Beyond the Hype: Realising Responsible AI through Data Protection in South and Southeast Asia

A Review of Data Protection Regulations in the age of AI governance

EngageMedia

ACKNOWLEDGEMENTS

Researchers:
Merl Chandana, Research Manager, Data, Algorithms and Policy (DAP), LIRNEasia
Nusrat Aditi Zaman, Programme Coordinator, Digitally Right Limited
Sinta Dewi Rosadi, Associate Professor, Faculty of Law, University of Padjadjaran

Contributors:
Siti Rochmah Aga Desyana, Project Officer, EngageMedia
Prapasiri 'Nan' Suttisom, Project Coordinator, EngageMedia
Debby Kristin, Project Officer (Indonesia), EngageMedia

Editor:
Katerina Francisco, Editorial Coordinator, EngageMedia

Special thanks to the following:
Samik Kharel
Jamael Jacobs, Foundation for Media Alternatives

EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentaries. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights. Learn more at engagemedia.org

Draft Zero* - September 2024

*This report represents a Draft Zero and is intended as a working document. We invite feedback from experts and professionals to refine and strengthen the analysis. Please contact us at info@engagemedia.org for any suggestions or contributions.

Contents

Executive Summary

The adoption of Artificial Intelligence (AI) and Machine Learning (ML) holds great potential to benefit society. However, without careful assessment to ensure these technologies comply with both international norms and national laws, they may bring about unforeseen risks and unintended consequences. As data processing capabilities evolve at an unprecedented rate, core data protection principles may need to be reconsidered to effectively address the emerging challenges. For instance, big data analytics can render traditional notions of consent obsolete, as users typically lack insight into how algorithms function, how their data is utilised, the purposes for which it is processed, and the conclusions drawn by such technology.[1] The deployment of AI systems also presents significant privacy concerns at a societal level, particularly when trained on individuals' data for surveillance purposes.

Given that data is the backbone of Artificial Intelligencel and Machine Learning, this report examines the growing challenges of data protection in South and Southeast Asia as AI governance takes centre stage. Focusing specifically on the data protection laws of Indonesia, the Philippines, Bangladesh, Nepal, and Sri Lanka, the report analyses how well these laws can mitigate potential risks arising from AI adoption.

Key Findings

- **Lack of fundamental, comprehensive regulation to properly protect personal data.** Countries that do not have a comprehensive data protection law in place (Cambodia, Nepal, and Bangladesh) currently use an amalgamation of existing regulations, which – while principally sound – can be outdated and not necessarily accommodative to the current landscape and challenges of digital data collection and processing. We recognize it will require political capital to pursue amendments to these legislative changes; we invite lawmakers to revisit existing legislations to leverage and harmonise the protection framework e.g. consumer protection etc.
- **Vague definitions and parameters of exceptions that override data subject consent for data processing.** From our review, certain existing laws and drafts of Data Protection Regulations (Philippines and Bangladesh) have determined a set of exceptions to override the consent required from data subjects. However, many of these exceptions are not properly defined and can create loopholes for data abuse. Cambodia for example has established that consent can be overridden in the event of

[1] Response To Call For Inputs For The Report On 'the Right To Privacy In The Digital Age, Centre For Communication Governance At National Law University Delhi

a data subject's personal emergency, national interest, or data controller's legitimate interest, the latter being fully determined by the Ministry of Posts and Telecommunications (MPTC).[2] Bangladesh has also regulated that national security and public interest are legitimate exceptions to override data subjects' consent, but did not specify what constitutes such under the regulation and instead leaves it under the discretion of the Data Protection Officer.

- **Insufficient redress mechanisms for data breaches, data abuse, and faulty results of automated decision-making.** Indonesia, the Philippines, and Sri Lanka had outlined some rights for Data Subjects regarding disadvantages caused by the collection and processing of their data. These rights include the right to be informed, to opt out, and in the case of automated processing results, to challenge the final decision made from such processes. However, accountability mechanisms for when data violation does occur remain incomplete, and this is particularly prevalent in scenarios where such violations were done by governments. In Indonesia and Bangladesh, for example, penalties for government violations that cause data breaches and/or unauthorised processing are not governed under the regulations, and no mechanism to access redress has been established as of yet.
- **Independence and transparency of the national data protection bodies.** Many of the countries reviewed in this paper have mandated the creation of National Data Protection Bodies under their Personal Data Protection Regulations. However, the transparency and independence of these National Data Protection Bodies vary; in Bangladesh, the Chairman and members of the Board are to be appointed by the government. Given these ties, it is difficult to assert whether the officer in charge of Data Protection can work independently and transparently, as their position is tied to actors who might also be perpetrators of data breaches and abuse of data.

Key recommendations:

1. **Multi-Stakeholder Dialogue on AI and Data Protection.** A high-level expert/working group/commission is necessary to deliberate and determine how data protection laws should be applied in the context of AI systems and machine learning. This group should consist of all relevant sectors, including law enforcement, data protection experts, private sector operators, NGOs, and academia, to work towards commonly acceptable solutions. These groups should provide recommendations that help form

[2] Article 15 (g) Draft Law on Personal Data Protection Cambodia

policies and laws for data protection concerns,[3] and we can look at the EU High Commission's High-Level Group as a model.

2. **Establish an accountability mechanism to ensure that individuals impacted by AI systems' infringement can access effective remedies.** The accountability mechanism should entail both mitigating measures to contain data breaches and abuse, a minimum requirement of public transparency reports of the violation, and criminal liability for such crimes proven to occur due to malicious intent or wilful negligence. It should also take into account when these violations are perpetrated by government agents or when it reaches a certain scale of damage that is massive and widespread in nature.
3. **Designate a Data Protection Body that is able to operate independently and with transparency.**[4] [5] Principally, a Data Protection Body should have the authority to decide on data abuse cases, provide advisory opinions on the application of personal data regulations, and provide guidelines for various sectors wishing to process personal data within their jurisdiction. Given this immense responsibility and the fact that many data violation cases are perpetrated by government actors,[6] the body should be designed to operate independently from the government and be transparent to the public on their works. This may include selecting members and staff through a merit-based, transparent selection process; not classifying staff and members as part of the Civil Servant schemes; and assigning independent administrative and budgetary autonomy separate from the Presidency or the Republic at large. Brazil's National Data Protection Authority (NDPA) is a good model to emulate.[7]

---

[3] EU High Commission, High-Level Group (HLG) on access to data for effective law enforcement (2024) https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

[4] Greenleaf, G. (2019). Global data privacy laws 2019: 132 national laws & many bills.

[5] Jakarta Post, Why the Personal Data Protection Agency Matters (2023) https://www.thejakartapost.com/opinion/2024/07/08/why-the-personal-data-protection-agency-matters.html

[6] Enriquez, J.M. (2023) Data Security in ASEAN's Digital Economy: Lesson From the Philippines https://www.rsis.edu.sg/rsis-publication/rsis/data-security-in-aseans-digital-economy-lessons-from-the-philippines/ ; Nadarajah, H. *et. al* (2024) Indonesian Government Under Fire Following String of Cyber Breaches https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches ; Nikkei Asia (2023) Huge Bangladesh government data leak hints at other vulnerabilities https://asia.nikkei.com/Economy/Huge-Bangladesh-government-data-leak-hints-at-other-vulnerabilities

[7] DLA Piper, National Data Protection Authority. https://www.dlapiperdataprotection.com

BACKGROUND

This report builds on the findings of EngageMedia's previous report on Governance of Artificial Intelligence (AI) in Southeast Asia (2021) and the report on Biometric and Digital Identification systems in South and Southeast Asia. It will analyse the tensions of Personal Data Protection (PDP) implementation in the adoption of AI systems will allow for a holistic view of potential shortfalls in the existing provisions, enabling policymakers to formulate guardrails ensuring data quality, privacy, ethical use, and transparency in using the collected data for various sectors. The report considers the societal impacts of AI, with a focus on machine learning[8] applications, as it is most relevant to data protection and privacy concerns. Data privacy and security is crucial for Personally Identifiable Data, which can easily slip into the AI's training datasets, where the model can leak sensitive information.[9] Unauthorised access and abuse of personal data can also be exacerbated with AI, which has been linked to concerns about surveillance and monitoring attempts on targeted individuals. There are also data privacy risks specific to the impact of AI Implementation, such as the use of AI to re-identify purposefully anonymised personal data and the bias contained in the pool due to limited data representation.

