, the finance industry is focusing on the credit information act as it generates clear momentum to expand MyData business. The most important challenge of facing MyData in Korea is that it is limited to the financial industry, as other sectors lack an institutionalized legal framework. In sectors such as the medical and energy sectors, MyData has no legal basis on which to operate. It is necessary to consider the use of MyData in various industries and to prepare an institutional context in which to develop MyData industry. Such regulation could guarantee higher quality products.

3.4 Session 2: Cooperation Tasks for Global MyData

In this session, Professor Joo-Seok Park of Kyung Hee University in Korea, played the role of moderator.

This session aimed to explain the institutional, technical and cooperation tasks for APEC with regard to Global MyData. Speakers are representatives from both the private and public sectors who evaluate the current situation and propose plans of action. The expert presenters were:

- Mr Christopher Lee
  Director General, MyData Korea

- Mr Adrian Gropper
  CTO, Patient Privacy Rights, USA

- Ms Hyo Young Lee
  Professor, Korea National Diplomatic Academy, Korea

3.4.1 Presentation by Mr Christopher Lee

Mr Christopher Lee suggested what governments can do to establishing a better MyData ecosystem. Personal data should be explained from the perspective of individuals and businesses regarding the use of personal data across borders. As there are barriers inherent in personal data, such as language, legal protection, and different rules of engagement for each economy, governments should prepare a means to ensure transparency and interoperability. Transparency is about creating trust in the ecosystem and keeping individuals and organizations accountable for their actions and decisions. However, transparency is not necessarily profitable. Meaning, regulations are necessary. Regulation and remedial procedures are a part of the critical infrastructure for transparency. It is why we are seeing personal information protection laws being revised and amended recently. Japan, Korea and Singapore have revised their personal information protection laws in this year. These measures are prerequisites for cross-border personal data interaction. In order to be a part of a MyData ecosystem, transparency must be enforced. Interoperability implies transportability. There must be a way to transport personal data. In order to be a part of a MyData ecosystem, guarantees for individuals to take their data with them, again physically and virtually, are necessary. To ensure the safe flow of data, we have to establish international standards. Mr Lee suggested establishing a minimum set of standards he dubbed the Gold Button for the MyData ecosystem. Also, as part of the MyData roadmap, he mentioned that a key takeaway is that cross-border collaboration is the starting point. Inter-connecting government agencies should come first, where generic human-centric standards are established. Private sector business considerations are important too, but not as important as ensuring the cross-border infrastructure can provide a frictionless experiences at the individual level.

3.4.2 Presentation by Mr Adrian Gropper

The most important technical task is to build global standards to respond to the separation of concerns (different businesses, interactions and services) which enable trust and innovation. Mr Gropper explained the separation of concerns, of which there are four. Standards organizations define the data representations with the related data model. The same or other SDOs define the consent form to support data sharing of these data. Developers are businesses which create a free/libre open source app that implements data acquisition and processing-based on the standards. A cooperative, non-profit, or for-profit entity hosts and processes data submitted by an individual. They participate in open, non-proprietary standards and development in order to protect their brand and avoid burdensome

regulations as they compete for customers. Auditors are independent of the three roles above (standards, developers and hosts). Auditors could be government agents or for-profit service providers. Policies that govern the four actors (standards organizations, developers, hosts and auditors) should be based on ethics and overall societal benefits. Consultants and system integrators compete to implement the standards for hosts and provide the requisite documentation of the system. In response to those concerns, he emphasized the need for common standards. Concerning standards, multiple parties must implement standards for debugging, and the proposed Gold Button may be a defined bundle of standards.

3.4.3 Presentation by Ms Hyo Young Lee

Data protection in the APEC region is characterized by a high level of diversity among APEC member economies and different ways of recognizing of the varied legal regimes governing data protection. The extant system allows for voluntary rules, reflecting the non-binding nature of the organization, instead of mandatory rules and minimum standards for personal data protection, which would promote global interoperability of privacy regimes. Key focus areas for the APEC Internet and Digital Economy Roadmap are developing digital infrastructure, promoting interoperability, achieving universal broadband access, developing holistic government policy for the Internet and the digital economy, promoting innovation and adopting enabling technologies and services, enhancing trust and security in the use of ICTs, facilitating the free flow of information and data for the development of the Internet and the digital economy, enhancing inclusivity on the Internet and in the broader digital economy, and facilitating an E-commerce and advancing cooperation on digital trade. Challenges include better utilizing the APEC CBPR system and introducing more APEC-certified accountability agents; there are just seven accountability agents in the APEC regions. Considering the number of APEC economies, more certification agencies will be necessary. Interoperability between CBPR and GDPR is necessary to encourage the spread of the digital economy. As the EU is vast market, if we enhance interoperability with the EU GDPR, we will have more business opportunities.

.

3.4.4 Designated Discussion

Mr Paul-Olivier argued that there are all different interventions concerning governance and the role of standards, and that there exists a process of convergence between different economies. It is definitely correct to mention the separation of concerns as presented by Mr Gropper, but Mr Paul-Olivier thinks that it should be driving the process of convergence between different actors around the world also more locally in the APEC region. Discussion opportunities are very important to adjust the differences of each actor. In this regard, progress has been made as people construct new forums or new entities that they can discuss and when they form structures that they can discuss. Also, even though we focus on data protection from an individual perspective, focusing on data access and processing is also important, as it is related to accountability.

Ms Viivi said that it is important to take into account the different values, abilities, and goals of people all around the work. Also, when we construct the framework for MyData, we have to consider that there are vulnerable groups who need special protection. When we talk about power of a human-centric approach of personal data, we have to keep in mind that all humans are not exactly the same. A human-centric view is to have interoperability.

4. Outcome & Recommendation

Below is a list of core findings of the PPD:

a. LifeSemantics, a PHR platform and digital health service provider, employs a business model based on gene data, EMR data and lifelog data with medical information, big data, AI, cloud computing blockchain technology.

b. NTT is a personal data bank provider that allows customers to manage personal data based on entrusted agreements on utilization of individuals' personal data provides data on behalf of the individuals to third parties in agreement with the instructions of the individuals or pre-specified conditions.

c. Meeco provides tools to access, control and create mutual value from personal data. It allows customers to securely store personal data, access it across all devices and automatically update data after editing. The firm provides trusted data ecosystems to develop B2B relationships for enterprises.

d. Christopher Lee of the MyData Korea hub addressed institutional challenges. Transparency and interoperability are key principles to hold while establishing institutions. Mr Lee emphasized cross-border collaboration as a starting point at which the APEC economies may begin sketching the roadmap for the implementation of MyData.

e. Adrian Gropper describe the technical challenges facing MyData. The most important technical task is to build global standards to respond to the separation of concerns which enable trust and innovation. He suggested a set of standards called the Gold Button.

f. Hyo Young Lee outlined tasks for cooperation to better utilize the APEC CBPR system. She argued that more APEC-certified accountability agents are necessary. Certification agents exist in just seven APEC regions; more are required. Also, interoperability between CBPR and GDPR is necessary to encourage the spread of the digital economy.

PART II. Research Paper

Directions for Promoting Data Utilization within APEC

1. Preface and Introduction

1.1 Rationale

□ **The breakneck growth of the digital economy**

○ *Defining the digital economy*

- The term “digital economy” was first coined in Tapscott (1996) as “...a new economy in which information assumes a digital form.” But there remains no consensus on what the term means and a number of different definitions exist

<Table 1> Competing definitions of Digital economy

Source	Definition
OECD (2012)	A market based on digital technology that facilitates trade in goods and services through electronic transactions
EC (2013)	An economy based on digital technology
Rouse (2016)	A global network of economic activity made possible by information technology; in short, an economy based on digital technology
UNCTAD (2017)	The application of internet-based digital technology to the production and trade of goods and services
APEC (2019)	The components of economic activity that utilize and depend upon digitized data and online platforms to facilitate trade in goods and services.

- Taken as a whole, the digital economy can be understood as playing a role in which, through the use of digital technology, it injects dynamism into the greater economy

○ *Size of the digital economy*

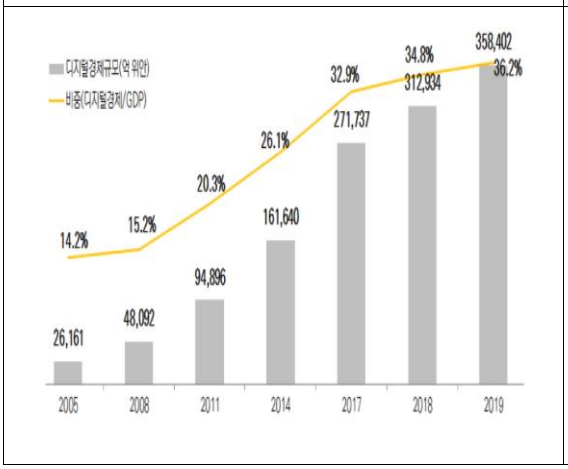
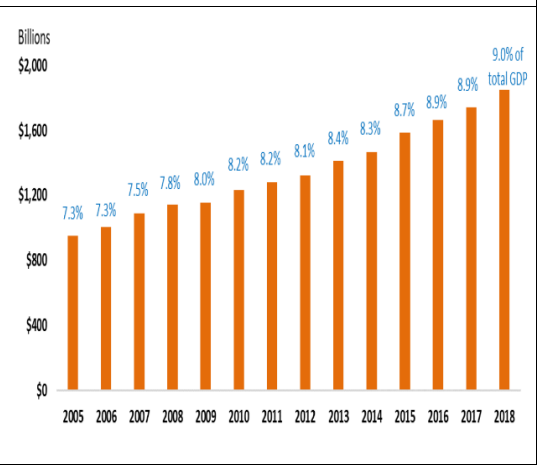
- That the digital economy is growing is a commonly-shared view, but as shown previously a singular opinion of what constitutes the digital economy is lacking.

- Of particular note is the fact that methods for measuring various aspects of the digital economy are still in their infancy. Thus to what degree the digital economy has expanded is another matter of divergent and varying perspectives

- Given the lack of measurement tools, the growth of the digital economy is inferred through fragmentary and partial statistics and observations of growth in related activities

- The digital economy of China was estimated to have exceeded 35% of Gross Domestic Product (GDP) in 2019. In the US, the digital economy was found to account for nine percent of GDP in 2018

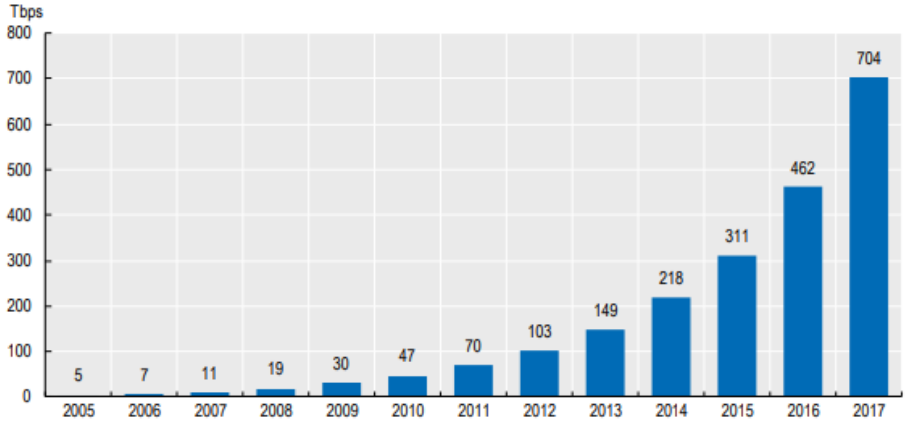
<Figure 1> Share of the digital economy in China and the US

China	US
	

Source: China Academy of Information and Communications Technology (www.caict.ac.cn), BEA (2020)
Note: In the left-hand graph, the yellow line refers to the digital economy's percentage share of GDP in China. The grey bars refer to the size of the digital economy, in units of 100,000,000 CNY (6.53 CNY = 1 USD). In 2019, the size of the digital economy measured in US dollars would have been roughly 5.4 trillion USD.

- Cross-border movement of data, which can be said to be the very essence of the digital economy, surpassed 704 terabytes per second (Tbps) in 2017.

