T20 INDONESIA 2022 THINK

Policy Brief

REGULATING CROSS-BORDER DATA FLOWS IN THE DEVELOPMENT CONTEXT

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Thomas Dewaranu, Center for Indonesian Policy Studies
Glen Hodgson, Free Trade Europa
Pingkan Audrine, Center for Indonesian Policy Studies

Abstract

Internationalization of digital services and products shifts the way data is collected, processed, and stored, from only within domestic settings to regional or even international level. While this has helped create digital innovation and improved digital products and services, some governments feel that they are receiving less than a fair share from the value creation of the data collected under their jurisdictions. As a response, they create barriers to transnational transfer of data from their jurisdictions, undercutting growth and development of the digital economy. Navigating around this issue will require G20 leaders facilitated by the Digital Economy Working Group (DEWG), to adopt a development-sensitive approach on data policy and promote solutions that address concerns from the data suppliers.

Challenges

Digital data is the lifeblood of the digital economy and has been the main resource for digital service innovation and digital intelligence. As the digital sector becomes more globalized, data collection and processing take place across different jurisdictions. Free cross-border data flows is, therefore, foundational to help spur innovation and productivity, especially as global growth becomes increasingly reliant on the internet economy. The contrary, as shown by some studies, negatively affects trade, investment, and GDP, as well as preventing the development and roll out of innovative products and services (Bauer et al., 2014).

Unfortunately, the past few years have seen a growing tendency especially from developing countries to claim sovereignty over their digital data that is typically manifested into data localization policies. Although cyber security, consumer privacy, and law enforcement are commonly used as underlying rationales for the digital protectionist stance, concerns over distributional impact of the value extracted from digital data is also often at play.

India for example, is known for efforts to maximize domestic digital development by imposing data localization and mirroring. Article 33 of India's Personal Data Protection Bill 2019 allows "sensitive personal data" to be transferred overseas subject to certain conditions, but still mandates data processors to keep the copy in India. The broadly defined "sensitive personal data" exacerbates the issue. The Bill has included financial and health data, official identifier, and sex life as sensitive data, but still allows the government to add more into the category in the future[1].

Although the Indian government has recently withdrawn the bill from the parliament due to heavy criticism, similar requirements can still be found in the National E-Commerce Policy draft (Ministry of Commerce and Industry of India, 2019). The title of the draft—India's Data for India's Development—indicates that the distributional issue in digital technology is among reasons for the restrictive approach. The draft admits that restrictions on cross-border data flows are intended for, among others, the "creation of high-value digital products in the country"[2].

[1] India's Personal Data Protection Bill 2019 is accessible at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[2] See p.15 of the draft. Accessible at https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

When concerns over unequal distribution of the economic gains from data are contrasted with risks of transnational data transfer such as public security, incentives to hoard data within national borders grow. China, for instance, has three laws that altogether form a regulatory framework for data processing both within and outside of its jurisdiction—Personal Information Protection Law (PIPL), Data Security Law (DSL), and Cybersecurity Law (CSL). Liu (2020) argues that cybersecurity and national security are a central theme for the framework, resulting in restrictive requirements for "data handling activities" especially overseas. Article 38 of the PIPL requires cross-border data transfers by "general" data controllers[3] to either undergo security assessment by the Cyberspace Administration of China (CAC), third-party certification through a competent government authority, or complying with a standard contractual clause (SCC) developed by the CAC.

The Chinese and Indian approaches have been replicated by numerous countries under different narratives and with varying justifications. The number of data localization measures has doubled in the last four years—from 67 barriers by 35 countries in 2017 to 144 restrictions by 62 countries in 2021 (Cory and Dascoli 2021). Following China as the world's most data-restricted country are Indonesia, Russia, and South Africa—all of which are G20 members.

Restrictions on the free flow of goods are admittedly a classic issue in trade discussions. In the data economy, however, many unique attributes of the digital data complexify efforts to measure the contribution of free data flow to the digital economy—and consequently also the negative impact of its barriers. For instance, some see that tariffs on cross-border electronic transmissions negatively impact GDP and tax revenue due to higher market price and shrink consumptions (Lee-Makiyama & Narayanan, 2019). Others, on the contrary, argue that moratorium on custom duties on electronic transmissions forced developing countries to bear 95 percent of global loss in tariff revenue (Banga, 2019). Regardless, the World Trade Organization (WTO) members have agreed not to impose custom duties on electronic transmissions.