South and Southeast Asia is a rapidly evolving economic region that requires a rethinking of legal frameworks to ensure they effectively minimise and/or mitigate the harms posed by emerging global digital challenges. Among these concerns is the governance of data, given that nearly all aspects of our existence, from personal information to work details to preferences in social media, have been increasingly digitised into data over the last decade and are used as basis for standardisation, automation, as well as personalisation of digital products and services.[10] With this incredible value placed on our data, there is an increased necessity to govern its privacy to ensure that existing data collection, management, and utilisation practices do not violate digital rights. However, there are also concerns on overregulation, particularly its impact on business innovation. Cambodia, for example, had expressed a preference for a localised "soft-law" approach that is more fitting for the ASEAN

[8] Definition from The Internet Society (2017): "machine learning…instead of giving computers step-by-step instructions to solve a problem, the human programmer gives the computer instructions and rules to learn from the data provided. Based on inferences gained from the data, the computer then generates new rules to provide information and services."
[9] Kurniawan, D. "The Role of Data Governance in The Era of AI" (2024).
[10] Popescu, Andrei-Dragos, "The Value of Data from an Artificial Intelligence Perspective", Annals of the University of Craiova for Journalism, Communication and Management, Vol. 5 (2019), pp. 172 - 194.

context as opposed to GDPR provisions within their jurisdiction given the latter regulation's complexity and rigidity.[11]

Presently, the sub-region is gearing up to legalise and implement privacy laws in the context of digital usage. Out of the seven focused countries of our research on Biometric and Digital Identification systems, three (Indonesia, Philippines, and Sri Lanka) have enacted a stand-alone, unified, digital data protection legislation. Of these three countries, two are still in the early stages of implementing and operationalizing their laws. The remaining three countries – Nepal, Bangladesh, Cambodia, and Maldives – are either in the drafting stages of their law or have not initiated any draft bills. Despite having legal frameworks in place, Singapore (2.7) and the Philippines (2.8) ranked among low-performing countries for personal data protection in a study by Comparitech (2022)[12]

Despite the show of willingness to protect digital personal data, critical elements of key data protection mechanisms are absent, such as accountability mechanisms for data breaches and data abuses. In **Indonesia,** the PDP bill was issued in 2022 and has raised some concerns regarding the levels of accountability between breaches made by the government and private entities. Private violation of the regulation is subjected to criminal charges[13], whereas government violation is not violated at all. **Sri Lanka** had also recently legalised the PDPA in 2022, although the impact of the latter is yet to be fully realised. This transition aims to decentralise data storage and government control but may introduce challenges such as third-party access, authentication records, and real-time surveillance.

Countries in South and Southeast Asia are rapidly advancing their Artificial Intelligence (AI) implementation strategies, with national AI approaches outlined across the region (see Annex). However, the Global Index on Responsible AI (GIRAI) indicates that global progress toward setting guidelines ensuring responsible/ethical use of AI is lagging behind its development and adoption, especially in the Global South. Many countries in the region lack sufficient data privacy safeguards as they implement these emerging technologies. Indonesia, Sri Lanka, Philippines and Bangladesh scored around 50-60 on Data and Infrastructure readiness for adopting AI technology for public service delivery. This shortfall underscores multiple risks and harms, including repeated data breach incidents due to a lack of cybersecurity measures. We observe the region continues to be infested with data breaches at various scales; in the **Philippines,** the Department of Science and Technology

[11] Cambodian Ministry of Industry, Science, Technology & Innovation (MISTI). AI Landscape in Cambodia: Current Status and Future Trends (2023)
[12] Each country was given a score per category based on a number of criteria in data protection. Countries with scores ranging from 2.6-3.0 indicate some safeguards but weakened protections.
[13] Article 67-72 Law No. 27 Year 2022 on Personal Data Protection

confirmed a cyberattack resulting in the compromise of at least 2TB of data, leading to system lockouts. At least 230 public agency servers have been impacted by the recent ransomware cyberattack on **Indonesia's** National Data Center, including the Immigration system. The National Telecommunication Monitoring Center (NTMC) in **Bangladesh** experienced a severe data breach, exposing the centre's vast database to the open web and compromising extensive personal data.

Data Protection, AI, and the Regulatory Gaps

Rapidly, countries like Indonesia, Philippines, Nepal, Sri Lanka, and Bangladesh have released some AI strategies and/or policies that outline what implementation would look like in various sectors of governance, business, and public interest. We find that the development of AI in the examined countries is at various stages depending on each country's interests; however, they commonly share similar concerns of trying to strike a regulatory balance that would allow development while still ensuring the protection of personal data at large.

Most national data protection laws are guided by the Privacy Guidelines first laid out by the OECD in 1980. The deployment of AI may cause tensions with multiple data protection principles outlined. We look at the following aspects:

- **Collection Limitation, Purpose Specification and Use Limitation.** Most data protection laws require that there be a lawful basis for collecting and processing personal data.[14] Purpose Specification and Use Limitation principles dictate that personal data should be collected for specific purposes and only used for those purposes or others that are compatible with the original purpose. AI complicates this notion, as they often necessitate the collection and use of broader datasets, in some cases, AI can enable the re-identification of previously anonymized data through machine learning[15], extending data use well beyond the scope to which individuals initially consented. The modern landscape has also drastically changed the concept of consent: users are often left with no choice but to agree to terms as a condition to access services. The "notice and consent" model needs to be reevaluated in the age of networked privacy and AI.. Experts argue that without clarity on what data is

[14] For example, under the EU's GDPR (Art 6), organisations can gather data under the GDPR is to have one of six lawful bases to gather the data about a data subject: (1) consent; (2) necessary for a contract; (3) necessary to comply with a legal obligation; (4) necessary to protect a person's vital interests; (5) necessary for the public interest; and (6) necessary for legitimate interests and not "overridden by the interests or fundamental rights and freedoms of the data subject.

[15] Zimmer, M. (2020). "But the data is already public": on the ethics of research in Facebook. In The ethics of information technologies (pp. 229-241). Routledge.

collected, how it is processed, and the inherent biases involved, individuals cannot provide meaningful consent.[16]

- **Data Minimisation and Retention Limitation**. Data minimisation requires that no personal data is used than is necessary and the data collected is relevant to the purpose. Retention limitation typically requires that data not be stored for longer than is necessary for the specified purpose. If interpreted narrowly, data minimisation and retention limitation make it difficult to effectively assess and govern AI systems. For example, if certain features such as race and gender are not collected and retained, it becomes nearly impossible to evaluate whether a given AI system is biassed in certain directions.
- **Automated Decision-Making & Redress Mechanisms.** Limits on solely automated decision-making are a significant aspect of some data protection regulations and have direct implications on AI systems which often rely on automation for efficiency and scalability. These limitations stem from concerns about bias and the potential for unfair automated decisions made based on wrong or incomplete data. The EU's GDPR, for example, provides strong protections against profiling and automated decision-making. Automated decision-making is prohibited unless one of three exceptions in Article 22(2) applies. Importantly, the GDPR prevents the use of "legitimate interest" as a legal basis for such processing, restricting when data can be used for profiling. Additionally, as laid out in Article 22(3), individuals have the right to contest automated decisions and seek human intervention. This includes mechanisms for remedy and redress with at least the right to obtain human intervention on the part of the data controller.