<Figure 2> Cross-border data movement



Source: McKinsey Global Institute Analysis (2019)

□ **Clear growth trends in digital trade**

○ *Defining digital trade*

- Consensus on what constitutes digital trade is in the process of being formed. Generally, it is defined as the innovations that extend to production activities, including orders and deliveries, which have traditionally been measured

- It is appropriate to think of digital trade as a meta-concept that includes both e-commerce or e-business in defining the trade activities of the digital economy

<Figure 3> The concept of digital trade

Source: Authorial conceptualization

○ *Digital trade growth trends*

- There exist several notable efforts to measure the digital economy. The Organization for Economic Co-operation and Development (OECD) in 2014 released a key report entitled *Measuring the Digital Economy* (2014) which identified salient issues and proposed a set of relevant objectives; in 2017 it formed the Working Party on Measurement and Analysis of the Digital Economy research task force and launched its Going Digital Project

- As with measurements of the digital economy, statistics and data on digital trade point to an expansionary trend

- The United Nations Conference on Trade and Development (UNCTAD) in 2019 found that in 2018 at least 330,000,000 people had engaged in cross-border online trade; the COVID-19 pandemic has greatly accelerated this trend

<Figure 4> Online shopping trends

Source: UNCTAD (UNCTAD estimate of global e-commerce, 2018)

- The expansion of digital trade has led to an increase in the issuance of digital trade addenda for existing trade agreements and the drafting of separate digital trade agreements

□ **Data and technology are the heart of the digital economy**

○ *The digital economy and related digital technologies*

- The digital transformation is in full swing, spearheading sweeping changes across all elements of society. Two fundamental changes include the digitization of information and the digitalization of business practices through the use of digital technology

- Digital technologies include foundational networking and information technology technologies that make up the core infrastructure of the digital economy as well as more recent innovations. These include: artificial intelligence (AI), the Internet of Things (IoT), robots, 3D printing, big data, cloud computing, digital twin technology, virtual reality (VR), augmented reality (AR), blockchain and 5G

○ *Digital technology is based on data*

- Digital technologies are ultimately those that make use of the data continuously generated as the digital infrastructure develops

- Data is to today's industry as oil was to the industrial world of yesteryear; digital technology creates new value through the use of data

□ **Personal data protection is a key issue in data utilization**

○ *Data utilization issues requiring attention*

- Data creation and utilization underpin the growth of the digital economy, and are growing exponentially

- On the other hand, the legal and institutional environment surrounding personal data, a key element of all big data, can be an inhibiting factor with regards to the availability of data

- It is critical that ongoing privacy concerns be addressed and problems resolved in order to maximize the value of strategically-leveraged personal data

○ *Finding a balance between the protection and utilization of personal information is critical*

- There are doubts as to the effectiveness of the extant regulatory environment in protecting personal information

- It is difficult for individuals to understand how entities in possession of their private information (principally private firms, which dominate the information ecosystem) create, use and protect that data

- Overhauling the system governing the utilization and protection of personal data is a matter of the greatest urgency and a prerequisite for galvanizing the digital economy

2. Objectives

□ MyData, a balanced approach to the protection and utilization of personal data

○ Balancing privacy and usage of personal data: the MyData initiative

- A plan that makes possible the harmonization of privacy protection and balance is a precondition for the innervation and development of the digital economy

- The MyData initiative began with a novel, forward-thinking approach as a reaction to the existing system for protecting and utilizing personal information

○ Pursuing an information-ownership ecosystem centered around the individual

- MyData is a system designed to transform the current information ecosystem - which is centered around private enterprises -- to one focused on the individual as principal agent, while simultaneously pursuing the objective of protecting personal data even as it is being utilized

- The MyData system comprises an entirely new information substructure in which individuals exercise agency in every step of data processing. It does so by collecting, storing, sorting and utilizing the data of individuals possessing ownership over their own information

□ Implications carried by the potential applications and limitations of MyData

○ Potential applications of MyData

- Vitalizing the digital economy requires not only government-level strategies but cooperative, multilateral efforts on the global level

- With this in mind, in this report we seek out strategies for applying MyData at the transnational level through analyses of related systems being worked out and applied in major economies

○ The limits of MyData

- A lack of international agreement on digital economy and digital trade issues is also evident in discussions of MyData

- As mentioned previously, the successful introduction of the MyData framework faces several obstacles. Efforts must be made to understand surmount these, chief among which include resolving institutional and technical challenges hampering strengthened international cooperation

2. The Importance of Data and Associated Norms

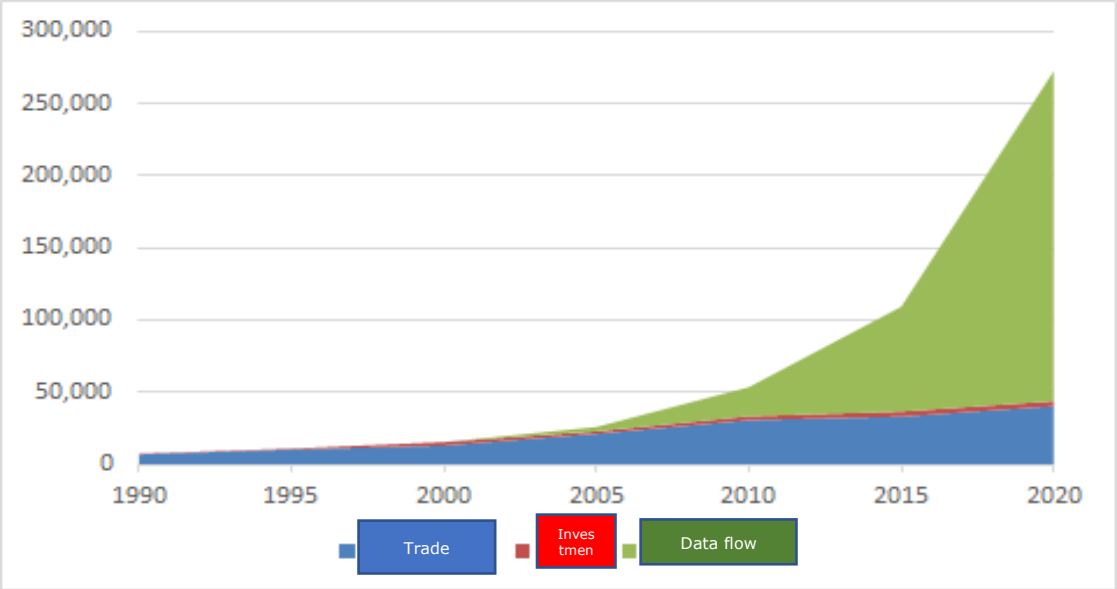
2.1 Definition and Status of Data Economy

□ **The digital economy**

○ *The importance of data in the digital economy*

- The expansion of the digital economy can be seen through the explosive growth of data flows.

<Figure 5> Changes in data flows over time



Source: Peterson Institute for International Economics (2018), “Can digital flows compensate for Lethargic trade and investment?”

- It is worth noting that as the digitization of information makes the generation of new and diverse business models commonplace, firms that do not make use of data face are likely to find themselves in a business environment in which their very survival is threatened

- Governments and industries alike are actively promoting data-related investments and policies

<Table 2> Data economy development policies in core regions

Region	Policy
US	The U.S. regime for protecting personal data encompasses both state-level legislation (the most recent and comprehensive being California's 2018 Consumer Privacy Act) as well as sector-specific Federal legislation (e.g. privacy provisions of the 1996 Health Insurance Portability and Accountability Act, and the Financial Services Modernization Act of 1999.). In addition, the 1998 Children's Online Privacy Protection Act (COPPA), 15 U.S. Code § 6501-6505, prescribes specific protections governing the collection and dissemination of data of minors.[1] Separately, the Federal Trade Commission actively enforces against breaches of privacy protections based on Section 5 of the Federal Trade Commission Act, which generally proscribes unfair and deceptive practices in the commercial sphere. Outside the commercial sphere, the 1974 Privacy Act protects personal data held by the Federal government, which also has state-level analogues. Additionally, the United States has in recent years enacted the 2020 Federal Data Strategy and the American AI Initiative. However, the American AI Initiative is subject to changes by the new U.S. Administration.
EU	2017 data economy development strategy; 2018 General Data Protection Regulation
Japan	2017 future investment strategy; 2019 comprehensive AI strategy
China	Outline of National Action for Facilitating Big Data Industry Development plan promulgated in 2015; big data industrial development vision and next-generation AI development plans announced in 2017

○ *Defining the data economy*

- The data economy is an economic structure in which data is an essential production factor in economic activity and plays a role in facilitating the efficient allocation of resources

- The standard operating procedure for modern corporations is to minimize production costs through mass production, secure cost competitiveness with low-wage labor and strengthen global production networks. But it is also important to seek out and identify advances driven by data-based technologies

- Eventually, developments in data-driven digital technologies will completely remake the way business is now conducted

□ **The current state of the data economy**

○ *The data utilization segment*

- Data in and of itself is of limited value. Rather, it is services that make use of data that create vast areas of added value

<Figure 6> Makeup of the EU's data economy in 2017

Source: *Frontier Technology Quarterly* (2019), "Data Economy: Radical transformation or dystopia?

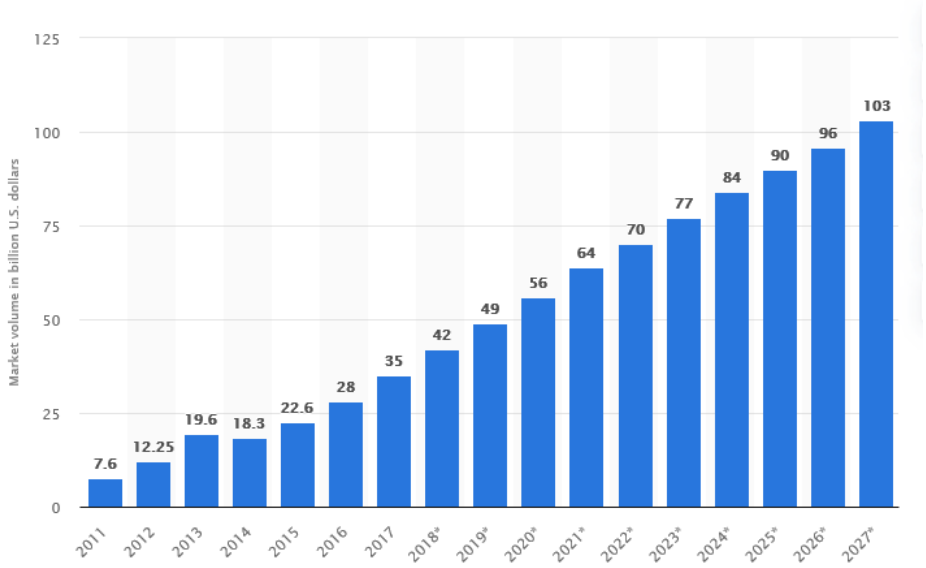
- As seen above, the data market itself accounted for just 19% of the total economic impact of data in 2017; the proportions of products and services made possible by data or those that use data are much higher

○ *The scale of the data economy*

- The above figure shows that the data economy in 2017 accounted for 2% of the EU's GDP. It is possible to see that the actual scale and economic impact of the data economy is not accurately reflected in this figure

- In fact, looking at 2016 data in the American market, the top 25 technologies companies had a market value of six trillion USD, for an aggregate market capitalization rate of 20%. Most of these firms have data-driven businesses at their core

<Figure 7> Current and projected value of the global big-data market



Source: Statista : (https://www.statista.com/statistics/254266/global-big-data-market-forecast/)

- The rate of growth in the size of the data market has been meteoric over the last decade

- Accenture found in 2016 that 75% of all data produced was related to personal information. This reflects the importance of utilizing personal information in growing the digital economy

<Figure 8> Average annual rate of data growth in major regions, 2010-2018

Source: *The Economist*

2.2 Key Points of Contention in Data-Related Norms

- Explosive growth of data is driving the digital economy and digital trade, but challenges remain

- Regulations on data collection and use have direct impacts on the growth of the digital economy

- For instance, tough new regulations on the use of personal information are coming into force, and it is critical to find ways of dealing with them

□ **Notable regulations**

○ *Regulations on cross-border data movement*

- Corporations seek market access and pursue efficiencies through the free movement of data, but domestic regulators often impose measures to hinder this flow with the goal of promoting personal data privacy and security or to support local businesses

- Typical policies include localization measures that require data to be stored in specified jurisdictions or server farms/computing facilities be located where data is originally generated

- These measures and others throttle transnational movement of data. They thus comprise a significant barrier to companies that use data to maximize operational efficiency or provide valuable services to overseas customers

○ *Cybersecurity and data protection*

- Cooperation on cybersecurity between APEC economies can help facilitate the cross-border flow of data in a responsible manner and highlight that data flows are a key element to cybersecurity.

