This policy brief was prepared by obtaining input from the Digital Economy Ecosystem II Webinar Series with several stakeholders on data governance and digital economy policies in Indonesia which was organized by CSIS Indonesia, in addition to various studies that have been carried out previously. This public discussion was attended by representatives from the government, namely the Ministry of Communication and Information, Bank Indonesia, the Central Statistics Agency, representatives from organizations, and digital economy business actors. This policy brief aims to provide a review of the discussions and provide policy recommendations related to data governance that protects users and supports the development of innovation in the digital economy.

CSIS Policy Brief
Department of Economics

Implications of Data Governance Regulatory Framework Towards the Digital Economy in Indonesia

Yose Rizal Damuri & Dandy Rafitrandi
Departemen Ekonomi CSIS Indonesia

Digitalization and globalization constitute an enabler in international trade and investment which has caused the acceleration of the digital economy for the past few decades. Electronic data flow from the interaction between people in the economy has increased sharply from 100 gigabytes per day in 1992 to 150,000 gigabytes per second by the year 2022.[1] This trend is also in parallel with the global

[1] Digital Economy Report Value Creation And Capture: Implications For Developing Countries (2019). UNCTAD Digital Economy

consumption of mobile data per month which has increased by ten times in the last five years so that on average, every smartphone uses 9.4 gigabytes every month.[2]

Due to this, many nations have released regulatory frameworks related to data governance, including Indonesia. However, the main challenge that arises is how these frameworks can guarantee protection among users while also guaranteeing economic growth and innovation that rely on using and analyzing data intensively.

This policy brief would discuss some of the issues related to data governance, specifically on data protection and data sharing in the context of digital economic growth in Indonesia. The first section will discuss data and its types and the dynamics between stakeholders in data governance, namely users, the private sector, digital service provider platforms, and the government. Furthermore, some crucial issues in data governance, especially on regulations related to the digital economy, will be explained in the second part. In the third part, the discussion will then focus on data sharing and its potential implications in developing the digital economy in Indonesia with several case studies from other countries. Policy conclusions and recommendations will be discussed in the last section.

Data Governance and Stakeholders

Electronic data is one of the crucial elements behind the digital economy since it is an enabler of multi-side markets which is the main characteristic of digital platforms such as e-commerce and ridesharing. These platforms make traffic and exchange between various stakeholders, often referred to as data sharing, become unavoidable. It should be noted that the data collection process by one digital platform provider will be combined with data from other providers to obtain a more accurate analysis result. Furthermore, analysis of the data collected by digital platforms could also be used for policy formulation and implementation of regulations and other national interests, which means that the government also has an interest in gaining access to the data.

The use of data collected by digital platforms must also be accompanied by a commitment to ensure the protection of its users, who are the data source. As a result, data security is becoming increasingly important to prevent data breaches from becoming more frequent. The protection of user interests thus becomes very crucial about the aforementioned massive exchange of data. This is not only in the interest of users, but also affects the development of the digital economy in the future. With guaranteed protection of their data, digital platform users will also have more confidence in the technology and services being used, which in turn will encourage further innovation and development.

However, finding a balance between protecting personal data and supporting the development and innovation of the digital economy is not easy. It can often happen that the use of data has the potential to harm the user. For this reason, data governance needs to meet the interests of various parties in a balanced, accountable, transparent way that can be implemented properly.

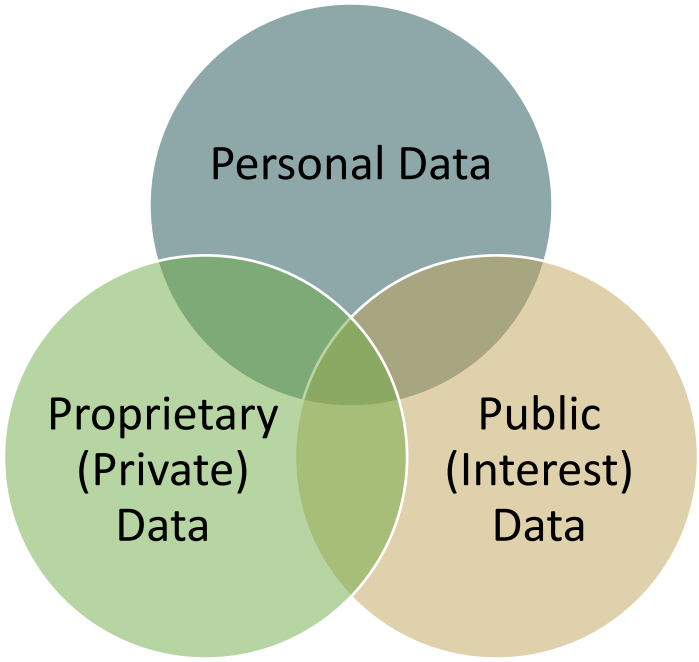
According to the Organization for Economic Co-operation and Development (OECD)[3], data can be divided into several types. First, personal data includes data related to identification or can be identified