Furthermore, there is also the privacy dimension of the discussion which has taken centre stage in recent years. The growing trend is the realization that personal data belongs to individuals and not to governments or public authorities. In addition to tariff revenue, consumer protection becomes one of the key interests in regulating transnational data flows.

Against this backdrop, encouraging Data Free Flow with Trust (DFFT) as agreed in the G20 Digital Ministerial Meeting 2021 in Osaka requires G20 leaders to adopt appropriate measures that balance these competing interests. G20 leaders need to adopt development-sensitive

3 The Chinese laws differentiate between general controllers and other special types of data operator such as 'automobile data processor' or 'critical information infrastructure operator' (CIIO)

approaches on data policy and promote at least these three things. First, a clear and commonly accepted data classification based on risk. This is to encourage countries to rethink their data restriction policy based on risk without denying their regulatory authority, especially on oversensitive data that carries national security risks. Second, data transfer should uphold the accountability principle. Countries must be encouraged to develop national-level data protection regulations that meet the commonly accepted standards for data protection and privacy, cyber security, and legal accountability in managing digital data. In addition, they can also engage and subscribe to relevant plurilateral arrangements on data protections. Third, ongoing research and discussions on the economic value of data especially in the development context should be in the G20 agenda.

Proposals for G20

The perceived unequal distribution of gains from data combined with the risk of data transfer overseas requires G20 leaders to factor in the multidimensionality of digital data in their effort to encourage DFFT. Free data flows narratives need to explore reasons beyond the economic dimension and take into account security and privacy concerns. In addition, the distributional impact of digital intelligence should also be considered even from a "light touch" perspective in each of the suggested recommendations and action steps.

At the center of the narratives, G20 Digital Ministers must underline that individuals should own their personal data[4], but non-sensitive information should be shared and processed freely across borders within a clear accountability framework. This creates opportunities for businesses to improve their services, governments to make data-informed decisions, and individuals to benefit from them.

1. Developing a clear and commonly accepted data classification based on risk

For this to materialize, risk-based classification of digital data is required to help balance commercial and security interests in data collection and management. There are different types of data based on different taxonomies. The most common dichotomy is between personal and non-personal data, but there are other classifications such as public versus private data. Within each category, differentiation of digital data can be made based on the sensitivity and risk level.

When privacy rights are taken into account, regulations typically make access to personal data more restrictive than non-personal data. However, not all personal information carries the same risk. Personal data on bank accounts or protected health information, for example, are more sensitive than information on name or date of birth. As such, exercising the same level of barrier to access for all types of personal data would not be a desired solution.

The risk of each type of personal information is typically associated with the degrees of identification. Higher levels of identification would usually lead to higher risks, and as a corollary, extra layers of protection are typically imposed when it comes to personal identifiable information

[4] Personal data is typically defined in a broad sense as information related to an identified or identifiable natural person. Different wordings with similar meanings may be used. In Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), for example, personal data is defined as any factual or subjective information, recorded or not, about an identifiable individual.

(PII). OECD (2020, pp.13-14) developed a worth referring risk-based personal data classification as follows:

- *Identified data*: Data that can unambiguously be associated with a specific person due to the observable PII in the information.
- *Pseudonymised data*: Data for which all identifiers are substituted by aliases. The alias assignment is irreversible by anyone except for the party that performed them.
- *Unlinked pseudonymised data*: Data for which all identifiers are erased or substituted by aliases. The assignment function is erased or irreversible, such that the linkage cannot be re-established including the party that performed them.
- *Anonymised data*: Data that is unlinked and which attributes are altered (e.g., attributes' values are randomised or generalised) in such a way that a person cannot be identified, directly or indirectly, by the data alone or in combination with other data.
- *Aggregated data*: Statistical data that does not contain individual-level entries and is combined from information about enough different persons that individual-level attributes are not identifiable.

This categorization also shows that there are ways to anonymize identifiers in personal data to minimize the security risk from sharing them. When personal data is effectively anonymized, they would be excluded from a certain degree of security requirements that are put in place to protect privacy (OECD, 2020). Data controllers and processors have started to use this in their cookies, aiming to balance the need to measure their website performance while also respecting individual privacy. This option serves as an alternative to costly data localization and data mirroring.

As for public sector data, there are several recognized standards to which countries can refer. For instance, categorization of public sector data can draw lessons from the National Institute of Standards and Technology (NIST) 800—60[5]. The NIST 800-60 suggests information reclassification based on different security risk levels of low, moderate, and high, which will determine the level of security controls applicable to them. The grouping is decided according to the potential security impact in the event of unauthorized disclosure, modification, destruction, and access disruption to each type of information and data.