- Compromised cybersecurity systems can threaten the entire global IT ecosystem, and increasingly mobile data flows increase the risk that health, financial or other sensitive information could become exposed

2.3 Data Regulations and Trade Policies in Major Economies

□ **EU regulations and policies**

○ *The main law regulating data use in the EU is the aforementioned General Data Protection Regulation (GDPR)*

- The law went into effect on 25 May 2018, and applies directly to all EU member economies

- The GDPR includes a provision introducing the concept of pseudonymous information, while also stipulating that personal credit information can be used for statistical and research-related purposes. The law also facilitates cross-border data flows following standards determined by Brussels.

- At the same time, the GDPR law adopts high standards of accountability in personal data processing, extending the right of information ownership to individuals and in doing so enabling them to control their own data (such as the right to be forgotten). It also requires companies to hire dedicated data security staff, or Data Protection Officers (DPO) in the language of the law

- Serious violation of the law's provisions results in a hefty fine of four percent of the previous years' global revenues (or 20 million EUR). This applies not only to companies operating inside the bloc and even economies outside the EU that handle the personal information of EU citizens

○ *The digital single market (DSU) of the EU*

- EU policy planners seek to harmonize the digital markets of bloc members in pursuit of the following three objectives:

- (i) Enhance online access to digital goods and services through cross-border online activity, (ii) support fair competition and boost investment with a fast, secure infrastructure and regulatory regime and (iii) guarantee the digital economy serves as an engine for growth through investment in infrastructure, research and innovation and the formation of an inclusive society of highly-skilled citizens

- In sum, the EU is promoting the unification of digital markets to overcome the limitations of the smaller markets of its member economies and secure innovative growth

- However, by imposing restrictions on the collection and analysis of information and enforcing strict rules on security and privacy through the GDPR, the EU's policy stance toward the cross-border movement of data can be seen as passive.

□ **US regulations and policies**

- In general, US policies support the openness, interoperability, security and reliability of the internet, which includes the free movement of data

- American digital firms have voiced concerns that the increasing number of technological regulations and domestic standards, which take together constitute barriers to digital trade, could hamstring business in the global digital market and chip away at America's leadership position in technology

- In sum, American policy objectives aim to balance privacy and economic interests without sacrificing either

- Whereas the US also promotes a digital trade policy that focuses on monitoring all digital trade restrictions and removing those restrictions where appropriate to remove all digital trade barriers where appropriate through US-led free trade agreements (FTA) or in multilateral World Trade Organization (WTO) negotiations. This is being done primarily to reduce barriers to businesses, including small- and medium-size businesses, that affect their ability to export their services and enter foreign markets.

- The US has in fact made efforts to ensure that its FTAs with other economies reflect its digital trade policies. The results of these efforts differ by a matter of degrees, but are nonetheless evident in the Korea-US FTA, the Trans Pacific Partnership agreements, the US-Mexico-Canada agreement and the US-Japan digital trade agreement.

2.4 Summary of Main Points

□ **Global governance is not keeping up with the growth of the digital economy**

- The digital economy, based on data and digital technologies, is poised to grow even more rapidly going forward

- But from a global perspective, the formation of norms and rules related to data and the digital economy lags far behind, complementary in most cases only to traditional industries and trade in those industries' goods and services.

□ **Measures for personal data protection and utilization are necessary**

- Amid explosive growth in the volumes of data produced the importance of personal data is increasingly magnified. Given the variety of stringent domestic regulatory schemes related to the use of personal data, there exists a need for a personal information utilization system in which these regulations are consolidated

- Recently a number of economies and non-profits have held dialogues on the MyData system, acknowledging it as a way to achieve both data utilization and the protection of personal information

3. The MyData Project

3.1 Definition and Background of MyData

□ **The definition of MyData**

○ *What is MyData?*

- MyData is known by various terms, including the Personal Data Economy, Self-data, Vendor Relationship Management and The Internet of Me

- At its core, MyData is an open and decentralized data management and utilization ecosystem built around data subjects, the individuals whose data is being used, and the idea that those individuals should ultimately have control over their own information

- MyData makes it possible to pursue an approach that balances the protection and utilization of personal data

○ *How select economies define MyData*

- Korea: The Committee on the Fourth Industrial Revolution provides the following definition for MyData: MyData aims to transform the existing data utilization system into one that revolves around the data subjects, by allowing those individuals to obtain and either directly use their own data or provide it to a third party

- EU: The DECODE project exhibits some similarities with Korean regulations. DECODE is “a practical system that allows data subjects to determine how their data is managed and gives them the ability to make it available to third parties based on their needs.”

- *Finland:* The Ministry of Transport and Communications authored a white paper on MyData, holding it up as a Nordic Model for personal data management. Specifically, it defines MyData as an approach to building an open personal information ecosystem applicable to all industries and not limited to specific fields such as health care or finance. The report also notes that MyData could surmount the lock-in effect resulting from a small number of data aggregators controlling so much information by guaranteeing the interoperability and portability of personal data. It identifies MyData as an effective personal data control and management system based on the existing distributed storage environment

- *US:* There exist no standardized regulations explicitly concerning MyData, but the federal government has promoted (through the Smart Disclosure initiative) the ability for citizens to easily download their publicly-held health, energy, education and solar-energy-related information. This project is often referred to as the “Blue Button” project, owing to the fact that in the case of medical information, individuals can download their data by clicking on a blue button.

- At private-sector organizations known as Personal Information Management Services Communities, trust and confidence, self-determination and maximizing the collective benefits of personal data are among the six basic principles proposed for realizing the core values of MyData

<Table 3> PIMS communities’ six basic principles of MyData

Principle	Subject matter
Human-centric control of personal data	Make it so that the individuals whose information is being used understand personal data protection policies and guarantee their right to consent to their data being shared or to recant that consent
The data subject (individual) as the point of integration	Ensure that individuals become the hub of the information ecosystem
Individual empowerment	Allow individuals to be able to control how their personal data is managed, and provide them with the means (technical or otherwise) to do so
Portability	Make it possible so that individuals can freely and directly download their data and transmit it to third parties. The data provided must be structured, universally compatible and machine-readable
Transparency and accountability	Organizations using individuals’ personal information must obtain those individuals’ advance consent in advance, notifying them of the purpose for collecting and using their information and where it is to be used. Individuals are to be able to ascertain the status of their information as it is being processed and submit relevant inquiries
Interoperability	In order to lubricate the flow of information and prevent lock-in effects, it is critical to demand that common practices and standards be used in the broader personal data infrastructure (such as open APIs) so that individuals retain control over their data and the ability to move and repurpose it

Source: Korea Data Agency (K-Data) (2018, data industry white paper)

□ **MyData background**

○ *The MyData project has its origins in the development of the Open Data movement*

- The idea that free access to and disclosure of data would enhance is usefulness originated reports of the US National Research Council dating back to 1995

- Internet experts and advocates of open government gathered in Sebastopol, California (outside San Francisco) in 2007. They urged presidential candidates to pledge via their campaign platforms to adopt an open public data initiative that defines public data as a public good and applies open source principles

- In 2009, the Obama administration proposed an open government initiative incorporating the principles of transparency, participation and collaboration

- Despite continued emphasis on the public nature of data, there remain factors obstructing the availability and interoperability of data

- Threads connect the formal intent of MyData (which aims to empower individuals to be able to use, repurpose and distribute their own data) with the Open Data movement, which advocates the need for anyone to be able to use, re-use and circulate data

- A salient difference between MyData and the Open Data movement lie in the fact that MyData is primarily concerned with personal information

○ *The environment necessary for promoting MyData*

- Despite dazzling growth in the amount of data produced, the dominance in the data market of a small number of information holders is a factor limiting data universality by hobbling inter-firm data interoperability and mobility

- A trend has emerged in which individuals and businesses alike have increasingly opted to use only a small handful of large, well-established online platforms and operators in possession of data. This in some cases disrupts the introduction of innovative new data-based products and services

- There are doubts as to whether the few proprietary information holders will actively work to actively provide an alternative to personal data protection

- The Max Schrems case highlights global firms' continued violations of individuals' personal information and related issues. In 2011, Facebook — one of the major proprietary information holders — was found to have moved European users' personal data to servers overseas

- Furthermore, the global legal vacuum in the realm of personal data severely handicaps efforts at protecting it

- Some economies have come to agreements on matters of digital technology and data. But as of yet there exist no rules or norms with which to frame a global consensus, and discrepancies in the data environments of individual economies greatly limit negotiations

- MyData is a system that aims to harmonize the protection and utilization of personal information in the current environment

3.2 Guiding Principles

□ **The MyData architecture**

○ *Main components*

- The architecture of a traditional personal data processing mechanism consists of three core components: the data subjects (individuals), the data holders and the data users that apply the data to various ends

- The subject of the data is the individual who produced the personal information in the first place. The data holders are the organizations or individuals in possession of the data. The data users are individuals or organizations that provide services based on their processing of the data

* To illustrate, take the following example. In financial transactions, individuals withdrawing money or taking out loans would generate data and are data subjects. Financial institutions that record and store that information produced in the course of those financial transactions would be the data holders. And finance outfits — say, for example, credit card companies — that provide financial services to individuals making use of their data are the data users. In some cases, data holders and users may be the same organization or individual

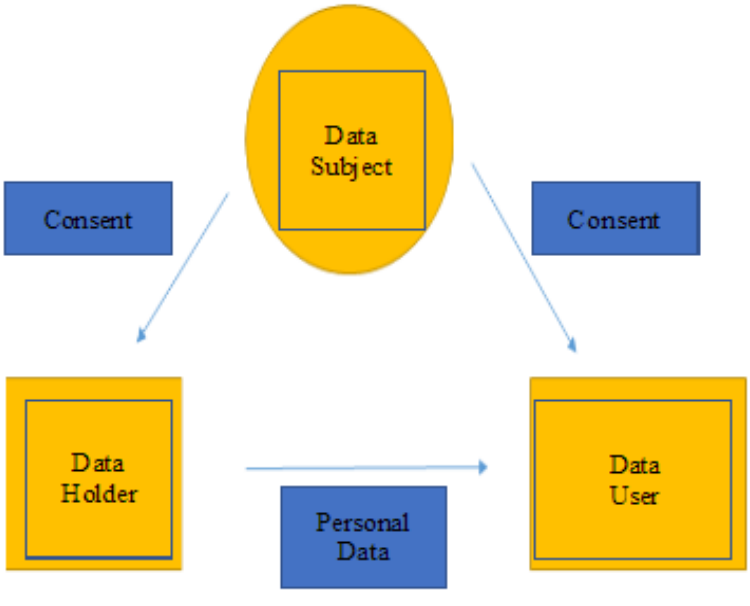
- The MyData system is differentiated from the traditional data ecosystem described above in that it features MyData operators, which are to play new roles in the data ecosystem

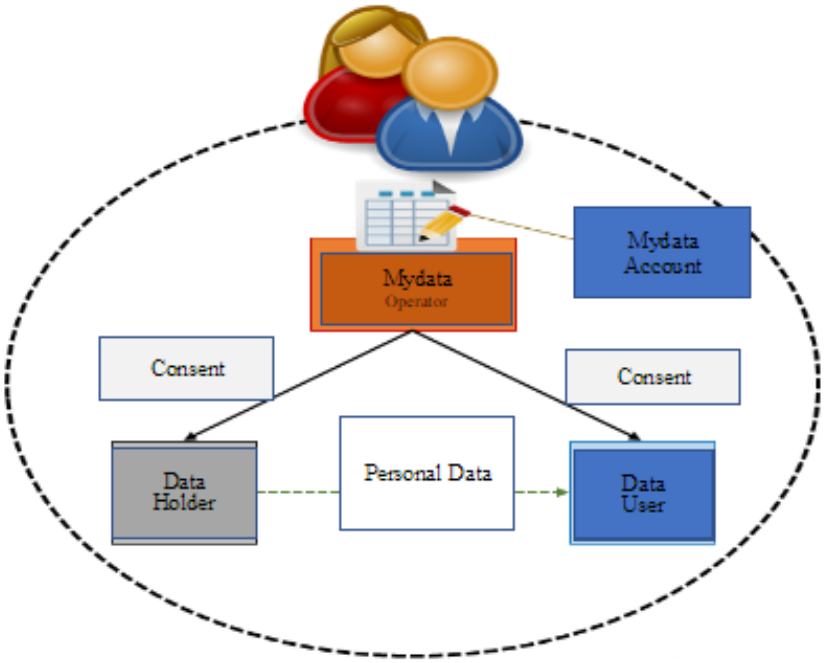
<Table 4> Roles and functions in the MyData ecosystem

Role	Function
Data subject	Data subjects are the individuals whose personal information comprises the data that flows throughout the ecosystem, and in the MyData ecosystem have ultimate authority over how their data is used
Data holder	Data holders are the government agencies, financial and medical institutions and telecommunications firms that possess raw and unprocessed data generated from the activities of individuals
MyData operator	MyData operators provide MyData accounts, which enable individuals (the data subjects) to manage their own personal information. This has the effect of strengthening the efficiency of data protection and s dynamic data utilization
Data users	Using personal data provided to them, data users are entities that process data to provide services. Any given entity could be both a data user and a data holder.