[2] https://datareportal.com/reports/digital-2021-global-overview-report

[3] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en

against individuals to make up a private domain. Second, proprietary data or those protected by intellectual property rights such as copyrights and trade secrets. Finally, public data is not protected by intellectual property rights and other rights to be freely accessed and reused, including data for the public interest. With the acceleration of data flows and their future usage, the scope between the data above types will blur. This will be a challenge for policymakers attempting to make the appropriate regulatory framework.

Figure 1: Scope of Data Types



Source: OECD (2019)

With the increasing risk of data security, data users, the government and the business world have aspirations towards data governance. The government must realize this to strike a balance between the benefits and risks arising from data governance. On the one hand, the government has a goal to protect the security of user data through policies. But on the other hand, the government also has an interest in using data more optimally, especially through a data-based policy-making process to improve the quality of public services. The government also has an interest in protecting confidential and strategic state data.

From the user's perspective, an important issue of data governance relates to how their data is collected, processed and used. This is tied with threats associated with the misuse of personal data that can be detrimental in the future. In addition, trust in digital service providers and the government in terms of data governance still needs to be improved. The business world also has concerns about data regulations that are too restrictive, which threatens innovation. Restrictive data regulation also can increase compliance costs, which negatively impacts the investment climate, especially in the digital economy sector.

With the intensification of data exchange between various parties, there is a need for better data management starting from data collection and processing, *data sharing* regulations, and access to data,

specifically for the government as a regulator and protection of user data. This must be reflected in a regulatory framework equally applied to all parties and upholds equal principles and mechanisms. The following section will look at the regulatory framework for data governance in Indonesia and some specific discussions for each regulation.

Issues in Data Governance Policy in Indonesia:

While data governance has a fairly broad definition, this policy brief focuses on the policies and regulations related to data protection and data sharing. Figure 2 below attempts to provide a simple overview of the relevant regulatory framework of data governance in Indonesia.

Figure 2: Regulations Relating to Data Protection and Sharing in Indonesia

Source: Author

One example of data protection and sharing regulations is Government Regulation Number 71 of 2019 concerning Electronic Systems and Transactions and the Personal Data Protection Bill (PDP). This regulation is expected to protect and guarantee the fundamental rights of citizens relating to personal protection and guarantee the public of services from the government, business actors, and other organizations/institutions. In addition, this regulation requires government access to electronic systems and electronic data for monitoring and supervision purposes. This can increase the burden of compliance costs (especially for digital start-ups) and reduce trust among users. Furthermore, the unclear mechanism for implementing data sharing and protection and the weak coordination between government agencies are still the main challenges for the government. The impact of this, among others, creates confusion among the public, especially for business actors and potential investors in the digital economy. About the PDP bill, rules requiring explicit consent for all types of data processing can pose a cyber threat risk as data subjects need to share their information at various stages. In addition, requiring data controllers for verification can pose a security risk as data subjects need to share their personal data regularly, which could burden the business sector.

In addition, Government Regulation Number 80 of 2019 has also been explicitly issued regulating Trading Through Electronic Systems (PMSE). The Central Statistics Agency (BPS) is an institution authorized to collect data, specifically related to electronic trading data. The governance of data sharing

in the trading sphere is also further regulated in Government Regulation Number 5 of 2020 concerning the Trade Information System which includes articles related to the types of data trading and the authority of the Minister of Trade to request data from business actors and other ministries/institutions. Yet despite these two regulations, several issues still arise concerning the scope of data and the mechanism of data sharing between ministries/agencies which is still unclear. This will be a crucial factor in maintaining the integrity, transparency and security of data governance in Indonesia. Regarding the possibility of data leakage/failure, future follow-up regulations are expected to have clear standards in handling this matter.

About the payment system, which is an integrated aspect of the digital economy, Bank Indonesia has the Indonesia Payment System Blueprint (BSPI) 2025 which aims to reform the payment system regulations in Indonesia. Several strategies and initiatives are present, such as developing public data infrastructure and ensuring the open access and protection of personal consumer data. Of course, this data will be used for the national interest, specifically to support digital transformation in Indonesia. However, finding a balance between innovation, consumer protection and integrity of data governance is not an easy matter.

