# Data Protection in an Interconnected World

## Dialogue 1 in the Series "Frontiers of Digital Economy"

*Report of discussions of the Expert Round Table on "Data Protection in an Interconnected World"*

*28 June 2021, 0830 – 1030 UTC*

*Via Zoom*

LIRNEasia Solutions
Ideas that fit

LIRNEasia is a pro-poor, pro-market think tank whose mission is *catalyzing policy change through research to improve people's lives in the emerging Asia Pacific by facilitating their use of hard and soft infrastructures through the use of knowledge, information and technology*.

Contact: 12 Balcombe Place, Colombo 00800, Sri Lanka. +94 11 267 1160. info@lirneasia.net
www.lirneasia.net

*The "Frontiers of Digital Economy" series is supported and sponsored by Facebook.*

# Executive Summary

- As we collectively grapple with the COVID-19 pandemic, cross-border data flows have supported trade, businesses, governments, and people all over the world. More than ever before, essential services such as education and healthcare rely on digital tools and internet-based services. Cross-border data flows facilitate all of this.
- Increased data protection legislation in all parts of the world shows that many countries have begun to realize the importance of data protection for users whose data is increasingly being collected and processed online, especially when it comes to protecting privacy.
- The increase in data protection legislation, however, has also brought trends towards data localization laws. Concerns have been expressed that data localization policies could harm the local economies where they are implemented, undermine privacy and freedom of expression, and are bad for consumers.
- Although the EU's GDPR is often cited as an example to follow, it could be too costly for low-to-middle-income countries and low-income countries to emulate when developing data protection frameworks. The adequacy procedure is also quite problematic.
- Regional and international frameworks could be beneficial in allowing foreign and domestic firms to easily move data, provide data security without placing undue restrictions on cross border data transfers, increase domestic employment, and support growth.
- Any regional or international agreement on privacy and/or data protection must strive to be both effective in protecting information and not unduly restrictive to trade. In trade agreements, data protection should be considered as important as any other obligation.

# Introduction

Data protection has risen in salience, partly because the pace of datafication and associated phenomena are increasing at a rapid pace. The coming into effect of the General Data Protection Regulation (GDPR)[1] which asserts extra-territorial jurisdiction has contributed to bringing data protection legislation to the fore, especially in countries that have significant trading relationships with the European Union, including service exports in the form of business process outsourcing. At present, at least three of the BBNMAPS (Bangladesh, Bhutan, Nepal, Maldives, Afghanistan, Pakistan, Sri Lanka) countries have developed draft legislation, with texts from Pakistan and Sri Lanka published online for consultation.[2] The influence of the ongoing data protection discussions in India also cannot be discounted.[3] Likewise, the Cross Border Privacy Rules (CBPR) of the Asia-Pacific Economic Cooperation (APEC), which is a voluntary framework for APEC members, are also relevant,[4] as is the ASEAN Framework on Personal Data Protection.[5]

This is to be expected in an interconnected world, especially in relation to what connects it: data and communication. Not only does data travel easily across borders; notions of what is to be permitted and prohibited also move across borders. When legislation is being drafted on technical subjects and regulation is being considered, it is common for the experiences of others to be examined. Especially in cases such as data protection where extra-territorial jurisdiction is being asserted, the incentives to do so are stronger. One of the key elements of data protection legislation that is being heavily discussed is data localization, whereby some large countries have sought to limit cross-border data flows and make mandatory the local processing and storage of data or subsets thereof.

The concept of data protection has numerous implications. Given the importance of data to the global digital economy, regulation of the flow of data will inevitably impact international trade. Data protection legislation is also important in safeguarding the privacy of individuals whose data is collected by either private or state entities, and in precluding the abuse of personally identifiable information (PII). The debate around data localization includes an important human rights dimension, as some have argued that data localization rules can be

[1] General Data Protection Regulation (GDPR). European Union. 2018. Retrieved on 20 July 2021 from https://gdpr-info.eu/

[2] Draft of Personal Data Protection Bill, Sri Lanka. Retrieved on 20 July 2021 from https://www.icta.lk/icta-assets/uploads/2021/03/Data-protection-Bill.pdf ; Personal Data Protection Bill 2020 Consultation Draft V. 09. 04. 2020, Pakistan. Retrieved on 20 July 2021 from https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pd

[3] The Personal Data Protection Bill, 2019. As Introduced in Lok Sabha. India. Retrieved on 20 July 2021 from http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[4] Gribakov, A. (2019, 3 Jan.) "Cross-Border Privacy Rules in Asia: An Overview." *Lawfare.* Retrieved on 20 July 2021 from https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview

[5] ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): Framework on Personal Data Protection. Adopted in 2016. Retrieved on 20 July 2021 from https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf

used to surveil individuals and limit the freedom of expression by enabling government agencies to gather sensitive data.[6]

To understand how these debates are playing out in and affecting the BBNMAPS, LIRNEasia convened an expert round table discussion on 28 July 2021, 0830 – 1030 UTC, over Zoom. The dialogue consisted of a panel of six invited experts, followed by a round table discussion with invited senior decision makers from the BBNMAPS nations. The discussion followed Chatham House rules, in which participants may communicate the content of the discussion but not attribute comments to any particular person. This report follows the same rules.