- MyData operators may play a variety of roles depending on the MyData model employed by any given entity, but in general operators must support the creation of a MyData account, through which data subjects can manage how their information is being processed across the board.

<Figure 9> Traditional data systems vs. the MyData system

Layout of a traditional data ecosystem	

Layout of the MyData ecosystem	

Source: MyData international cooperation promotional directives

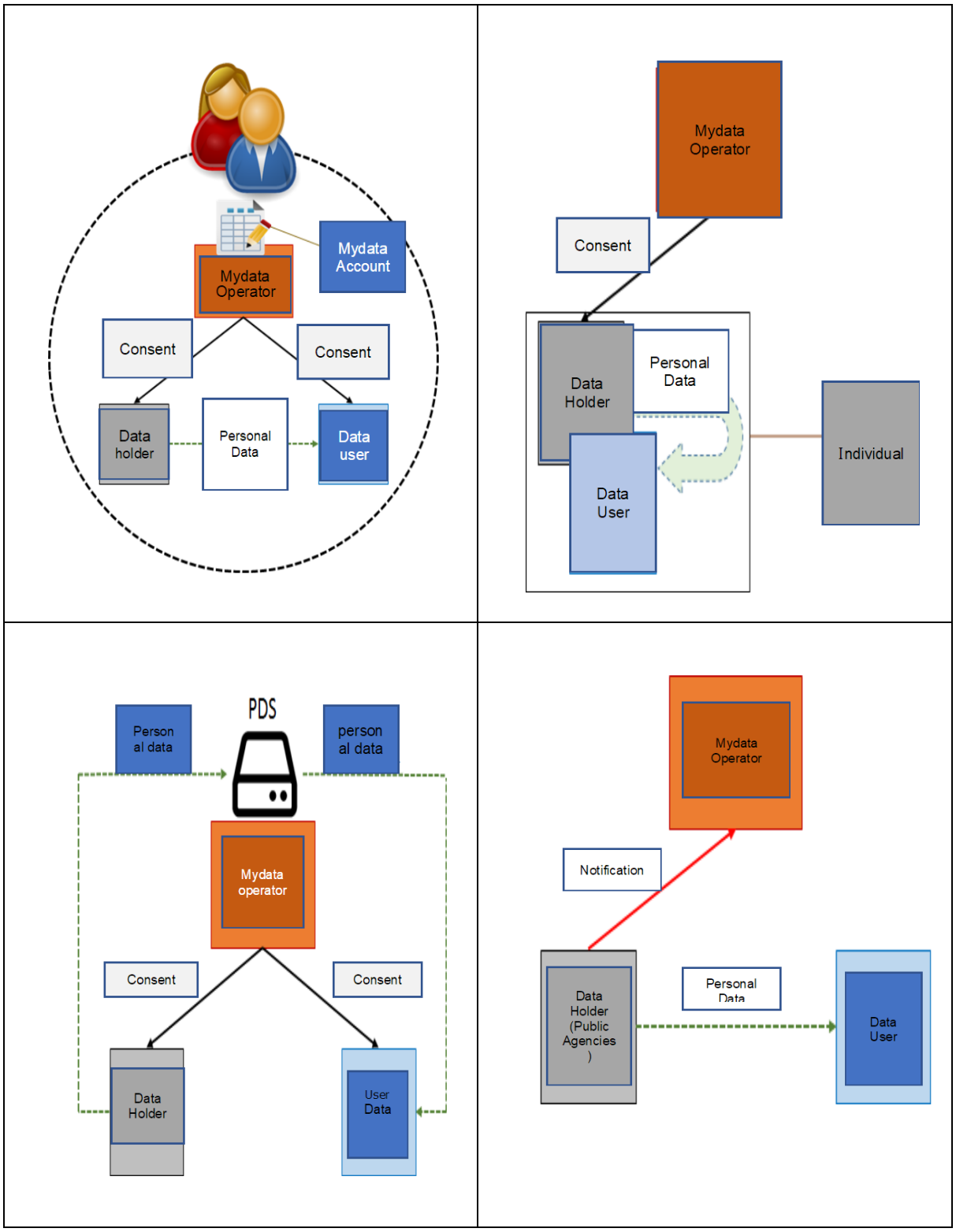
○ *The architecture of MyData according to data processing method*

- The MyData system can work in four ways that correspond with the directions of personal information flows and the nature of the data subject's consent. The methods by which the system can work are illustrated in the figure below and explained in detail.

- The following numbers correspond with the numbers of the boxes in the above figure. 1) For data users to use personal data, both the data holder and data users must obtain consent from the MyData account holder via the MyData operator. 2) For use other than the original verification of the data holder, the processing of personal data is limited to the data holder 3) Personal data stored by on the servers of personal data services (PDS) is linked to MyData operators 4) In case the data holder is a public institution, there is a special form of data processing that does not require direct consent from the data subject

- There are various workable models for the MyData system, but the key feature they all share common is that the individual — the data subject — is in control over his or her own information.

<Figure 10> The structure of the MyData system by data processing method



Source: Excerpted from MyData international cooperation promotional directives

□ **Operating principles of MyData**

- The presence of MyData operators distinguishes the MyData ecosystem from existing personal data systems

○ *The role of MyData operators*

- The main role of MyData operators is to provide a platform for managing personal information that functions as a relief valve

- This platform takes the form of a MyData account, through which data subjects (individuals) can exercise control and decision-making authority over their information

- MyData services provide transparency, trustworthiness, control and value

<Table 5> Key characteristics of MyData services

Trait	Explanation
Transparency	Disclosure of data collection and utilization activities to verify that personal information of the data subject (individual) has not been utilized by data holders (firms)
Trustworthiness	In the process of utilizing personal information and providing services, MyData operators are a point of trust and reliability
Control	Individuals exercise control over their data by requiring consent before providing information to data users
Value	Includes the individual in the revenue model and the provision of information is compensated

Source: K-data (2020), MyData information handbook

- MyData also functions as a professional intermediary in transactions involving personal information. It can systematically perform tasks that individuals themselves are incapable of doing in the current personal information ecosystem, enabling individuals to receive superior service for their data

- Put another way, when a data user requests a data subject for permission to use data, MyData operators determine and relay to the data subject how the requested data is to be used, providing a sound basis upon which the data subject can judge whether or not to consent to the use of his or her data

- Thus, MyData operators serve not only as an approval management system through which data subjects (individuals) can consent to the provision and/or use of their information, but also as an interface through which data subjects and data users can communicate and interact

<Table 6> Functions of MyData operators

<table>
<tr><td colspan="3">Locating Personal Data holders and Users,
Analysis of data holders' and data users' profiles
Concierge service for buying/selling personal information,
Provision of personal data service (PDS)
Data processing and conversion</td><td>Optional
Functions</td></tr>
<tr><td>Consent Management</td><td>Service Registry</td><td>Account Provision</td><td rowspan="2">Obligatory
Functions</td></tr>
<tr><td colspan="3">User Interface (UI)</td></tr>
</table>

○ *Core operating principles of MyData*

- It is easy to grasp the operating principles of the MyData system through a comparison with the structure of the existing personal information ecosystem and principles

- (Convenience) As visually depicted in the left-hand portion of Figure 9, the current personal data ecosystem is comprised of data subjects, data holders and data users. In this system, data users must request data holders to provide them with personal information in order to themselves utilize data and provide services based on that data. In this process, the data subject must grant consent simultaneously to the data holder and data user.

- Whereas in the MyData ecosystem, consent flows between the individual (the data subject) and the MyData provider

- To employ an example, say that one individual (the data subject) wants to use the services provided by ten different data users. Under the current personal data regime, individuals must provide consent for every service, to the data holders and data users — that is, he or she must issue consent 10 times over. But in the MyData ecosystem, the data subject grants consent just once, to the MyData operator

- (Consistency of management) Since consent must be constantly provided to data users in the current personal information ecosystem, neither the format nor content of the data remain consistent over time. This makes it difficult for individuals to manage their consent history

- Whereas on the other hand, in the MyData ecosystem, it is possible for individuals to manage their consent history in an organized format through whatever method MyData operators might choose

- In addition, it is much easier to retract consent using MyData, as it can be done without contacting each data user individually

3.3 Basic Features of the MyData Service

□ **Consent management**

○ *What is included in the provision of consent*

- Providing consent allows for the collection, use and application of personal data and certifies acknowledgement of both the scope of the data and its recipient

- Consent forms should be abbreviated (for example, a title or short description), cogent, concise and written in language that is easy understand

- Summarizing the content of agreements in an easy-to-read format makes it possible for data subjects (individuals) to provide specific, individualized consent, based on a more complete understanding of what they have agreed to

○ *Consent management*

- Through an account provided by a MyData operator, individuals must be able to provide and retract consent and reauthorize consent in real-time

- In the United Kingdom, the re:consent platform allows provides a service that allows individuals to quickly and easily review or modify consent history for sites such as Google or Facebook

- MyData operators must provide individuals with a platform to review and understand to whom and what they have authorized consent at a glance. Such a platform must also provide users with the ability to provide and retract consent in a similarly user-friendly manner

□ **Downloading personal data**

- Downloading personal data refers to the act of MyData users saving their personal data in both machine-readable and unstructured human-readable formats for the purposes of storage, review or reuse

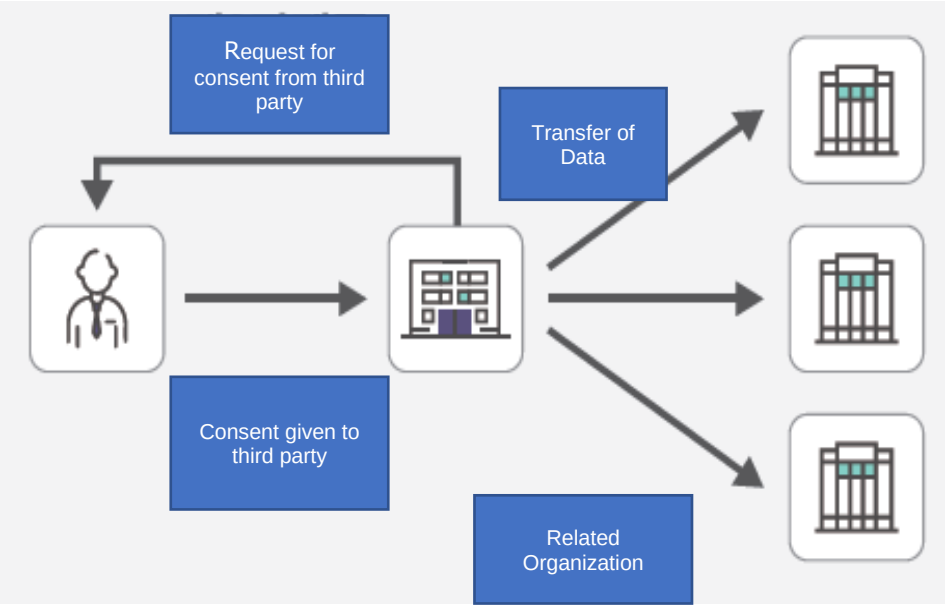
- Users of MyData services must be able to select the scope, date range and type of personal data they want to download, as well as how they would prefer to receive the data. For example, by saving it directly to a device or receiving via e-mail or a messenger service
- The functionality described above, which MyData operators provide, mimics similar services offered by existing platforms. For example, Amazon allows for users to download and store up their purchase histories (up to three years' worth) in the CSV file format; Google users can download their data through their Google accounts