In summary, all stakeholders need to pay attention to the consequences of implementing the above regulations. First, the absence of a standardized data protection mechanism among ministries/agencies will increase the potential for overlapping policy making and implementation related to data governance. The government's increasing attention to the role of data in policymaking must also be interpreted as an increasingly urgent need to expand the government's capacity to manage data in accordance with good mechanisms and standards. In other words, this does not only mean collecting more and more data from the business sector.

Second, the government must also realize that the business sector has responsibilities to data users/owners so that data sharing is only possible for aggregated data. More disaggregated levels of data will increase the possibility of misuse if it is transferred in different formats, has an unclear legal basis and is not accompanied by a good data sharing mechanism.

Third, restrictive regulations can increase compliance costs for the business sector, putting a negative impact on the business climate in the digital economy sector. In addition, if these regulations have different principles from the best practices in other countries, Indonesia may not receive the full benefit of the cross-border data trade and flow.

Finally, several points that should be underlined relating to the regulatory framework for data protection and sharing in general include:

- Data protection and sharing regulations should apply to all stakeholders without exception. All parties must uphold the principles and mechanisms that are equal and in accordance with the regulations that apply to all parties, including the government. For example, in the current regulatory framework, there is no mechanism in place in case of misuse or leakage of personal data from the government side

- In other words, unequal and more exclusion of responsibilities can give rise to the abuse of power. Therefore, all stakeholders' same responsibilities and obligations in complying with procedures and mechanisms for data collection, processing, and sharing are essential aspects

in establishing a balanced regulatory framework and supporting Indonesia's digital economic climate.

- Coordination between ministries/agencies is a crucial factor in maintaining the integrity, transparency and security in data governance in Indonesia. Regarding the possibility of data leakage/failure, future regulations are expected to have clear standards in handling this matter.

- Regulatory frameworks relating to data protection and sharing procedures must ultimately pay attention to legal principles and human rights. Reflecting on the practice in other countries, regulations related to this are usually discussed at the statutory level by including public participation such as the Electronic Communications Privacy Act (ECPA) in the United States which has been revised many times.

Learning From the Experiences of Other Countries

Several regulations related to data sharing will be discussed as case studies, including the European Union, Singapore and Australia.

General Data Protection Regulation (GDPR) – European Union

The GDPR applies to each European Union member state, aiming to create a more consistent consumer and personal data protection across all EU countries. Some of the key privacy and data protection regulations in the GDPR include requiring subject consent for data processing, anonymizing data collected to protect privacy, providing data breach notifications, handling cross-border data transfers securely and requiring certain companies to appoint data protection officers to oversee GDPR compliance.

Compared to GDPR, Indonesia's PDP Bill includes some stricter provisions. For example, the PDP Bill stipulates a very short timeframe for data controllers as they have to respond to data owner requests within 72 hours and must provide a notice of infringement within 72 hours. In contrast, GDPR allows data controllers to respond to data owner requests within one month. It also requires that the data controller notify the breach within 72 hours while providing a reason for a delay if the notification is not made within 72 hours.

GDPR mandates cooperation between data controllers and processors with regulatory authorities under strict conditions. The GDPR also prohibits controllers from "processing" personal data unless one of six situations, or permitted purposes, applies. Before sharing personal data with government agencies, the controller must determine its applicable permitted purpose, such as consent of the data subject, where necessary to protect a person's vital interests, and where necessary for the performance of tasks implemented in the public's interest.

The Indonesian regulatory framework, such as Ministry of Communication and Information Information Regulation No. 5/2020 concerning Private Scope Electronic System Operators broadly regulates authority access to corporate systems and data, which is not in line with the international standards set by GDPR.

GDPR is seen as a model regulation for data governance. It sets data protection standards which also inevitably increases compliance costs for digital companies operating in the EU. While companies

now have more standards to comply with, GDPR is generally seen positively because it also provides assurances and protections for personal data that previously did not exist. After two years of implementation, the GDPR has positively and negatively impacted the digital economy.

The positive impact is that it provides a new standard of personal data protection for citizens, increasing user trust and encouraging more people to use digital services. This standard is also widely used to benchmark other countries in organizing their regulatory framework for data governance. On the other hand, GDPR has the potential to complicate the compliance process and increase operating costs (especially for start-ups), presenting obstacles to the free flow of information.

2018 Public Sector Governance Act – Singapore

According to the Public Sector Governance Act, when a *data sharing* directive is given, Singaporean public sector bodies and their officials are authorized to share information under the control of that agency with other Singaporean public sector bodies to the extent permitted by the data sharing directive. A centralized agency has been set up to ensure that raw data is properly anonymized before being released to the relevant agencies.