In addition, many domestic legal frameworks struggle to draw the line between personal and non-personal data, especially relating to the degree of protection that should be ascribed to these classified data. GDPR itself cannot provide a definitive list of what personal data entails and opts to give a definition, as application differs case-by-case and are highly dependent on the context in which it's collected.[17] The boundaries have become increasingly blurred due to the correlations and inferences that can be drawn from combining different datasets. AI complicates this issue further by requiring more and varied types of data to function effectively, and by using powerful computational tools that can combine data in ways that make it possible to identify individuals, even from non-personal data. The complexity deepens because AI often performs better when more data is collected about

[16] Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679.
[17] Irwin, Luke. (2024). GDPR: What Exactly Is Personal Data?. IT Governance European. https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

individuals, even if those individuals don't need to be identified. For instance, AI might require personal health data to predict heart attacks in the elderly, but identifying specific individuals is unnecessary—and not being able to collect such data could introduce bias and degrade the AI system's overall performance.

The rapid pace of AI development also raises unique concerns that existing data protection regulations often fail to fully address. For example, the need to address algorithmic bias is not explicitly tackled in most data protection regulations.[18] Additionally, although the EU's GDPR includes a right to an explanation, this may be insufficient for complex AI systems and isn't a universal feature in data protection laws worldwide. AI also poses privacy risks for individuals belonging to groups who may never have directly shared their personal data yet their information may be indirectly captured and revealed by AI systems, such as indigenous populations.[19]

Currently, governments are engaging in discussions regarding the integration of AI into their jurisdictions. In places where these conversations are lagging, the private sector has taken the lead to self-regulate, conceptualise, and guide the development of industry standards, particularly for business streamlining and, to a lesser extent, public services.[20] This situation presents a significant challenge, as the private sector's focus on business use cases often overshadows the potential and needs of AI for public benefit. Consequently, governments, especially those in the Global South will face an uphill battle in developing their own legislation to leverage AI effectively for public services.

Scope and Methodology

This report examines the data protection laws of five specific countries in South and Southeast Asia: Indonesia, the Philippines, Bangladesh, Nepal, and Sri Lanka. It assesses these laws in the context of growing AI adoption, analysing their ability to mitigate the unique risks AI systems can pose to personal data. The report utilises a qualitative approach, primarily reviewing and analysing existing literature, legal documents like data protection bills and existing legislation, and policy documents, such as national AI strategies (from 2018-2024) and circulars on data protection.

---

[18] King, J., & Meinhardt, C. (2024). Policy Provocations for a Data-Centric World. Stanford University. https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

[19] Majeed, A., Khan, S., & Hwang, S. O. (2022). Group Privacy: An Underrated but Worth Studying Research Problem in the Era of Artificial Intelligence and Big Data. Electronics, 11(9), 1449. https://www.mdpi.com/2079-9292/11/9/1449

[20] Amba Kak and Sarah Myers West, "AI Now 2023 Landscape: Confronting Tech Power", AI Now Institute, April 11, 2023, https://ainowinstitute.org/2023-landscape.

Southeast Asia

Indonesia

Sinta Dewi Rosadi

Background to the Personal Data Protection Regulation in Indonesia

Indonesia upholds and safeguards the right to privacy and the protection of personal information as stipulated in Article 28G verse 1 of the 1945 Constitution of the Republic of Indonesia. Indonesia's data protection is governed by Law No.27/2022 on Personal Data Protection, or known as UU PDP, which applies to every person, public body, and international organisation that carries out legal actions as regulated in this law.

Another law that is crucial in governing individual data is Law No. 8/2011 on Electronic Information and Transactions, better known as UU ITE. While it is not limited to personal data, it established the general norms for data collection and data use.

- **Definition of Personal Data.** In its official legal explanation, UU ITE regulated that the protection of personal data is part of the larger privacy rights, which was defined as an individual's rights to monitor their personal data and to be free of disturbances and/or surveillance.[21] UU PDP defined personal data as an identifiable personal information, directly or indirectly, filed through electronic or non-electronic systems. It further links the right to personal data protection to a larger constitutional right for welfare and social security under Article 28H and Article 28J of the Constitution. Indonesian definition protects privacy by linking it to constitutional rights, emphasizing its significance for individuals and society.
- **Purpose Specification & Use Limitation.** UU ITE specified that usage of personal data must obtain prior consent from data subjects. Such obligation is once again reiterated in Article 20 of UU PDP. It stated the obligations of data controllers, one of which is to acquire **consent** from data owners upon the collection and processing of their personal data.
- **Data minimisation & retention limitation**. UU PDP classified personal data into two major categories: specific–which typically contains more sensitive, inalterable data such as biometrics–and general.[22] Security and privacy obligations vary for these categories, with specific data having stricter requirements. UU PDP also obliges the Data Controller to inform data subjects on the duration for retention of said subject's

[21] Legal Explanation, Article 26 Verse 1 Undang Undang Informasi dan Transaksi Elektronik (UU ITE)
[22] Article 4 verse 1&2 Undang-Undang Perlindungan Data Pribadi (UU PDP)

personal data,[23] and to delete personal data once the retention period is over and/or requested by the data subject.[24] Given that this regulation will only take effect this October, however, it remains to be seen how these provisions will be enacted.

- **Automated decision-making**
  Law No. 8/2011 on Information and Electronic Transaction (UU ITE), Article 1 number 8 defines electronic agent as an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by Persons. Electronic agents still fall under the provision of electronic systems, which is defined as "an electronic system is a set of electronic devices and procedures that serve to prepare, collect, process, analyse, store, display, announce, send, and/or disseminate Electronic Information."[25] However, under its Article 10(1), UU PDP explicitly mentions automated decision-making and acknowledges the right of personal data subjects to "file an objection to decision-making acts based solely on automated processing, including profiling, which give rise to legal consequences or have a significant impact on the Personal Data Subject".[26] Despite both regulations using different terminologies, the term automated processing still correlates with 'electronic agent'.[27]
- **Breach and data abuse accountability**
  The person/public body/organisation processing personal data to generate various outputs based on its purposes, are classified as "Data Controller",[28] and is responsible for protecting and ensuring the data that they process are subjected to proper systems.[29] In the event of a data breach and failure of personal data protection, the Data Controller is obliged to inform the details of such failure to Data Subjects and the Institution. However, full criminal accountability mechanism only exists for those who performed a deliberate act with intent to breach and/or abuse personal data[30] and breach due to negligence is only subjected to administrative sanction with unclear redress mechanism.[31] The regulation also does not govern accountability mechanisms when breach and abuse is conducted by / under the jurisdiction of a government agent.

[23] Article 21 verse 1(d) Undang-Undang Perlindungan Data Pribadi (UU PDP)
[24] Article 16 verse 2(g) Undang-Undang Perlindungan Data Pribadi (UU PDP)
[25] Article 1 number 5 UU ITE
[26] Article 10 verse 1 Undang-Undang Perlindungan Data Pribadi (UU PDP)
[27] Enni Soerjati, "Urgensi Pengaturan mengenai Artificial Intelligence pada Sektor Bisnis Daring dalam Masa Pandemi Covid-19 di Indonesia", Jurnal Bina Mulia Hukum, Vol. 6, No. 2, 2022.
[28] Article 1 verse 4 UU PDP
[29] Article 35 UU PDP
[30] Article 67 UU PDP
[31] Article 47 UU PDP

Indonesia presently does not have a Data Protection Body operating within its jurisdictions, despite such a body being mandated by UU PDP. The MOCI had only recently expressed intent to form the Body.[32] As of now, cases of high-level data breaches and abuse such as the National Data Center infiltration and the PeduliLindungi data-leak have not been publicly investigated or prosecuted, with nobody being held accountable.