□ **Selective sharing**

- Data holders (individuals) designate which data users (third parties) are to receive their data. The request is transmitted to the MyData operators' platform, which in turn transfers the relevant data

- This differs from the method currently in widespread practice, in which data holders obtain permission from individuals to provide data to third parties. Under selective sharing, individuals themselves determine who receives their data

<Figure 11> How information is provided to data users (third parties)



Source: K-Data (2020), MyData service information pamphlet

- The Green Button project in the US is a prime example of selective sharing of energy data

4. Current State of MyData and Challenges in Facilitating Global Adoption

4.1. MyData Policies in major economies

1) US

○ *Public sector Open Data policy*

- In 2011, the Obama administration established a task force under the National Science and Technology council to promote the productive use of public data; in that year it also promulgated the Open Government National Action Plan

- In 2013, the federal government issued an order designed to facilitate the disclosure of federally-held data in a machine readable format titled “Making Open and Machine Readable the New Default for Government Information”, a notable accomplishment in the movement toward Smart Disclosure

○ *Smart Disclosure*

- Smart Disclosure refers to the release of federally-held personal information to data subjects (individuals). Data subjects are able to download their personal data in four different fields (health care, energy, education and solar power) by clicking buttons with colours corresponding to one of those fields. They are then able to share that information with third parties

- This approach is an example of a government data holder promoting a MyData-adjacent system using publicly-held private data

- It is also a model for a data ecosystem in which data subjects (individuals) are empowered to grant the use of their government-held personal information to information services of their own accord through the MyData system

- While the architecture of the Smart Disclosure program lacks a MyData operator, an basic component of the MyData ecosystem, by providing data management accounts and a user interface (UI), it can still be viewed as a MyData system

○ *How Smart Disclosure was used*

- Smart Disclosure promoted the development and application of a variety of value-added services by conferring the right to access and move information

- The Health Insurance Portability and Accountability Act and the Family Educational Rights and Privacy Act provided the legal basis for the utilization of personal information in the fields of medical care and education, respectively

- In 2010, the Blue Button project launched its inaugural medical data initiative targeting military veterans. The service enabled ex-service members to transfer medical and health records to organizations or individuals of their choosing through the click of a button online

- In order to improve the interoperability of data flows between data holders, data subjects (individuals/patients) and service providers (medical professionals), common standards for data architecture, transfer protocols and APIs were provided, and the OAuth 2.0 system was used to manage data subjects' approval

- There are a number of Smart Disclosure pilot programs underway in non-medical fields. In the energy sector, a major California gas and electricity provider went forward with implementing the Green Button project. In the solar power sector, the Orange Button project is moving forward following demand from industry

2) United Kingdom

- In the UK, a private sector platform called The Hub of All Things (HAT) and the midata project at the Department for Business, Innovation & Skills are both MyData initiatives

- The midata program was launched in 2011 and marketed as the Better Choice, Better Deal initiative. It is designed to provide corporate data on consumers to the consumers themselves, and in doing so strengthen consumer sovereignty in consumers' right to self-determination of personal information. It does so through voluntary programs based on government-business-consumer partnerships in key sectors of household spending, such as energy, telecommunications and credit cards

- Working in partnership with 26 organizations holding private data, the midata initiative returns private information to individuals in a secure and portable format. midata partners provide personal data in CSV format, which can be downloaded by data subjects (individuals) and shared with designated third parties as they wish

- In addition, a revision to the Enterprise and Regulatory Reform Act made it possible for data subjects to download a record of how their information was used in a digital format. The amendment to the Act also included provisions for the establishment of MyDex, a platform for the management and sharing

of personal information that enables users to store, analyze and share information with third-party service providers

- The Open Banking policy of the UK's Competition and Market Authority, designed to promote competition in the financial sector, serves as an application example. The updated Payment Services Regulations 2017 mandated that bank account information be made available to fintech firms. To comply, 25 major banks delivered information on balances and transaction histories to fintech firms through Open API

3) France

○ *Public sector policies*

- In France, government think tank Foundation Internet Nouvelle Generation (FING) and partner agencies introduced the concept of "Self Data" in 2013, going on to implement an extension project called MesInfos

- MesInfos was established in order to restore consumer confidence by better balancing corporate-consumer rights. It aimed to return personal information to data subjects (customers) held by private firms. In seeking ways to allow customers to take advantage of their own personal information, MesInfos sought to ensure a fairer distribution between companies and individuals of the benefits generated by personal information

- Relatedly, the personal information provided to do consumers, and specifically consumption data (receipts, invoices, and other records) contains a wide variety of real-life information. This data includes financial, energy, communications, web browsing, medical educational, employment and administrative information.

○ *Pilot programs*

- As part of the larger MesInfos project, the French government launched a pilot program dubbed Cozy Cloud in 2016, designed to apply the Self Data initiative in the real world

- The Cozy Cloud program comprises a mobile application that enables data subjects to empowers data subjects with consolidated control over their personal information in a number of fields

- The nearly 3,000 program participants were able to review and manage their personal consumer data held by firms in the insurance, energy, telecommunications sectors (and others)

- Other pilot programs include the My Health, My Data project in the medical field and the Rainbow Project, which is laying the groundwork for establishing personal data portability rights

- French follow-up measures to the EU's adoption of the GDPR in October of 2016 included the adoption of the Digital Republic Law, which introduces the concept of public interest data. This is data that is held by private entities but for which public disclosure is in the public interest. This kind of data might aid in preventing monopolistic market behaviour, ensuring the effective implementation of public policy and promoting scientific research and economic development

- The text of Digital Republic Act defines wide range of data produced by private entities as public interest data and requires that this data be made publicly available

- Private entities in possession of data newly-defined as public interest data are now obligated to provide this data to government agencies. Introducing the concept of public interest data reflects an attempt at getting around limitations on the utilization of personal information stipulated by the GDPR

4) Finland

- Finland in 2013 launched its Open Data policy initiative, through which personal information managed by the government and private firms is made available to individuals for their own management and/or use

- The specific measures of the Open Data policy are implemented by a number of agencies under the leadership of Ministry of Finance. The main objectives of the policy are to make open and better utilize public sector information and enhance information processing abilities. In short: the policy seeks to raise public sector productivity and promote efficient use of information in the private sector

- There are three key considerations in the practical applications of the policy. First, key public data must be machine-readable, free, and open to the public with easy-to-understand usage conditions. Second, the distribution and utilization of public data should be promoted through the application of a common model for the production, management and service of important public information. Third, a domestic data processing program is to be administered to improve the level of data processing technology

- Finland also runs a program to stimulate major innovations in the personal data ecosystem and the opening of public data. The fruit of this endeavour is the MyData initiative, launched in 2014 with support from the Ministry of Transport and Communications

- The Nordic Model informs the human-centric management and procedures of the MyData system, which was adopted as a pan-governmental policy item in 2015. Under the leadership of the Finnish government, the European Commission held a PIMS roundtable on personal information management systems and is committed to spreading MyData to the private sector
- The MyData Alliance focuses efforts on improving services, infrastructure and interoperability through the MyData system

- There are currently pilot services based on MyData in operation across Finland in a number of sectors, including transportation, medical care and finance, supported by government agencies and research organizations. No economy is more actively pursuing implementation of MyData initiatives

- The Finnish Population Center provides a digital platform (Suomi.fi) and the Ministry of Transport and Communications makes relevant information available to the public to support the development of traffic safety systems and eco-friendly transportation solutions

- The Finnish Institute for Health and Welfare (THL), a research agency under the Ministry of Social Affairs and Health, released a trove of information to the public with the goal of provoking innovations in health-related technologies. Meanwhile, Nordea — Northern Europe's largest financial services group — is promoting open banking in the form of personal financial data management services

<Table 7> MyData trends in major economies

Economy	US	England	France	Finland
Project	Smart Disclosure	Midata	MesInfo	MyData
Goals	Help consumers make informed decisions using data	Strengthen consumer sovereignty and support improved decision-making capacity	Make the benefits of personal data monopolized by firms available to the public	Human-centric privacy control and increasing the value of data \
Benefits	Increase consumer utility	Economic stimulation	Benefits of personal data use socialized	Growth of data economy
System	Specialized agencies (OMB, NIST) under general branches of cabinet (VA,	Public-private partnership of government (BEIS) and private sector entities (steering and action committees)	Private sector coalition (FING & Cap Digital) responsible for implementation	Public agencies entirely responsible for policy implementation (Ministry of Transport and

	Energy) responsible for policy implementation)	responsible for implementation		Communications, LVM
Private sector contributions	Greenbutton Alliance in energy, Bluebutton Alliance in medicine	26-member Steering and Action Committee, comprising regulatory agencies, consumer groups and firms from across industry	Corporate participation in pilot programs includes data providers, insurers, banks, six telecoms and two service support firms	The MyData Alliance, comprising 40 firms and gov't agencies including the Ministry of Transport and Communications
Associated policies	Open Government National Action Plan (2011)	Steering and Action Committee made up of representatives from public regulators, consumer groups and 26 firms from all fields	None	The Digital Business Growth Strategy (2015); The Data Business Activation Plan (2016)
Legal framework	Executive Orders mandate that public and/or private data be made available upon request	Better Choice, Better Deals(2011) Open data Initiative(20112) Open Data Strategy (2014)	EU GDPR/PSD2, Digital Republic Act (includes a clause on service data mobility)	EU GDPR/PSD2, Finland itself has no specific legal framework
Standards	Standards to be set and interoperability secured through public-private partnerships	Enterprise and Regulatory Reform Act of 2013 (Mandates for financial, energy and communications sectors)	Rainbow Button, a GDPR-supported data transfer and sharing framework project	Trust Network Framework, infrastructure that guarantees standards and interoperability
Applicable fields	Health, energy, education, others	Energy, finance, telecommunications	Medicine, energy, personal use, everyday life	Health

4.2 Application of MyData in Private Sector

□ Mint (Money Intelligence, mint.com)

○ *Scope of business*

- Mint was established in 2007 as a credit information service; acquired by Intuit in 2009 for 1.7 billion USD

- Mint provides a platform for individuals that makes integrated financial management through a single interface possible by automatically retrieving users' personal financial data including bank account, credit card and investment information

○ *Business methods*

- When a user links a bank, credit card or other financial account to Mint, the program retrieves all available transaction data from those accounts and organizes it for the user's consumption in an intuitive manner (using statistics and graphs, for example), allowing for users to analyze their consumption patterns