Public sector officers who share personal data of Singaporeans without permission can be fined up to $5,000, jailed for up to two years, or both. The same applies to those who use data for their own benefit or re-identify anonymized data without authorization. Moreover, criminal proceedings can still be instituted even after they leave Singapore's public service sector. On the other hand, Indonesia's regulatory framework has not included any sanctions for public sector officials who misuse information, disclose information without authorization, or are proven negligent in the data sharing process. It is important for policymakers to include such sanctions to prevent future moral harm.

Unlike the GDPR, the Public Sector Governance Act regulates data sharing among government agencies in Singapore. This regulation provides guidance for policymakers in Singapore when they receive, share and disclose data to relevant parties. This regulation also reassures companies as it sets the standard for data protection measures among government agencies. Overall, this regulation supports responsible data use and data sharing among government agencies, which will support good data governance in Singapore's digital economy sector.

The positive impact of this law is that is provides a new standard of personal data protection for public officials and agencies when they share data, providing guarantees for companies in case of data leakage and data sharing without permission. But on the other hand, this regulation relies heavily on government officials' competence to manage data, which will be a challenge if a similar policy is implemented in Indonesia.

Privacy Act and Data Sharing Principles – Australia

In anticipation of the government's growing need to share data between ministries and the private sector, the Australian government developed a guide on data sharing principles that provide Australian government agencies a clear guide when they share data with others. For example, before requesting and sharing data, government agencies in Australia must go through a *self-assessment* process, determining whether the data request is in accordance with the data used and has obtained approval from the data owner. The data sharing guide also provides government policymakers with questions that they must answer to ensure alignment between the request and the use of the requested data.

Despite having a Privacy Act since 1998, data privacy remains a major issue in Australia. People are very concerned and unfamiliar with the reasons behind collecting and using their data by the government and the private sector. Calls have been made to revise the law to increase the security of personal data. Nevertheless, Australia has adopted one positive approach: the establishment of the Office of the Australian Information Commissioner (OAIC) as the sole oversight body responsible for overall data protection in Australia.

The private and public sectors have largely welcomed the principle of data sharing as it has become the standard for government agencies in Australia when requesting data and sharing data. For example, the data sharing principle advises data custodians (those who own/own the data) to have data-sharing agreements with third parties (those who receive the data), and this applies to both the private and public sectors. This is a better practice to support the growth of the digital economy compared to what we have in Indonesia.

Conclusion: Towards a Better Data Governance

The factor of trust between stakeholders is one of the essential things in building a policy framework for data governance. Data protection principles need to be clarified and applied to all parties, not just the business world. This includes standards and mechanisms to prevent data leakage and misuse, including government agencies. Furthermore, applicable regulations must apply to all parties with minimum exceptions such as the GDPR. In principle, good data governance should be able to facilitate the responsible use of data by all parties which in turn can increase trust between stakeholders.

There is a consistent trend across government institutions to demand *e-commerce* players to share data and/or information. However, this trend is not followed by strong data protection commitments. Most of these regulations only require companies to share data without proper and detailed explanations of data protection measures. Moreover, there is a lack of coordination between ministries regarding how companies are expected to share data.

The lack of coordination between ministries can also be seen from the different data types required from companies and differences in data sharing mechanisms, scope, objectives, and government coordinators. This results in high compliance costs and a potential lack of trust from users, as users expect the private sector to be able to protect their data and not share it with other third parties including governments.

Finally, the issue of data governance is a global issue that still has many challenges. For this reason, regulatory convergence and international regulatory cooperation are things that must be encouraged in order to realize regulations that support the development of the digital economy. Examples in data privacy issues can be found in the OECD Guidelines on the Protection of Privacy Transborder Flows of Personal Data, GDPR and the APEC Cross-Border Privacy Rule. The principles contained in these *regulatory frameworks* can serve as a guideline for policy makers in Indonesia to provide effective data protection and avoid unnecessary information barriers. With regulations that are more aligned with international practices and a supportive digital economic climate, Indonesia's digital trade could reach USD 172 billion by 2030, an eight-fold increase compared to 2020 data. [4]

[4] Hinrich Foundation, 2019, "The Digital Komodo Dragon: How Indonesia Can Capture the

Digital Trade Opportunity at Home and Abroad." Available via the Internet: https://www.alphabeta.com/wp-content/uploads/2019/02/digitrade_indo_eng_1-pgview.pdf