Categorization of data based on risk allows governments to contrast the cost of one-size-fits-all restrictive data policies such as data localization versus the benefit from applying appropriate

[5] The NIST 800—60 is accessible at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

security measures based on the associated risks of each type of information. The cost of the former goes beyond direct investment cost in domestic data center and storage, and brings repercussions in trade and GDP, whereas the latter apply necessary measures to protect data only when they are relevant. For public sector data, the categorization helps governments to see that there is typically a small portion of highly-sensitive data where security interests will outweigh competing issues (US-ASEAN Business Council, 2019).

It is typical for governments to assume a right to extend the interpretation of sensitive data in their regulations. Without clear boundaries, this risks a non-transparent decision-making by authorities in determining whether a certain type of information would require extra security layers to manage. Risk-based data classification helps businesses and governments to agree to a common ground that such interpretation derives from a measurable consideration.

Risk-based data groupings also enable data governance based on the risk of data activities. Controllers may be subjected to reasonable security measures corresponding with the processing activities. For example, large and systematic processing of sensitive personal data may be subjected to extra requirements such as appointing a Data Protection Officer, or mandatory consultation with the Data Protection Authority.

2. Developing frameworks for accountable data practice through data protection law and plurilateral arrangements

Accountable practice in data management and data protection is crucial to encourage trust from digital users and governments engage in data activities. The trust between governments help encourage DFFT and digital innovation, while consumers' trust helps increase adoption of emerging digital technologies to support collective development agenda such as Agenda 2030 that is widely known as Sustainable Development Goals. Developing comprehensive data protection laws and engaging in different plurilateral arrangements help to facilitate the process.

Data protection laws

In order to build trust within and beyond national jurisdictions, G20 countries must have adequate national-level data protection laws that support accountable data management by both public and private institutions. In line with point 10 to 12 of Osaka Leaders' Declaration (G20, 2019), the laws need to strike a balance between different aspects of data, including privacy, data security, and data transfer to support innovation.

On a national level, data protection legislation is needed to incentivize accountable data management by both public and private data controllers and data processors. Data regulations in many G20 countries are scattered piecemeal across different policies with weak monitoring and enforcement mechanisms, making it difficult for data processors and controllers to comply.

Countries with lack of compliance and enforcement mechanisms in their data governance are also at risk of being excluded from participating in the global data economy. Data regimes such as European Union General Data Protection Regulation (EU GDPR), for example, allows data transfer only to jurisdictions with "adequate level of protection". Without far-reaching and enforceable personal data protection regulation, trust between businesses and governments from varying jurisdictions are difficult to achieve.

Comprehensive personal data protection laws are also needed to generate trust between countries. Personal data protection laws sow the seed of trust among digital users, businesses, and governments beyond jurisdictional borders. For developing countries seeking to maximize economic opportunities from the digital boom, consumers' trust is essential to increase adoption rate among the users.

The law needs to address common consumer concerns in the digital space. For example, consents are typically mandated by regulations prior to collecting user data, but digital platforms often use long technical and complicated text in their Terms and Conditions (T&C) documents. Constrained consumers' ability to read and fully understand the T&C render a question if consent on T&C can fully be relied on as contractual rights and obligations between platforms and users. Data protection laws can, therefore, accommodate the opt-in consent model as encouraged by the EU GDPR.

Part of developing an accountable data management framework is by establishing an independent supervisory function to minimize conflict of interest. An independent body that ensures that data collectors and processors, both public and private, abide by the best standards in protecting privacy rights, helps to generate trust among the users.

Plurilateral arrangements

Countries lacking data protection laws can alternatively subject themselves to both binding and non-binding plurilateral arrangements. Both public and private data controllers and data processors need to be encouraged to adhere to commonly accepted principles such as those in the OECD Privacy Guidelines or APEC Privacy Framework.

Where possible, binding arrangements such as the APEC Cross-Border Privacy Rules (CBPR) System is also an option for business entities in the G20 countries. Government-backed certification system in APEC CBPR allows private entities to perform data activities including data transfer upon proof of ability to meet the privacy and protection requirements. Likewise, model clauses such as the EU Standard Contractual Clauses for International Data Transfers (European Commission, 2021) and/or the Association of Southeast Asian Nations (ASEAN)

Model Contractual Clauses for Cross Border Data Flows (ASEAN, 2021), are also useful for companies to navigate varying data policies in different jurisdictions.

3. Ongoing research and discussions on the economic value of data especially in the development context

Ongoing discussions on data economy and how it can contribute to the development agenda are also necessary to complement efforts to minimize the risk of cross-border data transfer and empowering the rights of data owners. It is vital to underline how free data flows enable innovation and contribute to the overall development agenda.

Firstly, free data flows create an environment for innovation and are a key component of a global digital future, which is essential for jobs and growth. In particular, entrepreneurs as well as small and medium enterprises (SMEs) can benefit from easier access to data and the ability to process, send, and utilize it globally. Data needs to be seen as a public good as well as the lifeblood of opportunity, success, and growth.

A spirit of general openness and access to data needs to be created globally. This means that companies and individuals should be able to get access to non-personalized public data without administrative, organisational, or monetary barriers. This approach will be a cornerstone of fostering open innovation. As such, provisions should be put in place at the national, regional, and local levels to ensure that non-sensitive public data (from governments, municipalities and public authorities as well as private companies) is open. This will allow the development of new products and services which will facilitate businesses, support consumers, and help global populations. This can take the form of new business models as well as efficiencies in storing and processing data.

Further, free data flows across national borders should also facilitate new products and services across a wide range of development sectors—finance, renewable energy, trade, innovation and technology among others and more dynamic e-commerce solutions. This should also allow for the development of a broader range of simple-to-use solutions for individuals around the world, as well as moving data between cloud service providers. Better authentication and security in cyberspace will be brought about by the free flow of data, too, contrary to the false narrative spread in certain quarters that localized services are “by default” more secure than cross-border services. On the contrary, better and more thorough security detection, through the analysis of more threats and trends, will be possible through the free flow of data.

This approach will also tie in with the global development agenda. Removing existing data localization measures will drive down the costs of data services, provide companies greater flexibility in organizing their data management and data analytics, while expanding their use and choice of providers. This could boost GDP in developing countries as well as benefit citizens.

Developing countries could therefore become destinations for cloud services and IT resources. This is a strong reason to end the international trend of unjustified data localization requirements. Increasingly these restrictions can be viewed as barriers and tools of an industrial policy to protect national champions.

From a consumer perspective, increasing numbers of citizens in developing countries have a smartphone and this can be the gateway to a host of new products and services. The free flow of data needs to be ensured in order to allow this to grow. Sadly digital protectionism is growing and a shift to a digital bloc economy system is being followed. It is essential that this trend is reversed for the good of consumers, businesses, and governments.

The Digital Economy Working Group (DEWG) should be at the forefront in advocating these recommendations and facilitating lesson sharing between G20 Ministers responsible for the digital economy, on regulating data flows. Understanding country-specific effects of barriers to data transfer is of high importance. Indonesia's Ministry of Communication and Informatics—the focal point of 2022 DEWG—should create a forum where G20 Digital Ministers can share insights on how their data regulations have managed to balance competing interest in cross border data flows, and what can be learned from the experience.

The Industry Task Force, whose members are among the most affected from transfer restriction policies, should also actively engage in the discussion, sharing challenges in navigating around data transfer complexity. Digital industries should also share private-led initiatives (e.g., ways to anonymize personal data) that could serve as an alternative to strict data localization policy.

As geopolitical competition helps form data flows policy especially in trade context, G20 leaders should take an active role in shaping the global discussion about DFFT outside the G20 forum. For instance, six G20 members are joining the recently launched Indo-Pacific Economic Framework (IPEF) in 2022, in which free data flow is one of the focuses under Connected Economy pillar (White House, 2022). As the initiative involves other Asian countries outside of G20 it is imperative to ensure that the multilateral initiative accommodates the DFFT vision.

Conclusions

Hoarding digital data in local facilities is a costly measure since the value of data is created when it is used, analysed, and processed to help solve social and economic problems. However, while transnational data transfers should be encouraged, they must also be exercised with accountability. Encouraging DFFT in the development context requires efforts to minimize the risk of privacy and security breach, increase domestic consumers' trust, and continuous discussions on how the data economy works.

The latter is important especially to generate understanding among the G20 countries that DFFT is not a zero-sum game but rather a situation that allows everyone to gain. Given that more

opportunities globally are being created via the digital economy, this represents the lifeblood of potential growth and economic development.

To unlock this potential, it is vital that trust is built between businesses, platforms, and governments. At the same time there is a need for the synchronization of regulations and standards across jurisdictions. By following common rules—and bestowing common rights on individuals—data flows will be smoother and the benefits of new products and services will be enjoyed by a wider group, particularly with a view to meeting development objectives.

References

ASEAN, *ASEAN Model Contractual Clauses for Cross Border Data Flows*, 2021, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

Banga, R., Growing trade in electronic transmissions: Implications for the South. UNCTAD Research Paper, 29., 2019

Bauer, M., Lee-Makiyama, H., Van der Marel, E. and Verschelde, B., *The costs of data localisation: Friendly fire on economic recovery* (No. 3/2014). ECIPE Occasional Paper.

Cory, N. and Dascoli, L., *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology and Innovation Foundation, 2021

European Commission, *Standard Contractual Clauses for International Transfers*, Brussels, 2021, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

G20, *G20 Osaka Leaders' Declaration*, Japan, 28-29 June 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

Lee-Makiyama, H. and Narayanan, B., The economic losses from ending the WTO moratorium on electronic transmissions (No. 3/2019). ECIPE Policy Brief. 2019

Liu, J., *China's Data Localization*. Chinese Journal of Communications, 2020, Vol. 13(1). pp. 84–103.

Ministry of Communications and Electronics and Information Technology, *The Personal Data Protection Bill*, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Ministry of Commerce and Industry of India, *Draft National e-Commerce Policy*, 2019, https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

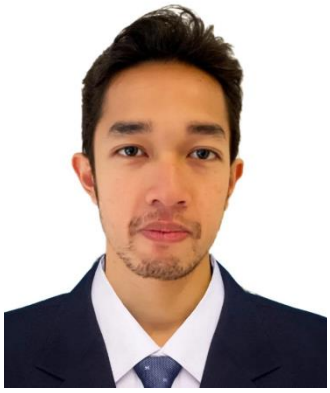
Organisation for Economic Co-operation and Development (OECD), *Mapping approaches to data and data flows. Report for the G20 Digital Economy Task Force*, 2020 https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf

US-ASEAN Business Council, *Digital data governance in ASEAN, Key Elements for a data-driven economy*, 2019, https://www.usasean.org/system/files/downloads/digital_data_governance_in_asean-key_elements_for_a_data-driven_economy.pdf

White House, *FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity,* 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/

About the authors

Thomas Dewaranu, Center for Indonesian Policy Studies



Thomas Dewaranu is a policy researcher at the Center for Indonesian Policy Studies. His policy research and advocacy work cover digital economy, economic opportunities, and rural development.

He is also an Indonesian lawyer with extensive exposure of various legal issues, including company and debt restructuring, financing, intellectual property, technology and communication, and dispute resolution. He advises for domestic and multinational companies and was involved in some of the biggest debt restructuring cases in the country.

Glen Hodgson, Free Trade Europa

With over twenty years' experience in communications, public affairs and lobbying, Glen is the founder of the think tank Free Trade Europa, which focuses on promoting free trade, openness and the rule of law within the European Union and internationally. Glen also leads a stakeholder initiative on the platform economy in the Nordics.

Glen was previously responsible for the Nordics, Baltics and Central & Eastern Europe within an international communications agency. Prior to this he worked for the European institutions as well as governments, blue-chip international companies, start-ups and NGOs as a lobbyist, strategist and communications advisor.

Glen was also the Secretary General of a European trade association for five years. Today, Glen is a respected commentator on European affairs, as well as a frequent presenter, moderator and panellist at European policy events. Glen is also a trainer and coach on technology, migration, labour force, transport and sustainability policy as well as communications techniques for the public and private sectors.

Pingkan Audrine, Center for Indonesian Policy Studies

	Pingkan has a keen interest in the nexus of digital transformation, trade, and diplomacy with an eagerness to championing multi-stakeholder approach. She has more than three years of public policy research & advocacy experience as a Researcher at the Center for Indonesian Policy Studies where she covers research on the digital economy; highly-regulated industry; and the impact of international trade and investment towards economic opportunities. She is also a part of the EU-ASEAN Next Gen Think Tank Dialogue (The EANGAGE Project) funded by the European Commission, serving as a Research Fellow under the Connectivity research cluster. Pingkan obtained her Bachelor of Political Science with Honours from Parahyangan Catholic University, majoring in International Relations with a minor in International Organizations & Regimes and completed her tenure as Coordination Intern at Office of the UN Resident Coordinator in Indonesia upon her graduation.