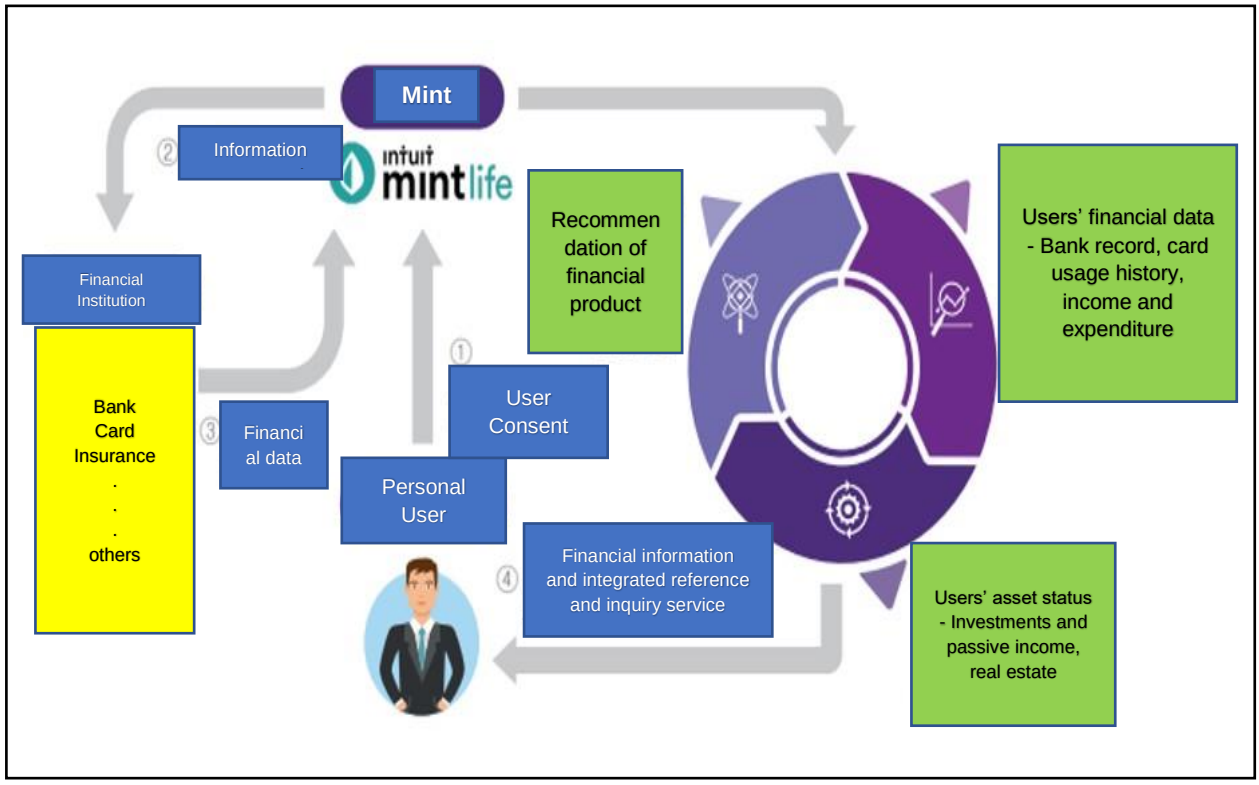
- It is possible for users to link and manage bank, card, insurance, securities, stocks and real estate through Mint

- It is worth noting that Mint employs an automated classification system based on US standard business classification. The system provides an automatic classification for at least 90 percent of classifiable items, maximizing the scope of automation

- The automated service expedites the once-gruelling task of classifying daily consumption records and dramatically enhances user convenience

- Thus, users are, by agreeing consenting to the use of their own personal financial data, able to view all of their personal finance information on single platform, allowing for a most optimal understanding of their current financial situation

<Figure 12> The structure of the Mint personal credit inquiry service



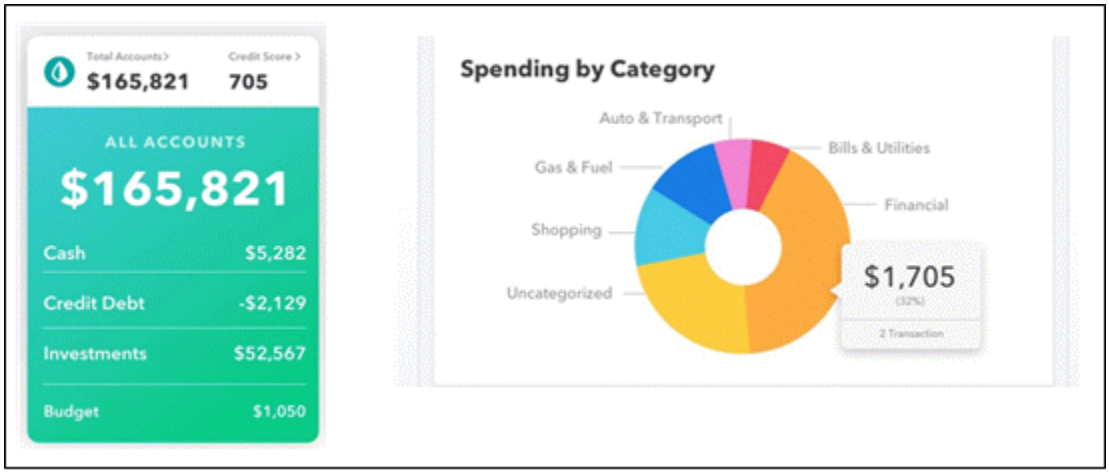
Source: KPMG Samjong Accounting

○ *Revenue structure*

- Mint makes recommendations for financial products to its users through its platform and receives a commission from finance firms (ranging from 20 to 60 USD) if a Mint user subscribes to a recommended product.

- Mint recommends financial products such as credit cards, loans, and more based on its users' spending and consumption patterns. For example, if a user holds a savings account bearing a low rate of interest, the platform will notify the user of a higher-interest savings product

- The nature of Mint's highly-personalized advertising structure results in a comparatively high ratio of clicks to impressions; the company reported a 12 % click through rate.



* Source: https://www.intuit.com/company/press-room/media-contacts/

□ Digime, personal data storage

○ *Scope of business*

- A UK-based personal data storage provider that provides an integrated platform for collecting, managing and utilizing personal information

○ *Key business operations*

- Digime provides an integrated platform for individuals to manage their sensitive financial and other information. The platform categorizes this information into financial, social, medical, health care and entertainment information

- Digime collects data on personal activities via partnerships with other firms (data holders)

- This includes data from activities such as posts and comments on social media platforms including Facebook and Instagram, Twitter, Pinterest and Flickr

- It also collects data from over 1,000 medical institutions in the US; the UK; Iceland linked through its platform. This medical data includes information on allergies, physical health, immunizations, prescriptions and drug use

- Financial data is also gathered from nearly 1,000 financial institutes connected through the Digime platform, including PayPal, Visa, MasterCard, American Express and HSBC. These data include purchase histories and transaction records

- In the health care field, FitBit and Garmin are linked through the platform, allowing data on steps taken, calories burned, hours exercised and hours slept to be collected
- Information on entertainment preferences is also collected, as the YouTube and Spotify services are linked through the platform. Personal user data on listening history, playlists, favorited videos and uploaded videos are gathered

<Table 8> Digime data sources

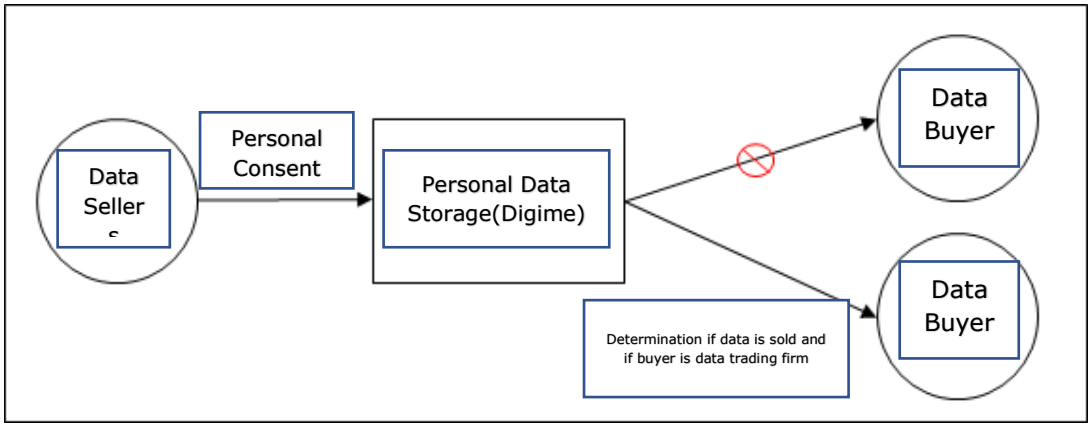
Type of data	Data source
Social data	Post and comment histories on the Facebook, Instagram, Twitter, Pinterest, and Flickr platforms
Medical records	Icelandic Health System, Blue Button Coming Soon, Hackensack University Medical Centre, Cerner, Epic, NHS
Financial data	Paypal, Visa, MasterCard, American Express, Citibank, Chase, HSBC, Barclays, etc.
Health & Fitness	Fitbit, Garmin
Music & Entertainment	Spotify, Youtube

Source: https://digi.me/sources/

○ *Usage method*

- 1) The user downloads the application 2) The user then selects a location to save data downloaded through Digime 3) The user links applications that are sources of personal data (such as Facebook, among others) 4) The user connects relevant sources and collects data he or she wishes to manage through a special Digime folder 5) The user selects which apps to use from within the Digime platform based on the shared data

<Figure 13> Digime's business model



Source: KPMG Samjong Accounting

- In short, Digime users can collect the information they want and determine which services they want to receive that utilize that information. Firms can use Digime to access high-quality, specific information

- It is thus a system in which individuals can directly manage and control their personal information proactively and a personal data service (PDS) to collect and manage personal information while enabling individuals to do so as well

○ *Revenue structure*

- Digime collects personal data and provides it to distributors or financial firms. In return, in collects a commission from firms when users link those apps to the Digime ecosystem

□ LifeSemantics'Life Record, a personal health data platform

○ *Scope of business*

- Lifecode, founded in Korea, provides a platform for users to collect and store individual diagnoses, physical measurements, life logs and other personal health record (PHR) data

○ *Business model*

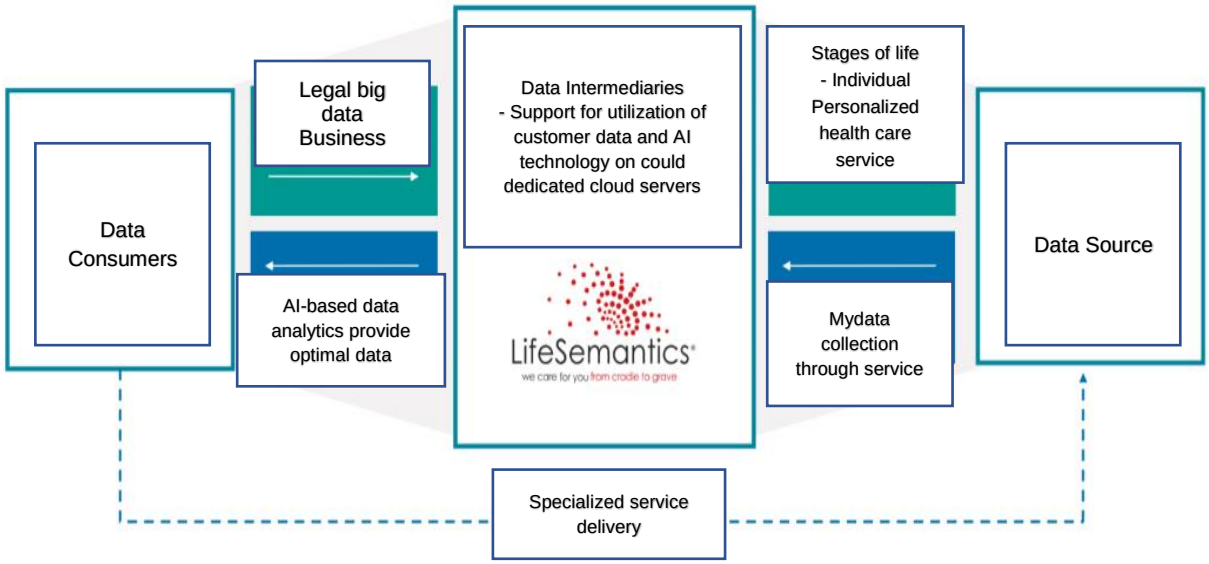
- Lifecode presents a service that predicts potential health problems and recommends ways to manage personal health through the collection and analysis of PHR

- LifeSemantics has secured a variety of users' PHR data through its operation wellness and medical device services that assess users' general health and recommend care

- In line with the fact that LifeSemantics deals with sensitive medical data, its platforms comply with the following domestic and international security standards: PIMS, ISO 27001 (Data Protection and Management System), ISO 27017 (Cloud Computing Information Protection), ISO 27799 (Medical Data Protection System) and HIPAA (US Health Insurance Quality and Portability Act)

- As depicted in the following image, through MyData individual users that provide medical records to data users (intermediaries) gain access to customized health management in all stages of life