AI Policy Development in Indonesia

In 2020, Indonesia launched the Indonesian National Strategy on Artificial Intelligence (Stranas KA), mandating the Ministry of Communication and Informatics (MOCI) to develop ethical guidelines for AI. In December 2023 it introduced the Circular Letter from the Minister of Communication and Informatics No. 9 Year 2023 to develop responsible AI regulations and enforce existing rules while passing new laws related to AI. Under the circular, AI is defined as "a form of programming on a computer device that is part of a larger data processing system."

To date, Indonesia has yet to establish dedicated legislation pertaining to the adoption of AI. Presently, data processing systems which incorporate AI are considered as an 'electronic agent' under UU ITE,[33] and those who process data using AI are also classified under the "Data Controller" category and have to adhere under UU PDP.[34]

Recommendations

For the Government, including the Parliament, Ministry of Information and Telecommunication, and Law Enforcement, we recommend the following:

1. **Ensure AI system compliance with existing law (PDP, Consumer Protection Law) as the guardrails for emerging tech deployment.** As existing regulations have covered the general purposes, mechanisms, and actors of AI systems, it is important to produce an official interpretation of how UU PDP and UU ITE apply to the existing use of AI systems in Personal Data processing context in order to ensure compliance of AI systems to these aforementioned regulations. Another follow-up letter to Circular Letter from the Minister of Communication and Informatics No. 9 Year 2023 can outline the interpretations that would be applicable, including how such compliance would look like in the context of AI.

[32] CNN Indonesia (2024), Kominfo Sebut Lembaga Pengawas PDP Bakal Dibentuk,
[33] Pg. 3 Circular Letter No. 9/2023.
[34] Pg. 7 Circular Letter No. 9/2023.

2. **Clarify access to remedy and litigation pathway for abuse of personal data,** including faulty results of automated decisions and data breaches. Article 10 maintains the right to file an objection to the result, but the guarantee for remedies to the damage and protection for the victim remains unclear. Solidifying such guarantees under the Law's derivative regulations (RPP) would empower affected entities to pursue legal means in seeking justice. Additionally, litigation pathways should also be outlined for abuses made intentionally and due to negligence.
3. **Commend Private Sectors for creating their respective internal redress mechanism.** This can be made via a derivative regulation or a ministerial instruction, and may include appointing a Data Protection Officer, setting up a complaints and reporting channel for customers, and outlining a clear pathway and timeline for redress mechanisms. Private sectors requesting to directly access and process their customer base personal data should be required to have such a mechanism in place prior to getting their licence approved by the Electronic System Controller under the MOCI.

Philippines

Sinta Dewi Rosadi, with Editorial Contribution from Jamael Jacobs

Background to the Personal Data Protection Regulation in The Philippines

In the Philippines, Republic Act No. 10173, officially known as the Data Privacy Act of 2012 (DPA), is the country's primary data protection legislation. The law established the National Privacy Commission (NPC), which is charged with its implementation, including the issuance of supplementary policies, the investigation of violations of the law, and the giving of advice on all matters relating to the protection of personal data.[35]

- **Definition of Personal Data**
  Under DPA, personal information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information. It can also refer to information that, when put together with other information, would directly and certainly identify a specific individual.[36]

[35] National Privacy Commission, "Powers & Functions", https://privacy.gov.ph/powers-functions/, [retrieved on 28/07/2024]
[36] Chapter 1 Section 3 Definition of Terms Republic Act 10173 Data Privacy Act Of 2012

- **Purpose Specification & Use Limitation**
  General data privacy principles—such as transparency, legitimate purpose, and proportionality—are laid out in Section 11 of the law.[37] The processing of personal data, except in certain instances, must adhere to these principles and comply with the other requirements of the law.
- **Data minimisation & retention limitation**
  The DPA categorises personal data between personal information, sensitive personal information, and privileged information. The processing of the first may be justified by any of the criteria listed under Section 12 of the law. Meanwhile, the processing of the second and third categories may rely on any of the grounds provided under Section 13. The distinction is critical because in the case of sensitive personal information and privileged information: (1) more stringent conditions must be complied with before they can be processed; (2) a higher level of security must be adopted by controllers and processors; and (3) heavier penalties are generally imposed on violators when they are involved.[38]
- **Automated decision-making**
  Under the DPA, there is no provision that specifically regulates the use of an automated system. However, under Section 16 of the law, among the information Data Subjects have the right to be given access to is "information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject".[39] This is reinforced under the law's implementing rules where additional provisions make reference to automated decision-making. For instance, Data Subjects are already given the right to be informed upfront if their personal data will be subjected to automated decision-making. They also have the right to object to the processing of his or her personal data using automated processes in limited circumstances.[40] Controllers are also duty-bound to notify the NPC if they adopt or make use of automated decision-making systems.
  This latter directive is emphasised anew in a subsequent issuance of the NPC (i.e., NPC Circular No. 2022-04) that establishes a definition for automated decision-making process[41] registration system for data processing systems

[37] Section 12 (a) Criteria for Lawful Processing of Personal Information Data Privacy Act Of 2012
[38] Section 11 Republic Act 10173 Data Privacy Act Of 2012
[39] Section 16 Republic Act 10173 Data Privacy Act Of 2012
[40] NPC Advisory No. 2021 - 01 on Data Subjects Rights.
[41] Section 2(A) NPC Circular No.2022-04: ""Automated Decision-making" refers to a wholly or partially automated processing operation that can make decisions using technological means totally independent of human intervention; automated decision-making often involves profiling."

maintained by various covered entities.[42] This mechanism has potential counterparts in other jurisdictions like Indonesia, where an electronic agent and/or electronic system is also needed to register under the Ministry of Communication and Technology.[43]

- **Breach and data abuse accountability**
  Chapter VIII of the PDPA governs criminal liabilities and restitution mechanisms for unauthorised access, processing, improper disposal, malicious disclosures and intentional breaches of Personal Information and Sensitive Personal Information. It differentiates scales and perpetrators of the crime, with crimes committed by Public Officers being more severe in penalty.[44]
  Circular no. 2023-05 introduced the concept of Philippine Privacy Mark Certification (PMC) Program, a voluntary certification process that assesses public and private organisations that implement data privacy and protection management systems using ISO/IEC standards.[45] The system is currently being developed in collaboration with Concept and Information Group, Inc.

AI Policy Development in The Philippines

After the release of its National Artificial Intelligence Strategy Roadmap (NAIS) in 2021, the government of the Philippines is looking into updating the NAIS in accordance with recent developments of various AI systems. The update is said to be completed by late 2024.

At present, there are no specific provisions that regulate the use of automated systems for processing data. However, the deployment of an AI system and the activities this entails may still fall within the scope of the DPA, particularly when personal data is involved. It may qualify as processing of personal data, which Section 3(j) of the DPA defines as 'any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data'.[46] Accordingly, an entity that operates an AI system that makes use of personal data must still comply with all the obligations imposed by the law. Given this, the NPC has released several circulars addressing how AI—classified as PDPS—are to adhere to the DPA. A data processing system under DPA is therefore to be registered with the Commission and is encouraged to partake in the PMC

[42] Section 5 NPC Circular No.2022-04
[43] Indonesia Government Regulation No. 71/2019
[44] Section 35 PDPA
[45] NPC Circular 2023 - 05 on Compliance to PIP and PICs
[46] Chapter 1, Section 3 DPA

Program. Overall, though, the Philippines' approach remains focused on general data protection principles, with AI-specific guidelines still yet to be developed.