The panelists were:

- **Drudeisha Madhub** - Data Protection Commissioner, Prime Minister's Office of the Republic of Mauritius
- **Raina Yeung -** Head of Privacy and Data Policy, Engagement, APAC at Facebook
- **Arthit Suriyawongkul** - Thai Netizen Network - A non-profit working on digital rights and internet freedom in Thailand.
- **Jayantha Fernando** - Chair Drafting Committee Data Protection Bill/Director / Legal Advisor, ICT Agency of Sri Lanka
- **Sami Ahmed** - Policy Advisor of the Leveraging ICT for Growth and Employment of the IT-ITES Industry (LICT-2) Project of the Bangladesh Computer Council, ICT Division.
- **Usama Khilji** - Director, Bolo Bhi - a digital rights non-profit, Pakistan

The panel discussion was moderated by Rohan Samarajiva, founding Chair of LIRNEasia.

The first three speakers based their comments on experience with data protection laws in multiple countries. The second set of speakers discussed the development of data protection laws in Sri Lanka, Bangladesh, and Pakistan.

The invited experts encompassed government regulators, researchers, digital rights advocates, legal experts, and representatives from the private sector, including mobile operators.

This report details the key points of discussion, and at the end offers recommendations on data protection which we hope will be of use to policymakers in the BBNMAPS, especially as they work towards developing their own frameworks and legislations.

[6] Shahbaz, A., Funk, A., Hackl, A. (2020). "Special Report 2020 User Privacy or Cyber Sovereignty? : Assessing the human rights implications of data localization." *Freedom House.* Retrieved on 20 July 2021 from https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty#footnote1_cy1n0z8

# Themes of Discussion

## Data Protection Laws and Frameworks

Many countries have begun to realize the importance of data protection, especially when it comes to protecting privacy. This is illustrated by the increased activity on data protection legislation. In terms of the BBNMAPS, the status of data protection legislation in Sri Lanka, Pakistan, and Bangladesh was discussed. It was posited that Sri Lanka could have tackled the creation of their data protection legislation in two ways: The country could have opted for soft laws such as the OECD framework and the APEC guidelines or they could have opted for a hard approach such as seen with the GDPR. The choice was to meet the middle ground between the two.

In the Sri Lankan draft, data localization rules differ depending on whether the controller is a public authority or not. Restrictions apply only to public authorities. A discussion arose regarding how the Sri Lankan draft bill defines "public authority," as the definition was noted to be quite wide. It was stated that the definition of public authorities has been clarified in relation to previous legislation which carry on the same meaning as in the data protection bill. The Companies Act of 2007, for example, states that a public authority could be a firm, but should be one where the government has more than 50% of shares in. The Right to Information Act also states that public authorities can be state/government authorities, including state-owned companies as defined above.

The latest consultation draft of the Pakistan Personal Data Protection Bill was released in August 2021,[7] and the bill is under consultation. It was noted that there is high demand for the bill, especially from the country's large IT sector. It was opined that the bill does a good job of putting forward the obligations that private companies have in great detail, but there are significant gaps in setting out the obligations of the public sector. Bangladesh is still in the midst of creating the legislation and has not released a public draft yet.

In terms of regional and international frameworks, it was suggested that any international contractual document on privacy and/or data protection should have two important elements to ensure they are effective in protecting data whilst ensuring that global trade does not get damaged. These two ideas are accountability and effective remedy schemes.

The influence of the EU GDPR was also discussed, as some participants noted that the GDPR is often cited as an example to follow. It was observed that the data protection legislation of Mauritius is like the GDPR. Mauritius was also one of the first countries to ratify Convention 108 plus, the only internationally binding instrument for data protection. It was argued that the political willingness to push data protection legislation is low in Thailand. Even though the Parliament of Thailand enacted the Personal Data Protection Act, its enforcement was twice postponed by Parliament in 2019 and 2020. Thailand's data protection legislation shares many features with the GDPR, but there are also some differences.

Critiques of the GDPR were also offered. For example, it was contended that Article 37 of the GDPR, which stipulates the appointment of a data protection officer could be too costly for

[7] The virtual dialogue was held in July 2021, prior to the release of the August 2021 draft. Hence, the latest publicly available draft that was discussed was the version released in April 2020.

LMICs and LICs to emulate when developing data protection frameworks. It was also stated that the adequacy procedure is quite problematic.

## Trade

It was noted that the free flow of data is crucial to the digital economy, and indeed the economy as a whole. Some participants noted that evidence shows that one of the main drivers of GDP and economic growth in Asian countries has been international trade, including the movement of data across borders. It was also noted that data flows were critical in allowing Small and Medium Enterprises (SMEs) to gain access to the global market and to enter into relationships with multinational companies (MNCs), both necessary to survive the COVID-19 pandemic.

In terms of regional and international frameworks, it was suggested that any international contractual agreements on privacy and/or data protection must be both effective in protecting information and not unduly restrictive to trade. The importance of accountability and effective remedy schemes was also noted. In trade agreements, data protection should be considered as important as any other obligation. Furthermore, any such obligations must be properly implemented and fully enforced.

For example, participants highlighted recent efforts to influence the Bangladesh government to implement data protection legislation to ensure foreign firms continue to invest and provide services in the country. An increasing number of startups and SMEs in Bangladesh are reliant on global services, such as Facebook and Amazon, to run their business efficiently and reach customers globally. Further, with a large pool of nearly half a million university graduates every year, local employment is heavily dependent on the establishment of foreign firms in Bangladesh. Some participants highlighted the importance of interoperability of national data protection legislation with regional and international frameworks. This would be crucial to allow foreign and domestic firms to easily move data, provide data security without placing undue restrictions on cross border data transfers, and increase domestic employment.

The rules provided by the GDPR in Articles 44 – 50 regarding the different transfer mechanisms for the transfers of personal data to third countries or international organizations were noted as well:

- Article 44 - General principle for transfers
- Article 45 - Transfers on the basis of an adequacy decision
- Article 46 - Transfers subject to appropriate safeguards
- Article 47 - Binding corporate rules
- Article 48 - Transfers or disclosures not authorised by Union law
- Article 49 - Derogations for specific situations
- Article 50 - International cooperation for the protection of personal data

## Data Localization

Data localization is on the rise in Asia, with new legislation rapidly arising. Several participants highlighted some concerns about data localization, including economic, privacy and human rights issues.

Some participants noted that data localization mandates, and other requirements that would impede or restrict the global free flow of data, may not help solve privacy concerns or grant data sovereignty to the countries. Some suggested that global models like the OECD Privacy Principles are examples of effective approaches that allow cross-border data flow while safeguarding privacy. Some contended that data protection regulations could ensure that privacy protections are tied to the data subject, so that the location of where the data is stored is not determinative. This would mean that localization is not needed for internet users to gain "autonomy" over their data.

It was argued by some that data localization policies could harm the local economies where they are implemented, undermine privacy, and be bad for consumers. There is empirical research that points out a direct correlation between cross-border data transfers and rise in GDP / global trade.[8] This is because they break the free and open structure of the internet, which reduces companies' and consumers' access to valuable communications, business, and data and network management tools, chills innovation, and weakens privacy and data security protections by centralizing data in a more accessible location. From the economic perspective, it was contended that the move to localization is very harmful to Small and Medium Enterprises (SMEs) because it is costly, impedes foreign investment due to burdensome compliance costs, requires the sourcing of internal expertise in establishing the necessary infrastructure, deprives them of access to some SaaS (software as a service), and restricts much needed access to a global digital market. For example, the sale of digital products to other businesses abroad could be hampered by data localization requirements. Studies show that the exchange of data is becoming one of the key drivers of the global economy, with digitally enabled trade worth between $800 billion and $1.5 trillion globally in 2019.[9] Also, segregation of data into sensitive, personal or other data in order to give them special treatment, such as local storage, may not be technically feasible for many businesses, particularly SMEs.

It was observed that as we collectively grapple with the COVID-19 pandemic, cross-border data flows have become dramatically more important for trade, businesses, governments and people all over the world. More than ever before, essential services such as education and healthcare rely on digital tools and internet-based services. Small and medium sized companies and large multinational corporations alike have transitioned to remote work and operations, and people increasingly depend on internet-based communications tools like video calls and messaging to stay connected with family and friends who they can't see in person. Cross-border data flows

[8] For example, see Manyika, J. et al. (2016). "Digital globalization: The new era of global flows." *McKinsey Digital.* Retrieved on 29 September 2021 from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows ; Cory, N. & Dascoli, L. (2021). "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." *Information Technology and Innovation Foundation.* Retrieved on 29 September 2019 from https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[9] Ketels, C. & Bhattacharya, A. (2019), "Global Trade Goes Digital." *BCG.* Retrieved on 29 September 2021 from https://www.bcg.com/publications/2019/global-trade-goes-digital

facilitate all of this.

In terms of individual countries, it was observed that Sri Lanka is taking a two-pronged approach to cross border data transfers and localization in the draft personal data protection bill. The private sector has flexibility to move data freely and store it in other countries, as long as minimum protection standards are fulfilled. Permission does not need to be obtained from the data protection authority. However, Binding Corporate Rules (BCR) are recommended to ensure adequacy of protection. The public sector has less flexibility. The first and main option they have is to simply locate the data within the country. If the public sector entity has gone through an adequacy test with the data protection authority and has sufficient reason to store data in foreign countries, they may do so.

There are plans in Bangladesh to put data localization laws in place, mainly for sensitive and critical personal data. However, this is not yet settled. The government is open for discussion and public consultation is yet to happen. It was stated that Bangladesh has tier 3 and tier 4 data centers for the localization of data. In response to the debate about setting up technology and the practicality of localizing data, it was noted that Bangladesh is proposing to give 5 years to the private sector to develop the necessary technology to separate critical personal data from other types of data. It was also stated that enough time will be given to foreign businesses to set up arrangements in order to process certain types of data in Bangladesh.

The Pakistani government has made it a requirement to hold 'critical personal data' within local data centers, but has postponed defining what comes under this scope in the draft bill.

It was noted that in Thailand, data localization is not a major problem, as long as businesses keep proper records of the movement of data. Confidential government data may have some localization restrictions, but none other than that. Businesses do not need to get permission for cross border data transfer from an authority.

The implications for data security and business continuity were discussed in the context of some countries lacking Tier 4 data centers, which means they lack the facilities to ensure redundancy and safe backups within the national territory. State-of-the-art privacy tools and compliance costs were observed to be expensive, particularly for SMEs. After investing in the capital required for regulatory compliance, companies are often unable to bear the additional cost to update their data management and security systems regularly. These costs could render prices higher for consumers, lower economic output, and put user data at greater risk of breaches. This could particularly pose difficulties for developing economies of the APAC region. The centralization of data storage could also create a "honey-pot" of data, leaving people's data more vulnerable to unauthorized access and cyber-attacks by malicious actors such as criminal hackers and foreign spies.

It was observed that in Mauritius, the country had tier 4 data centers. This makes data even more secure, as hacking attempts and others are usually made redundant by the vast amount of backup features and the "zero single points of failure" system. It was opined that the location for data centers is not too important, especially due to the digital nature of the world, and moreover security is more important.

To move away from localization that may carry costs that exceed benefits, it was suggested that the best starting point may be to work towards regional data protection frameworks, such as the APEC guidelines. Before making policies and laws, it is important to understand how

data is handled in actual practice and how companies do business and use data storage and services. It is also important to not conflate issues such as data protection, national security, management of mis- and disinformation, and lawful access. Each of these are important in and of themselves and deserve to be addressed with solutions that are specifically designed for purpose.

## Human Rights

Data protection is necessary for protecting individual privacy. As an example, it was noted that Article 14 of Pakistan's Constitution speaks of the dignity of people and privacy at home, and there could be a risk of these being violated without adequate data protection in a modern world. If there is a request for data from the government, even if there is harm that could accrue to some third parties, data is usually given to the government because of reasons such as the protection of national security. Pakistan has frequently requested ISPs to provide access to data from CDNs (Content Delivery Networks). When privacy is violated like this, it has a chilling effect on journalists and freedom of expression as a whole. As a result, it was argued that the Pakistani government should make some fundamental changes to the bill.

Data held by public and private companies should be protected and there should be oversight, such as a judicial warrant or transparency rules, to hold governments accountable for unreasonable requests to businesses that violate privacy rights.

Democratic governments should not consider privacy in isolation, but should take into account its intersection with other rights. It is important that the government does not denature data protection by putting it in the same realm as cybersecurity, as cybersecurity may need different approaches to surveillance. Therefore, distinctions should be made.

In terms of what private companies can do to protect the privacy of users, it was observed that some private sector entities, in the absence of binding legislation, may not voluntarily uphold ethical principles related to privacy. However, it was pointed out that some private sector entities did maintain good privacy policies.

# Recommendations

- Data flows and exchanges are vital for international trade. The economic advantages of the freer flow of data are important to the BBNMAPS, especially as these are emerging economies and trade is key to economic growth. However, it was observed that the protection of personally identifiable information must be ensured so that privacy is safeguarded. Both the public and private sectors have roles to play. Some participants noted that while binding legislation may be needed, private sector firms could also step up in terms of adopting Codes of Conduct, Binding Corporate Rules.
- Data security depends on the technical, physical, and administrative controls implemented by the service provider, regardless of where the data is stored. Policymakers should place more weight on ensuring the security of data and business continuity than on data localisation.
- International and regional frameworks should be considered to ensure that the Internet does not balkanize, entrepreneurs can build products that serve everyone, and individuals in all parts of the world can rest assured that their data is subject to robust privacy protections. They will also support emerging economies as they look to innovate, grow, and participate within the IT and digital economy by ensuring alignment with global norms, and reducing unnecessary local and international compliance costs.
- Global models like OECD framework and the APEC Cross-Border Privacy Rules system have been suggested as examples of effective approaches that allow cross-border data flows while safeguarding privacy. It is an open question to what extent these frameworks are cross applicable in different contexts.
- The EU GDPR was seen as a major influence in terms of data protection legislation. However, it was noted that nations that are resource-constrained may face challenges if they were to adopt legislation similar to the GDPR domestically. Further, the reliance on approvals and permits has proven to be inefficient and unworkable in other jurisdictions. For example, under the GDPR, the EU only managed to recognize 13 countries as adequate over the course of 2 years.[10]
- Exemptions in data protection legislation and the circumstances in which they take place must be carefully defined. A strict oversight mechanism is necessary to ensure that the exemptions are not abused.

We hope the above takeaways will be useful for policymakers and those involved in the development of data protection legislation and frameworks in the BBNMAPS.

[10] For example, see European Commission, "Adequacy decisions**:** How the EU determines if a non-EU country has an adequate level of data protection." *European Commission.* Retrieved on 29 September 2021 from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#latest ; Blackmore, N. (2019). "International: Feeling inadequate? The rarity of adequacy decisions in Asia Pacific." Retrieved on 29 September 2019 from available at https://www.dataguidance.com/opinion/international-feeling-inadequate-rarity-adequacy

# Annex: List of Participants

| **Panelists** | |
|---|---|
| Drudeisha Madhub | Data Protection Commissioner, Data Protection Office of Mauritius |
| Usama Khilji | Director, Bolo Bhi |
| Sami Ahmed | Policy Advisor, LICT Project, BCC, ICT Division, Bangladesh |
| Raina Yeung | Head of Privacy and Data Policy, Engagement, APAC, Facebook |
| Arthit Suriyawongkul | Computer Scientist, Thai Netizen Network |
| Jayantha Fernando | General Counsel, ICTA, Sri Lanka |
| **Participants** | |
| Ujjwal Kumar | Policy Analyst & Deputy Head CUTS CCIER |
| Damith Hettihewa | President Computer Society of Sri Lanka/Managing Director Nimbus Cloud Services, Sri Lanka |
| Prasad De Silva | President - Internet Society of Sri Lanka |
| Imesha Dissanayake | Research Associate, the Ceylon Chamber of Commerce. |
| Mr. Hameedullah Sherani | Board of Directors at Afghanistan Telecommunication Regulatory Authority (ATRA). |
| Mr. Ziaullah Karokhel | Sub-Director Data Management, Real Time Data Management System (RTDMS), Afghanistan Telecom Regulatory Authority (ATRA) |
| Ashwini Natesan | Research Fellow- LIRNEasia |
| Chanuka Wattegama | Director (Policy) Information and Communication Technology Agency of Sri Lanka. |
| Abu Saeed Khan | Senior Policy Fellow, LIRNEasia |
| Jahrat Adib Chowdhury | Chief Legal Officer & Company Secretary, Banglalink Digital Communications Ltd. |
| Sangay Zangmo | Market and Competition Division, Bhutan InfoComm & Media Authority |
| Tshering Choden | Sr.ICTO, Market and Competition Division, Bhutan InfoComm & Media Authority |
| Babu Ram Aryal | Chief Executive Officer, Internet Governance Institute |
| Bikram Shrestha | President, Nepal Internat Foundation |
| Sonam Penjor | Department of IT and Telecom, MoIC, Bhutan |
| Muhammad Hayat | Senior Policy Fellow, LIRNEasia |

| | |
|---|---|
| Monsur Quader Faruqui | Data Protection Officer, Grameenphone Limited |
| Dechen Chhoeden | Dy. Chief ICT Officer, BtCIRT, Department of Information Technology & Telecom, Ministry of Information & Communications, Bhutan |
| Dr. Sajeevani Weerasekara | Central Bank of Sri Lanka |