<Figure 14> MyData business models in the health care sector



○ *Business method*

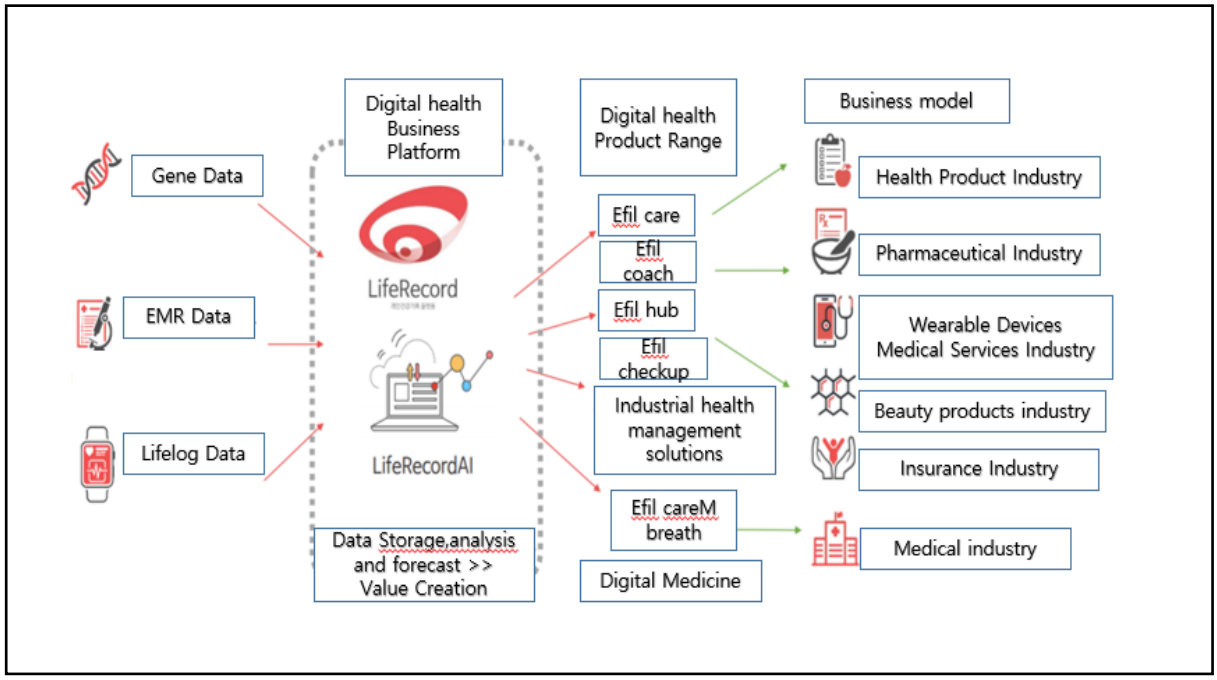
- Corporate data consumers can include insurers, medical device manufacturers, food processing and distribution firms and pharmaceutical companies

- Insurance companies should be able to secure direct sales channels to boost sales; medical device manufacturers might expect to sell more high value-added traditional medical devices. In addition, pharmaceutical companies can expect to reduce development times for new medicines.

- As for the revenue structure of LifeSemantics, the firm provides a variety of digital health services (efil care, efil coach, efil herb) through its LifeRecord personal health data platform once users save their health data to it. Put simply, once receiving data LifeSemantics convenient health management services

- In the process of providing the above services, LifeSemantics recommends health food products, medicines, medical devices and insurance products

<Figure 15> LifeSemantics' business model



□ Banksalad, a personal asset management service

○ *Scope of business*

- Established in Korea, Banksalad collects personal financial data and recommends individually-tailored financial products

○ *Business model*

- Banksalad provides an integrated platform through which individuals can manage their finances by linking bank, credit card and insurance account information with data on personal assets including real estate and vehicles

- By connecting customers' financial data with information on financial institutions' products, Banksalad provides a solution for recommending individually-tailored financial solutions and products. Currently, Banksalad collects data on 10,000 financial products and transactions from more than 200 financial institutions, analyzes the benefits of each product based on the data collected and recommends financial products customized to users' personal consumption patterns.

- A project is also underway to connect link personal health data into the ecosystem and make recommendations for customized insurance products

- In addition, the Banksalad application offers personalized advice based on analysis of personal consumption patterns. A “financial secretary” program analyzes average expenditures and alerts users when spending is excess of average is detected, encouraging more rational consumption behaviour.

○ *Business performance and revenue model*

- The Banksalad application has been downloaded six million times since an updated version was released in 2017. Through the app, 150 trillion KRW of linked financial products are being managed (1,000 KRW is roughly equal to 0.92 USD), and the average value of managed assets per use is 144 million KRW. An average of 5,000 new cards are issued through the service every month

- Core users are in the 25-44 age demographic and make up 73.2% of Banksalad’s total userbase. These customers are also most active in connecting to financial institutions and products and enrolling in products and services recommended by Banksalad. Whereas, the 35-54 year-old demographic makes heavier use of the insurance planning service

- Banksalad makes money through commissions received every time a user clicks on a link to a financial product recommended by the application and/or every time a user enrols in or purchases a recommended product or service

4.3 Challenges for the Global Adoption of MyData

- MyData has not yet proliferated globally, but has been introduced by a handful of major economies in the public sector to simultaneously protect and make good use of personal information. Many private firms are also undertaking projects using personal information

- It is likely that the dissemination of personal information and its use in various lines of business will become a subject of debate at the global level going forward. There exist a number of challenges to address not only in specific economies but at the international level as well

1) Technological challenges

① Establishing a MyData management system

□ **The necessity of a MyData management system**

○ *What distinguishes the MyData ecosystem?*

- In order to grow the MyData project, is necessary to find more applications for it. It is currently limited to processing consent management and bringing data into the public interest

<Table 9> Applications of MyData

Application	Description
Consent management	Use of personal information for agreed-upon purposes when data subjects (individuals) subscribe to services
Direct provision to data subjects	Direct provision of personal information to data subjects upon request
Personal data services	Data holders' transfer of personal information to data users immediately upon receipt of authorization; this process goes through personal data services provided to data subjects by MyData operators
Direct exchange between data holders and data users	Data subjects' authorization of simultaneous transfer of personal information from data holders to data users without use of personal storage device
Public interest utilization	Data subjects' personal information is transferred from one public institution to another without consent in out of concern for the public interest; individuals are notified afterward

- The fundamental difference the current system and the many applications of MyData as described in the above table — direct provision to data subjects, provision through personal storage devices and direct exchange between data holders and data users — is that the need for consent continually arises throughout the process of using personal data

- This requires a consent management system that can handle a wide range of frequent requests for processing consent; that MyData operators be able to manage this demand is important

○ *The role of MyData operators*

- To fulfill their roles in the ecosystem MyData operators must provide a user interface, persona MyData accounts and personal data storage services (PDS)

- Competitive MyData operators will be able to attract a large user base and fulfil the role they are meant to play in the MyData ecosystem. A market wherein multiple MyData providers compete to secure customers promises the provision of superior services

□ Approval management system

○ *Overview of approval management system*

- Data subjects use MyData accounts for consent/approval, review, transfer and provision of personal data

- Upon logging into the MyData system, data subjects are able to select data holders, set the scope and type of data to be provided, move data or review access histories, request and download specific personal information from data holders, connect and manage accounts at data users' platforms and manage MyData account settings

○ *OAuth 2.0 (Open Authorization 2.0)*

- Open Authorization 2.0 technologies enable data users' businesses to efficiently and safely use MyData

- OAuth 2.0 grants data users access to personal information only if explicitly authorized to do so by the data subject. The technology behaves as described in the following.

- First, MyData operators notify data holders of the intention to use select personal information of the data subject at the data subject's request. Next, the MyData operator notifies the data subject and data holder of the scope of data to be used (Data Scope). Then, the data holder provides the MyData operator with a login ID and password. The MyData operator saves the login information on its servers. Next, the MyData operator asks the data subject for the authority to receive the designated information from the data holder. The data subject then approves (or denies) this request. Then, the data subject connects to the data holder. To transmit the data to the MyData operator, the data holder asks for the user to confirm the login ID and password issued earlier.

<Table 10> Requirements and qualifications for MyData operators

Essential services/functions	Details of features/functions
MyData personal account	-Creation of personal MyData account -MyData account management

Management of connections with data holders	-Listing of data holders -Ability to connect to and sever connections with data holders -Ability to set the scope, type and temporal range of personal data held by data holders -Ability to review connection history with data holders
Management of connections with data users	-Listing of data users and services -Ability to connect to and sever connections with data users -Ability to set the scope, type and temporal range of personal data provided to data users -Ability to review connection history with data users
Direct review of personal information	-Ability to review personal information query records within MyData -Provision of data in machine-readable format (JSON) -Provision of data in unstructured (human-readable) format (CSV)
Access to record query histories	-Transparent disclosure of records related to provision of personal data to data users and nature of the data provided
Support for OAuth 2.0 protocol	-Support for OAuth 2.0 to enable data users' utilization of MyData service -Ability to manage data users' service applications
Provision of PDS	-Certain prerequisites must be met to satisfy security standards

② Data disclosure and format standardization

□ **The necessity of data disclosure and format standardization**

○ *The need for the standardization of data*

- To encourage the widespread adoption of MyData, the disclosure of data to the greatest possible extent is essential

- Yet even if personal data came to be broadly disclosed and shared, the reality is that would not produce an environment in which this data is actively utilized. This owes to the fact that as of now, the institutions that hold this data maintain it in proprietary, mutually unintelligible digital languages largely

which has led to the fragmentation of the MyData ecosystem and greatly restricts the utilization of this data

- So, in order to eventually overcome the limitations described above, data must be made available in a systematic and universal format under the MyData ecosystem

- In other words, storing data in XML, JSON, CSV and other machine-readable formats instead of unstructured document or PDF formats increases the digital accessibility of data

○ *Examples from select economies*

- Through the Smart Disclosure initiative, the US makes personal medical data, telecom payment records and energy use data held by government agencies and/or private firms available for direct download by consumers. The data is provided in machine-readable formats to promote the standardization

- Article 20 of the EU's GDPR guarantees the right to the movement of data and the right for data subjects to demand that data holders transfer their personal data to designated third parties or be made available for personal review. This obligates data holders to provide personal data in a universally compatible and systematic machine-readable format

- Finland has also agreed to release troves of public data in machine-readable formats as part of its Open Data policy

- Korea is also making pursuing legislation that will require public dated to be encoded in machine-readable formats. The law defines machine-readable formats as those for which software is used process the formatted data. These operations include identifying content and examining the internal structure of the data contained therein as well as modifying, editing and extracting data

□ Steps to improve data formatting for machine processing

- Even if data is stored in machine-readable formats, creating a competitive environment for MyData providers will prove difficult as long as data holders keep data in their possession in proprietary formats

- Ultimately, universalizing the data held by disparate data holders is ideal. As of now, the most effective method would be to unify data under the JSON format and serialize it

- In addition, there is a need to homogenize data architecture in order to increase data utilization

- This process can begin independently in individual economies, but in order to eventually secure global adoption multilateral consensus is essential

③ API disclosure and standardization

□ **The need for API disclosure**

- API comprises a set of definitions and protocols that can be used in applications to build and integrate software; it refers to an interface that allows for the control of the operating system or the functions of the programming language

- Open API is named as such because it is an API made freely available for public use. Google Maps and Open Street maps are two popular Open API applications, the use and functionality of which can be enjoyed on any website

- In simple terms, API allows users to provide access to resources in a controlled and secure manner, so service providers need only to decide to whom and how to provide the API

- Compared to screen scraping, a different approach to handling personal information, APIs do not require MyData providers to provide authentication-related information about data subjects, making APIs a superior tool for maintaining privacy and ensuring self-determination of private data

- Thus, pursuing API disclosure is a critical measure to enable data interoperability among components of the MyData ecosystem

□ Strategies for promoting Open API

○ *The scope Open API*

- As previously explained, Open API is critical to building the MyData ecosystem. In the short term, it should be made mandatory, and in the mid-to-long term, it will be necessary to pursue API standardization

- Already in the US data standardization and API standards are being established to improve the interoperability of data. In the EU, Open API disclosure of specific financial data through PSD2 is now mandatory

- However, obligating disclosure is likely to conflict with the interests of data holders, so it is necessary to agree on the extent of personal information that should be made available through Open API

- Thus at this point in time is appropriate to apply Open API to raw or unprocessed data — provided data and observed data — but not derived or inferred data

○ *Improve trust in Open API*

- The Facebook-Cambridge Analytica scandal is an example of the deleterious consequences brought on by the abuse of API

- Conversely, in the process of acquiring Smyte, Twitter blocked access its API without notifying the firms that were using its data. Hardship followed for the affected companies

- This necessitates that a system be established to prevent the misuse and abuse of APIs and to ensure continuity of business. There also exists a need to impose obligations on financial/structural integrity

2) Key systemic challenges

□ **Guaranteeing the portability of personal data**

○ *The need to guarantee the portability of personal data*

- Conferring the right to data portability is a prerequisite for advancing the MyData project; in the EU, this right has been legally recognized in the form of the GDPR

- The right to data portability means that data subjects retain the right to demand that personal information be made available for their own personal use or transferred to a designated third party

- Through this, data subjects are granted the right to privacy as well as the right to self-determination in the use of personal data

○ *Directions and proposals for encouraging acceptance of the right to portability of personal data*

- MyData is a neutral and independent approach to legal issues in the personal information space

- It can work regardless of whether the Opt-In or Opt-Out method is employed, and at the same time data subjects are able to protect and use their personal information

- As the right to portability of personal data gains legal and ideological traction, data holders in the current system are incentivized to oppose its introduction. They are threatened not only by the loss of their existing privileges but also by future competition from MyData operators or personal information service providers

- As part of this opposition, data holders might seek to defend their interests by defining the right to transfer personal information very narrowly or by confusing the issue of ownership of personal information by reducing the scope of applicable personal data to the greatest possible extent

- If the right to the portability of personal data is narrowly defined, it will be necessary to simultaneously promote mandatory API disclosure to solve the problem of read-only access to personal information

- While there are many hurdles to overcome in passing relevant laws and statutes due to the fact that the international community lacks a common understanding of data ownership, it is critical to build a multilateral consensus around the fact that data provided by and collected from data subjects (individuals) must be recognized as property of those data subjects (individuals).