Recommendations

1. **NPC to provide Advisory that address data subjects' right to challenge the results of faulty automatic decision-making processes.** Previous advisories had established the right of data subjects to be informed and the right to refuse automated processing of their data.[47] However, as many individuals might not possess the full extent of knowledge on the impact of automated decision-making until a decision has been made that disadvantages them, the NPC should also establish the right to challenge its faulty results that give rise to legal consequences and material loss.[48] This right should include a clearly outlined redress mechanism and protection from being subjected to countersuit during their pursuit of justice.
2. **NPC to provide Circular on PDPA applicability and compliance for AI systems processing personal data.** Presently, existing Advisory Opinion have established that AI is compatible with existing DPA regulations,[49] and should adhere to the NPC's Advisories on Privacy Impact Assessment & Data Subjects Rights in order to ensure compliance with the DPA.[50] To further outline the applicable provisions under the PDPA for data processors that employ AI systems in their chain, the NPC should provide a circular that specifies the specific compliance needs for AI Systems wishing to operate within the Philippine's jurisdiction.

[47] NPC Advisory Opinion No. 2024 - 04.
https://privacy.gov.ph/wp-content/uploads/2024/01/Advisory-Opinion-No.-2024-002.pdf
[48] Wachter, Sandra, *et. al.* Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (2016).
https://www.researchgate.net/publication/312597416_Why_a_Right_to_Explanation_of_Automated_Decision-Making_Does_Not_Exist_in_the_General_Data_Protection_Regulation
[49] NPC Advisory Opinion No. 2024 - 002
[50] *Ibid.*

South Asia

Sri Lanka

Merl Syrex Chandana

Background to the Sri Lankan PDPA

The Personal Data Protection Act (PDPA) No. 9 of 2022 serves as the primary legislation overseeing the safeguarding of personal data in Sri Lanka. It marks a significant advancement in the country's data protection framework and has direct implications for AI development.

- **Definition of personal data.** Section 56 of the PDPA defines personal data broadly, covering any information that identifies an individual directly or indirectly. This includes direct identifiers such as names, online identifiers, identification numbers etc. and indirect factors specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of an individual. However, as explained above, challenges in its application to AI exist because the distinction between personal and non-personal data becomes blurred when AI systems combine datasets.
- **Purpose specification and use limitation.** The PDPA requires that personal data be processed lawfully based on consent, contractual or legal obligation, emergencies, public interest, or legitimate interest, and restricts further processing incompatible with the original purposes. This conflicts with typical AI practices, where it is often challenging to anticipate all potential use cases at the time of collection, or the data needed for specified use cases.
- **Data minimisation and retention limitation**. The PDPA also has clauses that require proportionate processing of data (data minimisation) and obligations to limit the period of retention. If interpreted narrowly, data minimisation and retention limitation make it difficult to effectively assess and govern AI systems for aspects such as bias and fairness.
- **Automated decision-making & redress mechanisms**. Section 18 of the PDPA places restrictions on automated decision-making, though these are less stringent than those in the EU's GDPR. Notably, the PDPA does not prohibit automated decisions outright. While it does not grant individuals the right to direct human intervention by the data controller as a redress mechanism, it does allow them to request a review of such decisions and seek the erasure of their data if its use infringes on their rights. Additionally, Section 18(2) requires that, in cases of automated decision-making, the

data controller must follow measures and criteria to be specified by the Data Protection Authority to safeguard the rights and freedoms of data subjects.

AI Policy Development in Sri Lanka

Despite the existence of a globally-recognized IT-BPM industry, AI adoption is not widespread in Sri Lanka. It ranked 95th (out of 193 countries) in the 2023 Government AI Readiness Index by Oxford Insights.[51] In April 2024, Sri Lanka released a white paper titled "Artificial Intelligence in Sri Lanka" as a precursor to a five-year National AI Strategy. The paper acknowledges the country's early stages of AI adoption in both the private and public sectors and outlines a potential roadmap, with a National Data Strategy recommended as the first critical step. Although it doesn't specifically address data protection concerns in AI development, the white paper emphasises the need to "Create a Safe and Trustworthy AI Ecosystem for Sri Lanka," prioritising the protection of individual rights and freedoms while ensuring alignment with the existing constitutional framework.

Recommendations

At the time of writing, Sri Lanka's digital policy landscape is uncertain, with upcoming presidential and parliamentary elections potentially leading to changes in existing policies. The Sri Lankan Data Protection Authority (DPA) is currently finalising the implementation of its mandate, with key initiatives planned for late 2024 and early 2025.[52] Meanwhile, new national digital strategies are taking shape: a national digital strategy impacting AI was introduced earlier this year, as well as the National Strategy for AI, following the release of the white paper. Another key proposal under discussion is the establishment of a National Center for AI (NCAI) within a new Digital Transformation Agency (DTA), which will replace the current Information Communication Technology Agency (ICTA) with an expanded scope. Such policy uncertainties withstanding, the crux of the following recommendations for Sri Lankan legislators and policymakers should remain relevant.

1. **Provide necessary interpretations, additional guidance, to address points of tension and ambiguity surrounding data protection and AI**. For example, within the

[51] Hankins, E., Nettel, P.F., Martinescu, L., Grau, G., & Rahim Sulamaan (2023). Government AI Readiness Index 2023. Oxford Insights. https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-1.pdf

[52] President's Media Division, Sri Lanka (2024). Sri Lanka Data Protection Authority Moves towards Finalizing Regulations to Safeguard Citizens' Rights in Personal Data Handling. https://pmd.gov.lk/news/sri-lanka-data-protection-authority-moves-towards-finalizing-regulations-to-safeguard-citizens-rights-in-personal-data-handling/

context of AI development and adoption, it's important to clarify what constitutes "original purposes," provide detailed guidance on what qualifies as "legitimate interest," and interpret the principle of retention limitation when personal data is used for AI. While interpretations don't have the same legal force as legislation or regulations, they are crucial for data protection authorities to keep pace with the rapid evolution of AI as evidenced by the many guidelines on the application of GDPR to AI offered by the European Data Protection Board (EDPB). Further, as specified in the PDPA under Section 18 (2), it is recommended that the Data Protection Agency (DPA) considers the emerging risks of AI on personal data protection and provide additional guidance to safeguard the rights and freedoms of data subjects in cases of automated decision making.

2. **Build DPA capacity on AI.** Data Protection Agencies (DPAs) are generally skilled in data computing and fundamental rights, but to effectively manage AI-related risks, it's recommended to enhance the Sri Lankan DPA's expertise in AI technologies. Building this capacity will also be beneficial if Sri Lanka introduces AI-specific regulations, similar to the EU, where several DPAs are positioning themselves as key enforcers of AI regulations.[53]
3. **Help reduce compliance costs for the private sector.** As private sector companies increasingly adopt AI applications that use personal data, it's recommended that the DPA collaborate with the proposed National AI Center and domain experts to clarify how the existing PDPA applies to AI. Additionally, the DPA should simplify compliance requirements and offer tools, such as templates and automated solutions, to reduce the burden on businesses.

A key proposed initiative of the National Strategy for AI is developing an AI Governance Framework for Sri Lanka to manage AI-related risks. As a broad recommendation it is suggested that the complex relationship between AI, data protection, and individual risks be thoroughly examined during this process, with input from experts and representatives of strategic sectors targeted in the national AI strategy.

[53] European Data Protection Board (2024). Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework.
https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

Nepal

Merl Syrex Chandana

Background to the Data Protection Legal Framework for Nepal

Nepal's legal system, shaped by its history of monarchy and transition to a federal republic, has seen reforms to address data protection challenges. However, privacy and data protection-related laws are in the early stages of development in Nepal. Historically, data protection was governed by various laws, including the Muluki Ain (National Code), the Telecommunications Act, and the Right to Information Act. Nepal currently lacks unified data protection legislation.[54] The Data Act which came into force on October 13, 2022, was intended to consolidate laws related to data collection and improve the reliability, organisation, and timeliness of data production, processing, storage, publication, and distribution. However, the Data Act has provided limited clarity on data protection issues and lacks comprehensive provisions for data collection, processing, storage, and privacy, making it insufficient to address the protection of personal data, especially digital personal data stored and processed by electronic means.[55] It mainly focuses on regulating data collected by government and public entities for official purposes rather than addressing broader data privacy concerns. The Individual Privacy Act (2018) and the accompanying Privacy Regulation (2020), along with the Data Act, are considered the primary data protection legislation in Nepal.[56]

- **Definition of personal data.** The Privacy Act defines "personal data" as information associated with an identifiable individual, covering a wide range of details, including caste, ethnicity, birth, origin, religion, health, education, address, and more. Chapter 9 of the Privacy Act governs privacy protections concerning electronic means, encompassing all forms of personal information, documents, correspondence, and data in electronic format. Meanwhile, Chapter 1 provides for the protection and privacy of personal information, explicitly covering biometric data such as thumb impressions, fingerprints, retinal scans, and other identifiers. However, unlike other data protection regulations, it lacks explicit reference to direct and indirect identifiers, and it is comparatively narrow against other Data Protection Regulations in the region.[57] There is a possibility that attributes not covered in the "personal data"

[54] Chaudary, N. (2023) The Need for data protection law in Nepal https://kslreview.org/index.php/kslr/article/view/2225
[55] The Kathmandu Post (2023) Data Vulnerability in Nepal https://kathmandupost.com/columns/2023/10/18/data-vulnerability-in-nepal
[56] Pradhan, D. (2024) Nepal - Data Protection Overview. Data Guidance. https://www.dataguidance.com/notes/nepal-data-protection-overview
[57] Gautam, U. *et. al* (2022) Right to Privacy, its Migration and Evolution in Nepal, p. 159

might still make it possible to identify an individual, not to mention the blurry distinction between personal and non-personal data when AI systems combine datasets, potentially identifying individuals even from data not initially considered personal.[58]

- **Purpose specification & use limitation.** Rule 11 of the Privacy Regulation provides that unless otherwise provided in other prevailing laws, the personal data of a person collected in accordance with the Privacy Act and the Privacy Regulation shall only be used for the purposes for which it has been collected. Section 13(3) of the Data Act also provides such protection. The bases for collecting and processing data include consent, contractual or legal obligations, vital interests, and public interest. However, the applicable laws do not provide for a specific provision whereby personal data or information may be collected, stored, or processed for the legitimate interest of the data controller. Without "legitimate interest" as a legal basis, companies and organisations in Nepal face a more stringent standard for processing personal data for AI, as they must rely on other grounds, such as consent or legal obligation, to justify data processing. Even when it comes to public interest, it is often challenging to anticipate all potential use cases at the time of collection and it might make AI development for use cases with public benefit particularly challenging.
- **Data minimisation & retention limitation.** The Privacy Act and the Privacy Regulation lack specific procedures or time frames for data retention and do not explicitly address data minimisation or the collection of data proportionate to its intended purpose. While this absence of strict guidelines might offer flexibility, it also raises concerns about the long-term storage of unnecessary or outdated data, which could increase the risk of data breaches and unauthorised access, ultimately undermining public trust in AI systems.
- **Automated decision-making & redress mechanisms**. Neither the Privacy Act nor the Privacy Regulation nor the Data Act provides provisions relating to the right not to be subject to automated decision-making. As such, there are no corresponding redress mechanisms that specifically address AI or automated decision-making systems. Such provisions encourage the development of more ethical and transparent AI systems, fostering public trust and acceptance.

AI Policy Development in Nepal

Nepal is still in the early stages of AI development and readiness as evidenced by its 150th ranking (out of 193 countries) in the 2023 Government AI Readiness Index by Oxford

[58] Svensen, M.K. (2020) Reidentifying Anonymised Data Using Machine Learning p.13 https://home.simula.no/~paalh/students/MartinKSvensen-master.pdf

Insights[4]. In 2019 the Nepal government drafted the "Digital Nepal Framework" to support the advancement of ICT in Nepal which touched upon AI and emerging technologies. The initiatives in the framework included digitisation and development of policies for data security, data protection, and online privacy.

The Government of Nepal recently prepared a concept paper on the use and practice of Artificial Intelligence.[59] Observers of Nepal's data governance landscape have noted that the country has not yet fully addressed ambiguities or established comprehensive provisions for data collection, processing, storage, publication, and privacy.[60] As Nepal seeks to harness the benefits of artificial intelligence, it is crucial that this occurs in an environment of trust, privacy, and security. Recognizing this, the recently published concept paper for AI identifies the "absence of regulatory and legal frameworks for data security and privacy" as a key challenge and has proposed a "data protection framework" as a future direction. The Framework also considers AI development, it stresses 'benchmarking' the data protection regulations in accordance with international norms and standards. Additionally, the concept paper proposes a National Strategy for AI, with emphasis on Ethics, Data Privacy, Security and Regulations.

It is crucial to assess risks to individuals and the interplay between AI and data protection as Nepal builds on its recent concept paper. This assessment should guide a broader approach to responsible AI governance for Nepal, using tools such as the Global Index on Responsible AI. Strategic partnerships can also help Nepal adapt global best practices in data and AI governance.

Recommendations

1. **Continue efforts in materialising the Data Protection Framework.** In addition to addressing broader concerns like comprehensive protections for data collection, processing, storage, publication, and privacy. Policy makers should also take in consideration AI-specific risks by broadening the legal framework to align with international standards.
2. **Continue building on the sector-specific guidelines on data protection and responsible AI for key sectors and industries**. As laid out by the AI concept paper, given the relatively low AI penetration in Nepal, this approach may be beneficial by

[59] Samiti, R.S., (2024). Concept Paper on AI prepared for the first time in Nepal. The Himalayan. https://thehimalayantimes.com/science-and-tech/concept-paper-on-ai-prepared-for-first-time-in-nepal

[60] Pradhan, D. (2024) Nepal - Data Protection Overview. Data Guidance. https://www.dataguidance.com/notes/nepal-data-protection-overview

educating stakeholders on AI-related risks in a concrete manner, encouraging early engagement, and offering flexibility for adaptation. These guidelines could help mitigate risks, including those not typically covered by data protection regulations, provide a regulatory roadmap, and promote responsible AI adoption by highlighting best practices. The AI concept note recently introduced by the Nepal government also aligns with the need for sector-specific regulatory frameworks, as they specifically said that "it's essential to create sectoral regulatory frameworks for user privacy, security, and effective AI use. It would be appropriate for sectoral ministries, departments, and agencies to prepare guidelines and procedures tailored to their unique needs." Introducing such guidelines would then allow sectors to utilise AI with proper guardrails and develop respective measures to Data protection in accordance to their situation and needs, based on the minimum standards posited by the guideline.

Bangladesh

Nusrat Aditi Zaman

Background to the Data Protection Legal Framework for Bangladesh

Following several severe data breach incidents,[61] Bangladesh had initially introduced the Data Protection Bill in 2022. Since its introduction, it has received some heavy backlash due to its concerning provisions[62] and has undergone several amendments. By 2024, the Bill has been renamed to Personal Data Protection Act, 2023, along with a number of other changes in the provisions. However, concerns that the Act will be used as a tool for surveillance, extending more protection to the government rather than the people, still remain.[63] As of now, the legislation is still in the draft stage.

- **Definition of personal data.** The PDPA, 2023, defines "personal data" as any data regarding an individual that can be used to identify the individual except for pseudonymized, or encrypted data. The exclusion of pseudonymized data in particular from the ambit of personal data could be a cause of concern because the data subject can easily be identified from that data with the addition of the supplementary information which had been replaced as a security measure. With the vast areas of AI application being envisioned in Bangladesh and in turn the vast amount of data that will be handled by AI, there really is no guarantee that a data subject will not be identified from pseudonymized data.
- **Purpose Specification & Use Limitation.** The PDPA, if passed, will be applicable to the processing, collection, use, retention, and distribution of an individual's data within Bangladesh and outside Bangladesh if the data relates to a citizen of Bangladesh. Under section 7 and 15 of the Act, the consent of the data subject must be taken before any personal data is collected or processed and that consent can be revocable. The Act also distinguishes between personal data and sensitive personal data, which includes health, genetic and biometric data as well as data regarding any offence or criminal proceedings against someone. Explicit consent of the data subject is also required for the processing of sensitive data and it can only be done

[61] Nikkei Asia, Huge Bangladesh government data leak hints at other vulnerabilities (2023) https://asia.nikkei.com/Economy/Huge-Bangladesh-government-data-leak-hints-at-other-vulnerabilities

[62] The Daily Star, Data Localisation and Data Protection in Bangladesh: A Review (2024) https://www.thedailystar.net/law-our-rights/news/data-localisation-and-data-protection-bangladesh-review-3528661

[63] Transparency International Bangladesh, The Illusion of Personal Data Protection: Examining Surveillance, Supervision, and Suppression (2023) https://ti-bangladesh.org/articles/story/6700

under certain circumstances provided under Section 11 of the Act. However, the provision for both personal and sensitive personal data is that both data can be processed without consent of the data-subject if the processing becomes necessary for a number of reasons including public or vital interest, legal obligations, medical emergencies etc. This draft Act legalises the unfettered access to any data for national security, provides vast exemptions that override consent revocations of the data subjects for the sake of public interest, and mandates the localisation of data if said data is considered classified data. However, for all three of these provisions, what the draft does not do is set any criteria or parameters to define national security, public interest, or classified data. This means that the government has the discretion to declare any situation a matter of national security or public interest and any data as 'classified data'.

- **Data minimisation & retention limitation.** As per Section 25 of the Act, processed data will not be kept longer than it has been directed in the Rule for the fulfilment of the purpose the data was processed for and it will be the responsibility of the data fiduciary to erase the data once its purpose has been fulfilled. Chapter 2 of the legislation also has a set of principles to ensure the protection of data and one of the principles also requires data to be destroyed permanently at the end of the period authorised in the Rules. The Rules associated with this legislation are yet to be released, so it is hard to say what the authorised period for retention of data is going to be.
- **Automated decision-making.** The PDPA does not have any specific provisions on automated decision-making but it does define "processing" as any operation or set of operations which is performed on data or on sets of data, whether or not by automated means. The Draft AI Policy also intends to use AI to produce automated reporting in the financial sector. However, neither the Act nor the Policy defines what "automated" means.
- **Data breach/abuse accountability & Redress Mechanism.** The Draft Act sets down a complaint mechanism if any person violates any provision under this Act. The complaint has to be filed to the Data Protection Board by either the data subject himself or any other person who believes that a data controller, data processor or data collector has violated any of the rights given under this Act; however, for such violations, the Act only imposes administrative fines of varying range. For instance, the Draft will impose administrative fines for illegal processing of personal data, failure to adopt necessary data security measures, failure to comply with orders made under this Act, collecting, disclosing, transferring or selling of personal data that can cause harm to the data-subject, or for the violation of any other provision of this Act.

AI Development in Bangladesh

Bangladesh has very recently introduced the Draft National AI Policy in 2024. This Policy aims to integrate AI into a wide variety of sectors such as education, public service, healthcare, transportation, telecommunication and surveillance, environment, finance, manufacturing, scientific research and agriculture to boost economic growth, societal progress and national security. Across these sectors, AI is expected to be used for comprehensive threat detection, enhancing national security and surveillance capabilities, risk assessment and fraud detection in financial services and AI-driven public safety measures such as smart surveillance. It is also expected that AI will be used to improve legal processes and enhance access to justice, improve weather forecasts and energy sustainability, and facilitate job matching.

The provisions of this Policy have been constructed in an overly broad and vague manner leaving out essential details such as what type of AI systems would be used for the broad scope of application envisioned or whether there will be any human rights risk assessment conducted before such application. Far more concerning is that despite aiming to use AI for 'national security', the Policy neither defines the criteria for the term nor does it establish any auditing mechanism to ensure accountability, transparency and security of these data. The Policy acknowledges the need for regular audits to be conducted but does not elaborate on it any further. The PDPA, on the other hand, lays down a mechanism for audits to be conducted by stating that regular audits will be conducted to evaluate compliance with the provisions of PDPA. However, the auditor will be determined by the Data Protection Board. Since the Chairman and the members of the Board will be appointed by the government, questions regarding the independence of the process remain.

Recommendations

1. **Set out definitions and mechanisms that regulate exemptions of data processing under 'national security' and 'public interest'.** The current draft legislation leaves it up to the discretion of the government to determine what is a matter of national security and public interest and which data is classified. Clear parameters to these terms are necessary to prevent contradictory interpretation and abuse of power, especially given that these reasons can be used to override data subject consent or safety.
2. **Ensure the independence of the Data Protection Board.** Since the Chairman and the members of the Board will be appointed by the government, the government will

have unrestrained access to all data. Therefore, the provision for the formation of the Board needs to be amended to ensure its independence.

3. **Mandate judicial oversight as a prerequisite to unfettered access to data.** The legislation allows the unfettered access to data by the data processor in case of national security or to prevent/identify/investigate any crime and the process of such access will be determined by the Rule published by the Data Protection Board. Since there is a question regarding the independence of the board itself, access to personal data should be subject to judicial supervision or order.

How Singapore Leveraged Existing Data Protection Laws for AI Governance: A Model Approach

Sinta Dewi Rosadi

As the country that is known for its rapid and advanced technology in Southeast Asia, Singapore's primary legislation governing data protection is the Personal Data Act (PDPA). The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.[64] Article 20 of the Personal Data Protection Act (PDPA) obliges an organisation processing an individual's data to **notify** the individual in question.[65] Singapore's personal data protection approach emphasises obligations for organisations wishing to gather and utilise data.[66] Under Article 13 of the PDPA, personal data can only be used if the organisation has received meaningful **consent** for such use.[67] However, exceptions exist for business improvement. Organisations don't need consent to use data internally to improve efficiency, personalise products, or enhance services.[68] Per Article 25 of the PDPA, an organisation must destroy or anonymize personal data when the purpose of its collection is no longer served and retention is no longer necessary for legal or business reasons.[69]

The PDPA also obliges any organisation which collects, use, and manage personal data to make a reasonable effort to ensure that the data collected is accurate and complete in a way that would not impair the data owner should the personal data be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation.[70] Singapore imposed great sanctions on offences affecting personal data and anonymized information, including criminal and administrative liability. It does not differentiate between actors of breaches, and classifies criminal penalties based on the severity and scale of the offence.[71]

[64] Article 18 Personal data Act
[65] Article 20 Personal Data Act
[66] Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems, pg. 4
[67] Article 13 Personal Data Act
[68] Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems
[69] Article 25 Personal Data Act
[70] Article 24 PDPA Act.
[71] Article 9B Personal Data Privacy Act.

Regulation and Overseeing Organisation of AI Systems in Singapore

Singapore's Personal Data Protection Commission (PDPC), responsible for evaluating and adjudicating the implementation of PDPA and compliance of Data Processors, has released a guideline for data protection in AI systems, which focuses on Predictive AIs capable of decision-making, and a model AI governance framework for Generative AI, which focuses on Generative AI. Both cover the development, deployment, and procurement stages, and address how the existing PDPA Framework could fit into these stages.

The PDPC Guideline had described the deployment stage of AI as a process where an AI system is used to make a practical decision based on processing data,[72] and the aforementioned obligation for accuracy, safety, and obtaining an individual's consent under PDPA is also applicable to organisations using AI systems to automate their decisions based on the personal data they collected. Not only that, an organisation which deployed an AI system for its own purposes is also **responsible** for personal data in its possession or under its control.[73] In other words, consent and informing the data subject that their data is being processed by an AI system is mandatory under the PDPA.

Under the Model AI Governance and Framework, organisations deploying AI systems for their legitimate interests can be exempt from obtaining consent and providing notifications under certain circumstances. It generally refers to any lawful interest of an organisation or other person/organisation, such as when the AI system is used for evaluating processes, investigating illegal activities, obtaining legal services, and detecting or preventing illegal activities.[74] According to a Court Decision regarding the phrase's interpretation, companies relying on the legitimate interest exception must establish a standardised process for conducting and assessing the basis upon which they will be relying on this exception and ensure that appropriate measures are implemented to mitigate against any risks and adverse effects on individuals.[75] However, given that companies are entitled to determine their own standard for their respective legitimate interest, such standards may be prone to bias and will not have human rights perspective at the forefront of its consideration.

---

[72] Priyadarsini Patnaik, *A Policy Framework Towards the Use of Artificial Intelligence by Public Institutions Reference to FATE Analysis,* 2022.
[73] Article 11 Part 3 PDPA
[74] PDPC Assessment Checklist for Legitimate Interests Exception, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-C-Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.pdf
[75] PDPC Decision on Case No. DP-2105-B8405 in the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 against RedMart Limited.

Compliance Standardisation of AI Systems: AI Verify

Singapore had very recently introduced AI Verify, which is an AI governance testing framework and software toolkit that validates the performance of AI systems against a set of internationally recognised principles through standardised tests, and is consistent with international AI governance frameworks such as those from European Union, OECD, and Singapore. The AI Verify toolkit addresses the 11 governance principles, and allows organisations to self–assess their AI systems via process checks and technical tests.[76]

The AI Verify toolkit is unique in the sense that it is open-sourced. It invites developer, industry and research communities to contribute via their core codebase on GitHub or build algorithms and components on top of the AI Verify codebase.[77] This collaborative method enables the government to gain direct feedback from their stakeholders in the field, while still being in charge of determining the "risks pyramid" for the organisations, as opposed to self-assessment. Though, given that its current contributors are largely corporations, the government of Singapore still needs to ensure that the perspective of the toolkit is not for commercial interests. The over-representation of corporate actors, the potential for inadequate participation from civil society and impacted communities, and an over-reliance on technical solutions all raise concerns about whether this toolkit can effectively address the complex social, ethical, and political challenges posed by AI. To ensure its effectiveness and legitimacy, the development and implementation of the AI Verify toolkit should prioritise inclusivity, stakeholder engagement, and a balanced approach to AI governance that considers both the potential benefits and risks of these powerful technologies.

[76] https://aiverifyfoundation.sg/what-is-ai-verify/
[77] *Ibid.*

Conclusion

This report examined the evolving landscape of data protection in South and Southeast Asia, focusing on the growing presence of AI and its implications for privacy, fairness, and accountability. The analysis reveals a critical need for robust and forward-looking data protection frameworks that can effectively address the unique challenges posed by AI systems.

A key finding is the uneven and often inadequate nature of existing data protection regulations in the region. While countries like Indonesia and the Philippines have established comprehensive data protection laws, their implementation remains a work in progress, and significant gaps persist in addressing AI-specific risks, such as algorithmic bias and automated decision-making. In contrast, countries like Nepal and Bangladesh are still developing comprehensive data protection frameworks, highlighting the need for swift action to ensure privacy protections are not left behind in the face of rapid technological advancements.

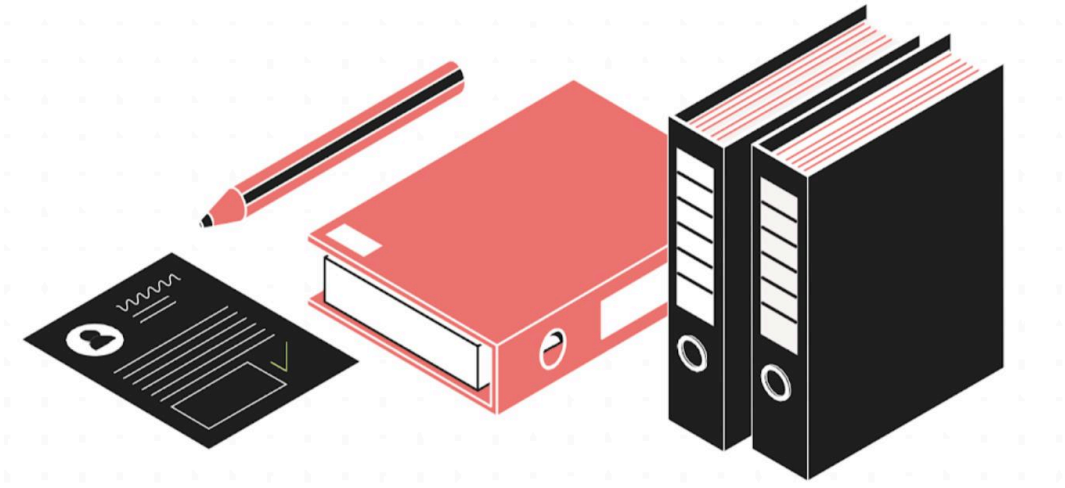
The findings also underscores the need for greater clarity regarding the application of existing data protection principles, such as purpose limitation, data minimisation, and consent, within the context of AI. The data-intensive nature of AI systems, coupled with their evolving capabilities, often clashes with traditional interpretations of these principles, demanding a more nuanced and context-specific approach. The report highlights Singapore as a potential "model approach" for leveraging existing data protection laws for AI governance. Singapore's Personal Data Protection Commission (PDPC) has taken proactive steps by issuing guidelines for AI governance, including specific guidance on using personal data in AI systems.The report cautions against potential bias in the "legitimate interest" exception and emphasises the need for continuous evaluation and refinement to ensure a human-centric approach that prioritises individual rights and freedoms. The path forward requires a multi-faceted approach:

- **Strengthening Data Protection Frameworks:** Countries must adopt comprehensive data protection laws that explicitly address AI-specific risks. This includes clarifying the application of core data protection principles to AI systems, establishing clear guidelines for automated decision-making, and ensuring effective redress mechanisms for AI-related harms.
- **Enhancing Capacity and Expertise**: Data protection authorities in the region must be equipped with the necessary resources and expertise to effectively regulate AI systems. This includes providing training on AI technologies,

fostering collaboration with technical experts, and promoting knowledge sharing between countries.

- **Promoting Transparency and Accountability**: Building trust in AI requires transparency in its development and deployment. This includes promoting explainable AI, establishing clear accountability mechanisms for AI-related decisions, and ensuring meaningful human oversight throughout the AI lifecycle.

Addressing the complex interplay of AI and data protection requires a collective effort from governments, civil society, and the private sector. By prioritising a human-centric approach to AI governance, South and Southeast Asian nations can harness the transformative potential of AI while safeguarding the fundamental rights and freedoms of their citizens.



Annex

Sub-region	Countries	National AI Approaches	Year
South Asia	Bangladesh	National Artificial Intelligence Policy 2024 (Draft)	2024
	India	National Strategy for Artificial Intelligence	2018
	Sri Lanka	Sri Lanka's National Strategy on AI	2024
	Pakistan	National Artificial Intelligence Policy (Draft)	2023
	Nepal	Concept Paper on the use and practice of Artificial Intelligence (AI)	2024
Southeast Asia	Singapore	National AI Strategy	2019
	Indonesia	National AI Strategy (Stranas KA)	2020
	Malaysia	National AI Roadmap (AI-RMAP)	2021
	Philippines	National Artificial Intelligence Strategy Roadmap (Summary)	2021 (v.1) 2024 (v.2)
	Vietnam	National Strategy on R&D and Application of AI (Ministerial Decision)	2021
	Thailand	National AI Strategy and Action Plan (NAIS) (Summary)	2022

Table 1: List of Countries in South and Southeast Asia that have Adopted National AI Approaches.