- However, as stipulated in the GDPR, information processed via deduction or implication may be excluded from the scope of the right to the portability of personal information

□ **Cross-border movement of data**

○ *The current state of cross-border data movement*

- Just as digital trade has thrived as the digital economy as developed, international cooperative endeavours for the protection and utilization of personal information are expected to occur going forward

- Thus cross-border movement of personal information will become a transnational diplomatic issue

- The current reality is that cross-border flows of personal information are strictly limited compared to intranational movement

- However global business platforms remain somewhat free to conduct operations under this regulatory regime. Yet there exists controversy over instances of reverse discrimination in which some economies have not applied these regulations

○ *Trade agreements related to cross-border data movement*

- To promote free and fair trade a number of trade agreements have already introduced provisions governing cross-border flows of personal data

- However these agreements do not specify the extent to data subject to regulation is related to personal data

<Table 11> Levels of liberalization of digital regulations in US trade agreements

Regulatory targets	**US-Korea FTA**	**TPP (now CPTPP)**	**USMCA**
Permissions re: cross-border data flows	Cooperation	Obligation	Obligation
Ban on data localization	No regulation	Obligation	Obligation
Data subject to localization ban	No regulation	Financial data excluded	Financial data included
Requests for disclosure of source code/algorithms	No regulation	Obligation (Limited to source code)	Obligation (Includes source code and algorithms)
Online platforms accountable for information brokering	No regulation	No regulation	Exemption
Use of open government data	No regulation	No regulation	Provision promoting use of disclosed government data

○ *Measures to expand cross-border movement of personal data*

- To stimulate cross-border flows of personal data, it is first necessary to conduct an analysis of domestic regulations concerning personal data and its movement

- What follows is the need for a discussion on regulations regarding the transfer of personal information abroad stipulated in the GDPR

- If marshalling the resources for a multilateral debate proves too difficult in the early stages, talks involving representatives from a pair or handful of economies willing to engage could instead be held
- Based on those early talks, it might become necessary to build a general frame on the cross-border movement of personal data and later expand it to include more economies

4.4 Challenges for the Adoption of MyData within APEC

□ **Public discussion of the MyData project**

○ *Public discussions of MyData, a new concept, must come first*

- MyData remains an unfamiliar concept to most. Discussions explaining the significance of introducing MyData should be prioritized

- Public debate on the matter helps lay the groundwork for future bilateral or multilateral cooperation; promoting MyData projects between economies that have reached some level of consensus prior is more effective

- APEC members that have reached some level of consensus on MyData or have MyData policies in place (Japan; Korea; US) should lead a policy seminar

- In order to gather more diverse opinions, cooperation should be expanded not only among APEC members but also with non-profit organizations such as Global MyData, a leading voice in the public discussions on MyData

○ *The effectiveness of proactive bilateralism*

- As aforementioned, levels of understanding of MyData differs between economies, so it is necessary for economies that possess a certain degree of mutual understanding to proactively pursue bilateral cooperation

- Through these early partnerships, it becomes possible to set global standards for the MyData project and lays the groundwork for cooperative measures with economies that want to be a part of these partnerships

□ **Measures for cooperation among APEC members**

○ *Exploratory research on the promotion of MyData*

- Research should be conducted that assesses the current status of personal information ecosystems in each economy, including existing policies in APEC member economies governing the protection and utilization of personal data. The results of these analyses could be shared in promoting blocwide discussions

- Such a study would raise awareness of the feasibility and efficiency MyData through by investigating relevant case studies in APEC economies

○ *Target areas in which to promote MyData partnerships*

- As most APEC member economies are brand new to the field of MyData, bloc-wide collaboration from outset should prove difficult

- Selecting and promoting MyData in fields deemed most feasible is a reasonable course of action. It is particularly important that avenues for cooperation be explored in the financial sector, where efforts at promoting MyData are already particularly robust

- Health care is (like finance) seen as a particularly viable sector for promoting the MyData project. But individuals are more wary of making personal health information available and domestic regulations governing the medical sector tend to be much stronger. Thus significant obstacles remain to be scaled

- To choose and promote specific fields in which cooperation is more likely, a comprehensive analysis of trends related to personal data protection as debated during the negotiations of recent digital trade agreements should be carried out. Analytical targets might include, for example, the Digital Economic Partnership (DEPA) Agreement, to which Chile, New Zealand and Singapore are party, or the Korea-Singapore Digital Partnership Agreement

○ Commissioning a MyData research task force the Digital Economic Steering Group (DESG)

- The most important measure to take is ensuring that APEC economies have a firm grasp of the MyData system and its key strengths

- If the proactive measures prescribed are taken and a research task force is formed within the DESG, research to promote the expansion of the MyData system within APEC economies should be continuously undertaken

- This task force is to thoroughly analyze norms related to personal information in APEC economies, ongoing debates within the bloc on the principles of MyData as well as challenges facing technological cooperation between member economies and other institutional issues

- Based on these studies, researchers could share the findings of the task force with Member economies at regularly-hosted DESG forums or seminars

- Simultaneously, the group could promote cooperation between economies and institutions playing leading roles in the research and application of MyData

5. Conclusion and Implications

□ **The growing importance of data amid the expansion of the digital economy**

○ *Expanding the use of information is critical for the digital economy*

- As the majority of individuals' activities undergo digitalization, the scope and scale of businesses that take advantage of this are poised to expand

- This expansion is robustly evident not only in the service industry but in manufacturing as well. But the speed of the development of the digital economy depends on how personal data — which accounts for 75% of all data utilized — is exploited

○ The importance of using personal data and notable factors restricting its use

- The personal data that firms require for their businesses is often sensitive, private information. The rigor of the legal and regulatory regime governing the use of this data is reflective of both its importance and sensitivity

- While moving data within the borders of any given border is problematic enough, the cross-border movement of data is an even more delicate issue. This owes to the fact that many economies are exceedingly sensitive to not only individual privacy issues raised by international data traffic but data sovereignty issues as well

- The limitations on the cross-border movement of data creates challenges for firms in terms of global management and costs

□ **MyData, a solution for the protection and utilization of personal information**

○ *An information ecosystem centered around the individual*

- MyData is a policy initiative that shifts the locus of the existing personal information ecosystem, which is centered on companies (the data holders), to individuals. It is a system that grants the data subjects real control over the processing of their personal information while increasing the productive utilization of that data

- The MyData system empowers individuals to manage and utilize their information, and to understand in real-time how their data is being used. The system achieves a balance between the protection and utilization of personal data

○ *Discussions of MyData remain in their infancy*

- In spite of its significance as a policy, neither discussions nor applications of MyData are as of yet widespread

- Even ignoring the great number of considerations that need to be taken into account when introducing a new system, leading global firms are not taking active steps to protect their competitiveness and data through the use of MyData

- Even so, public sector policies in major economies utilizing the MyData system and embracing the MyData philosophy are being proposed, and globally non-profits such as Global MyData are working to spread the word

□ **Challenges for encouraging the adoption of MyData globally**

○ *Technological challenges*

- To establish a human-centered information ecosystem differentiated from the existing personal information ecosystem, a MyData management system must be built

- Such a system can be realized by MyData operators providing a MyData platform. This platform would feature a user interface through individuals, using personal MyData accounts and PDS provided by the MyData operator, are able to and manage their personal information. Tools for managing consent, utilization, authorization and inspection are to be provided

- However, even in the event that a MyData system is deployed, the services available on such a system would be very limited if not accompanied by the disclosure of personal information and/or the standardization of data formats

- To utilize data that has been disclosed, data holders must disclose API protocols and release the data in a standardized format in order for MyData operators to be able to retrieve and utilize the disclosed data

○ *Institutional challenges*

- Guaranteeing the right to the portability of data is a precondition to the growth of the MyData project. This already been made law by the EU in the form of the GDPR

- This right holds that, at the request of the data subject, a data holder must transfer the personal information of the data subject to a MyData operator or a data user (that is, a third-party service provider)

- The unfettered flow of data across borders is a precondition for achieving widespread adoption of MyData, as if the MyData system is to succeed it will ultimately do so at the global level

- However it is necessary to address economies' concerns over personal privacy and data sovereignty arising from cross-border data movement, as many economies have sought to restrict these flows, voicing concerns over personal privacy and data sovereignty. Some trade agreements in place include measures to regulate international data movement

□ **Challenges for encouraging the adoption of within APEC**

○ *The public debate in APEC on the MyData system*

- The first step to promoting the utilization of MyData in APEC is to encourage public discussions in which it can be introduced as a new concept

- It is of particular importance that bloc members offer their support for and consent of the system based on applicability and significance of MyData

- The introduction of MyData into the popular lexicon is meaningful in that it lays the groundwork for future bilateral or multilateral cooperation. Such cooperation could take the form of various seminars and meetings, held regularly within APEC, and cooperation with other bodies leading the MyData movement such as the EU and non-profits such as Global MyData and others

○ *Promoting exploratory research for MyData*

- The results of an investigation into the policies and personal data ecosystem in Member economies as it relates to data protection and utilization could be used to initiate discussions within APEC

- A research group established under the purview of the Digital Economic Steering Group should thoroughly analyze MyData and related principles within APEC and norms related to personal information in member economies. It should also study technological and institutional issues for cooperation among APEC member economies

- Based on these investigations the research group could share its findings with APEC member economies at forums or seminars hosted at regular intervals by DESG

- Finally, to promote joint MyData partnerships, it is necessary to select a number of fields where applying MyData is most feasible and encourage bilateral or multilateral talks between economies that have expressed some degree of interest. These endeavours will aid in establishing standards for the introduction of MyData within APEC

References

Accenture (2016), *Guarding and growing personal data value*

Don Tapscott, *The Digital economy: Promise and peril in the age of networked intelligence*, 1996, McGraw-Hill

OECD (2012), *The Digital Economy*, OECD

BEA (2020), *New Digital Economy Estimates,* BEA

PIIE(2018) Can digital flows compensate for Lethargic trade and investment?

UNCTAD(2017), Information economy report 2017: Digitalization, Trade and Development

APEC(2019), APEC Economic Policy Report 2019

European Commission(2015), Digital Single Market Strategy

K-data(2020), Introduction to Mydata

UNCTAD(2019), UNCTAD estimate of global e-commerce 2018

Lee Han-young et al (2019), My Data International Cooperation Plan, Information and Communication Policy Association, China Academy of Information and Communications Technology (www.caict.ac.cn)

K-Data(2018), White Paper of Data Industry

Frontier Technology Quarterly (2019), “Data Economy: Radical transformation or dystopia?”

Online materials

Statista (https://www.statista.com/statistics/254266/global-big-data-market-forecast/)

The Economist

https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy