Harnessing Data for Democratic Development in South and Southeast Asia (D4DAsia) project

Country report for Thailand

Jompon Pitaksantayothin

2024-12-10

About LIRNEasia

LIRNEasia is a pro-poor, pro-market regional policy think tank. Our mission is Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology.

Address: 15 2/1, Balcombe Place, Colombo 8, Sri Lanka.
Telephone: +94 11 267 1160
Email: info@lirneasia.net
Website: https://lirneasia.net/
Twitter - https://x.com/LIRNEasia
Facebook - https://www.facebook.com/lirneasia/
YouTube – https://www.youtube.com/@LIRNEasia-
LinkedIn - https://lk.linkedin.com/company/lirneasia
Instagram - https://www.instagram.com/lirneasia/?hl=en

About this report

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

Table of contents

Executive summary

Data Governance in Thailand

Thailand's data governance landscape is undergoing a significant transformation, shaped by the country's ambition to modernize its administrative systems, promote digital development, and respond to rising concerns about privacy, security, and transparency. This report, developed under the D4DAsia initiative, examines how Thailand's evolving legal frameworks, institutions, and practices structure access to and use of data, and how these dynamics influence democratic development and civic participation.

Historically, Thailand adopted Continental European legal traditions during the 19th century as part of its broader efforts to avoid colonization and modernize its state machinery. Today, its data governance framework is anchored in the 2017 Constitution, which affirms the right to information and the protection of personal data. Over the past two decades, the country has enacted several key laws, including the Official Information Act (OIA, 1997), the Personal Data Protection Act (PDPA, 2019), and the Digitalisation of Public Administration and Services Delivery Act (DPASDA, 2019). Each of these laws represents a specific layer in the country's approach to regulating data access, transparency, and privacy.

However, despite these legislative advances, Thailand's data governance regime remains fragmented and uneven in implementation. A key challenge lies in the inconsistent application and interpretation of overlapping legal frameworks. For instance, while the OIA mandates the disclosure of public sector data, many government agencies exercise broad discretion to withhold information on grounds of national security, institutional convenience, or unclear data classification schemes. Similarly, the PDPA establishes individual rights to data protection and privacy but has suffered delays in full enforcement and is often misunderstood by public and private actors alike. These legal frictions result in a landscape where the same dataset might be simultaneously subject to open data policies and data protection restrictions, depending on the agency or context involved.

Thailand has made substantial efforts to promote data openness, primarily through the work of the Digital Government Development Agency (DGA), which manages the Government Data Catalog and the Open Data Portal. These platforms aim to consolidate and release public sector datasets to improve service delivery, increase

transparency, and foster innovation. The DGA also sets key performance indicators (KPIs) for agencies and offers training programs to support open data practices. Despite these efforts, most datasets (around 90%) remain accessible only through reactive disclosure mechanisms, such as citizen requests, rather than proactive publication.

Tensions between openness, privacy, and security are further complicated by Thailand's political and administrative culture. Security laws such as the Computer-Related Crime Act and the Cybersecurity Act, along with broad definitions of disinformation and national interest, often create a chilling effect on data sharing and public discourse. Moreover, institutions responsible for regulating or managing data – such as DGA, the Digital Government Development Committee (DGDC), and the Personal Data Protection Committee (PDPC) – face limitations in authority, coordination, and capacity.

Sector-specific case studies illustrate the practical difficulties and opportunities for advancing data governance. In the health sector, the National Health Security Office (NHSO) has demonstrated a proactive attitude toward data sharing and citizen participation, particularly in managing the Universal Coverage Scheme. Yet legal uncertainty about what data can be shared and under which conditions continue to inhibit transparency. In contrast, the financial sector has benefited from more coherent regulatory guidance, with the Bank of Thailand emerging as a leader in data governance implementation, particularly in the adoption of open banking standards. Nonetheless, even in this relatively advanced sector, inconsistent interpretation of the PDPA poses operational challenges.

Ultimately, Thailand's data governance system reflects a broader tension between aspiration and implementation. While the state recognizes the value of data for development, innovation, and democratic participation, it often defaults to risk aversion, legal ambiguity, and bureaucratic discretion. Capacity constraints—particularly among local-level officials and small- and medium-sized enterprises—further hinder effective compliance and innovation. Moreover, public awareness of data rights and participation in governance processes remain limited.

To move forward, Thailand must prioritize legal harmonization, institutional coordination, and capacity building. Clearer guidance on the relationship between openness and privacy, better training for both public officials and private actors, and more inclusive mechanisms for stakeholder engagement will be essential. Comparative lessons from countries like South Korea, Australia, and the UK offer valuable models, but successful reform will ultimately require local adaptation and political will. Data governance in Thailand is at a crossroads: whether it becomes a tool for democratization or control depends on the choices made in the coming years.

1 Introduction

This report is part of the "Harnessing Data for Democratic Development in South and Southeast Asia" (D4DAsia) initiative. The project seeks to critically examine how data governance is evolving across the region, with attention to both formal frameworks and informal norms. In the case of Thailand, this means analyzing how state, corporate, and civil society actors shape the production, access, and use of data in ways that either enable or constrain democratic values.

Thailand stands at a pivotal moment in its digital transformation journey, where the governance of data is increasingly central to questions of rights, development, and democratic accountability. As data becomes ever more embedded in public services, commerce, and civic life, the structures that govern its use – i.e., laws, policies, practices, and technologies – have profound implications for inclusive and equitable development.

Data governance is not only about protecting personal information or ensuring cybersecurity. It also involves addressing power imbalances, enabling innovation, and building systems that reflect public interest priorities. When effectively governed, data can support goals such as poverty reduction, climate resilience, and responsive public policy. When neglected or misused, it risks reinforcing inequalities and eroding public trust.

This report contributes to a broader comparative effort, joining case studies from India, Indonesia, Nepal, the Philippines, Sri Lanka, and South Korea. Each country offers distinct lessons. Thailand's experience, in particular, highlights the tensions between digital modernization and enduring governance challenges, and offers valuable insights into how data governance can better align with democratic aspirations. The research questions that this report attempts to explore and answer are as follows:

1. What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?
2. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
3. The emerging governance architecture involves trade-offs among objectives such as greater accountability of powerholders, economic growth, including creation of employment and wealth, resilience of systems, etc. How have

different societies: (a) explicitly recognized the trade-offs or not; and (b) handled them?

4. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from developed countries?
5. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
6. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?

1.1 Structure of the report

1.1.1 Legal background and landscape

Though never colonized, Thailand adopted Continental European legal traditions in the 19th century, becoming a civil law country. The 2017 Constitution, its supreme law, outlines state structure and key rights relevant to data governance – i.e., freedom of expression, access to information, and privacy. Data governance has shifted from secrecy laws to national information and communications technology (ICT) strategies like "IT 2000." While the public sector is governed by laws such as the Personal Data Protection Act (2019) and Digitalisation of Public Administration and Services Delivery Act (2019), the private sector faces fragmented regulation.

1.1.2 Increasing openness/access

This section focuses on constitutional guarantees of the rights to be informed by, and to access, public data or information held by the public sector. However, there is no legal requirement for the private sector regarding openness and access to data.

1.1.2.1 Open standards and software

This section focuses on how Thai government agencies – such as the Digital Government Development Agency and Digital Government Development Committee – ensure consistency in data format, quality, and interoperability. Despite this, the use and promotion of open-source software remain underdeveloped and underfunded.

1.1.3 Decreasing openness/access

This section examines legal frameworks that restrict data access, often citing national security, as seen in the Computer-Related Crime Act and Official Secrets Rules. Further limitations arise from disinformation laws, data localization, and retention requirements. It also reviews the Personal Data Protection Act (2019), which aligns with

constitutional privacy rights but faces implementation challenges due to ambiguous guidelines and limited enforcement capacity in both the public and private sectors.

1.1.3.1 Intellectual property law and data

This section explores the legal issues concerning data and copyright laws, including a discussion on AI.

1.1.4 Policy frictions and trade-offs

This section highlights how constitutional and statutory obligations to disclose information are frequently undermined by privacy and security concerns. These frictions lead to inconsistent implementation, reduced trust in public institutions, and an overall lack of legal coherence.

1.1.5 Good practices and potential learnings

Thailand has drawn on models from the United Kingdom, South Korea, and Australia to inform its data governance frameworks. While training programs and capacity-building efforts exist domestically, knowledge exchange across sectors and public involvement remain limited.

1.1.6 Policy development and capacity challenges

This final section assesses institutional and operational challenges facing data governance in Thailand. Barriers include insufficient resources, vague mandates, weak leadership support, and low digital literacy. These challenges are prevalent in both the public and private sectors, making meaningful implementation of governance frameworks difficult to sustain.

1.1.7 Sectoral deep dives

This section delves into the application of data governance across key sectors. In the public health sector, the National Health Security Office attempts to balance openness and privacy but faces limited capacity and unclear policy direction. In the financial sector, the Bank of Thailand has promoted open banking and digital statement sharing, although overlapping laws and inconsistent interpretations of the Personal Data Protection Act hinder effective data sharing.

2 Country overview

2.1 Legal background and landscape

Thailand, formerly known as “Siam”, is among a handful of Asian countries to have avoided colonization by Western powers. Nevertheless, it was indirectly forced to adopt Western legal systems and traditions to abolish the “extraterritorial jurisdiction” granted

to citizens of Western nations.[1] Consequently, in the 19th century, Thailand underwent a modernization of its legal systems, with special reference to the legal frameworks of France, Germany, and Japan, to align them with those of the Western world.[2] The 2017 Thai Constitution is the supreme law of the land. It defines the structure of the Thai government, including the roles of the monarchy and the legislature. Importantly, it guarantees the rights and liberties of the Thai people, including those related to data governance, such as the right to freedom of expression, the right to access information held by government agencies, and the right to privacy, which underpins the personal data protection framework.

At present, Thailand regards itself as a "civil law country", focusing on statutory law instead of relying on judicial decisions as in common law jurisdictions. It should be noted that Thailand is a unitary state, not a federal one. In terms of hierarchy, the Thai Constitution holds the highest position as the supreme law. Legislative elements, such as codes, acts, decrees, ministerial regulations and departmental announcements etc. occupy a subordinate level, ensuring that their content aligns with the provisions of the Constitution. While court judgments hold practical influence, it is important to note that, officially, they lack binding legal authority.[3]

The policies and legal regulations relevant to data are the product of piecemeal and disparate efforts by the Thai government from different periods of time. Prior to the late 1990s, Thailand already had criminal offences against disclosure of private secrets prescribed in the Sections 322-325 of the Thai Criminal Code, which came into effect in 1956. These can be said to be early "jigsaw pieces" of the protection of data (secrets). After several decades, in 1996, the Thai government proposed "IT 2000" as the first national policy on ICT with the main aims of improving economic and social competitiveness and preparing for changes brought by the digital age.[4] As regards legal infrastructure in relation to the ICT, the National Electronics and Computer Technology Centre (NECTEC) was commissioned to draft six ICT-related bills, among which were bills concerning electronic transaction, personal data protection, and computer crime.[5]

While the foundation of ICT-related laws was laid down in the late 1990s, prolonged efforts to increase the transparency of public administration initiated by Anand Panyarachun's cabinet (1991-1992) became successful when the OIA was passed in

[1] Yasuda, 'Law and Development from the Southeast Asian Perspective'.

[2] Yasuda, 'Law and Development from the Southeast Asian Perspective'.

[3] Odering, 'Library Guides'.

[4] Thuvasethakul and Koanantakool, 'National ICT Policy in Thailand'.

[5] Banisar and Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments'.

1997, during the government of Chavalit Yongchaiyudh.[6] It can be regarded as an important law in relation to the openness of data and information, which was consistent with Section 58 of the 1997 Thai Constitution that guaranteed people's right to access public information in possession of governmental agencies, which they could use to exercise their political rights effectively.[7] It should be noted that the right to access to public information in the possession of government agencies is now guaranteed by Section 41 of the 2017 Thai Constitution.

Three ICT-related laws — namely, the Electronic Transactions Act (No.4) B.E. 2562 (2019), the Computer-Related Crime Act (No.2) B.E.2560 (2017) and the PDPA — and the OIA have contributed significantly to the development of data-related framework beyond the secret protection-related provisions in the Thai Criminal Code.

In addition to the OIA, the DPASDA also plays a significant role in shaping the data governance framework, especially in the public sector. It is the primary piece of legislation that establishes the strategies and policies for the development and improvement of public administration and services, which in turn serve as the legal basis for the policies, standards, and practice guidelines pertaining to data governance in the public sector. In 2020, DGDC, a body established by the power of the DPASDA, issued the Announcement on Data Governance for Government 2020, which aimed to be part of the implementation of the DPASDA.[8] The 2020 Announcement was arguably the first policy that explicitly addressed data governance in Thailand. Given this, it can be said that the focus on data governance in the public sector is primarily driven by the Thai government's ambition to develop and achieve digital government.

To sum up, presently, the Thai government has established a clear framework and policies on data governance for the public sector. They are aimed at enhancing the efficiency of public services and integrating data and information held by various public agencies in a systematic, consistent, and secure manner. In addition, the data governance framework is expected to promote open data, accessible to the public. Interestingly, from the Thai government's perspective, data governance is viewed as a tool to accomplish, at the beginning, the development of ICT legal infrastructure and national ICT competency, and subsequently, more effective public administration and services; the latter is not the goal in and of itself.

[6] Office of the Official Information Commission, 'History of Office of the Official Information Commission'.

[7] Elamchamroonlarp, 'An Approach for Disclosure of Official Information containing Personal Data'.

[8] Announcement of the Digital Government Development Agency - Data Governance of the Public Sector.

In contrast, however, the Thai government has left the data-related framework in the private sector to be governed by a patchwork of disparate laws, such as the provisions of the Thai Criminal Code, PDPA, etc.[9]

2.2 Increasing openness/access

This section focuses on constitutional guarantees of the rights to be informed by, and to access, public data or information held by the public sector. As noted before, there is no legal requirement for the private sector regarding openness and access to data.

2.2.1 Open data and content

The 1997 Thai Constitution is widely recognized as the People's Constitution, as a majority of Thai people participated in its drafting from the very early stages.[10] It was promulgated after Black May 1992, one of the most violent crackdowns on demonstrators and a moment of significant political unrest in modern Thai history.[11] The Black May incident eroded Thai people's trust in their government[12] and intensified their demand for knowing and accessing information held by government agencies.[13] Currently, under the 2017 Thai Constitution, Section 41(1)[14] guarantees the right to be informed by and to access public data or information held by the governmental agencies. On the other hand, Section 59 makes it the duty of the Thai government to disclose any public data or information and also ensure convenient access to such data or information.[15] As stated above, the Official Information Act was arguably the first piece of legislation to address the issue of data openness.

As regards the Announcement on Data Governance for Government 2020, it is essential to examine the original policy paving the way to the passage of the DPASDA. The 2017 Thai Constitution requires the National Council for Peace and Order (the military junta established after the 2014 coup)[16] to make a national masterplan on long-term overall

---

[9] Personal Data Protection Act B.E. 2562 (2019) (English Version).

[10] Aphornsuvan, 'The Search for Order: Constitutions and Human Rights in Thai Political History'.

[11] Lim, 'Black May 1992 – the Last Shot Fired in Anger?'

[12] Deputy Director of Data Management and Analytics Department, Bank of Thailand, interview, 20 October 2023.

[13] Deputy Permanent Secretary of the Office of the Prime Minister (Thailand), interview, 27 October 2023.

[14] The Thai Constitution B.E. 2560 (2017), Section 41(1) reads "A person and community shall have the right to: (1) be informed and have access to public data or information in possession of a State agency as provided by law".

[15] The Thai Constitution B.E. 2560 (2017), Section 59 reads "The State shall disclose any public data or information in the possession of a State agency, which is not related to the security of the State or government confidentiality as provided by law, and shall ensure that the public can conveniently access such data or information."

[16] Sombatpoonsiri, 'The 2014 Military Coup in Thailand'.

national development.[17] The junta announced the 20-Year National Strategy, which requires all succeeding governments to adhere to the agendas therein from 2018 to 2037.[18] The National Strategy's Agenda 6 on Public Sector Rebalancing and Development[19] was translated into the 12th National Economic and Social Plan 2017-2021, which *inter alia* set a policy to improve the management of the public sector, prevent corruption, and establish good governance with an aim to achieve "transparent, effective, and accountable public administration".[20] This in turn paved the way for the Digital Development for National Economic and Social Plan, one of whose aims is to advance digital administration.[21] As a consequence, a series of Digital Government Development Plans were announced, including the first-phase plan 2016-2018,[22] the second-phase plan (drafted for 2017-2021 but never finalized),[23] the third-phase plan (2020-2022)[24] and the fourth-phased plan (2023-2027).[25] Notably, the DPASDA mandates the establishment of the DGDC and the DGA as the Committee's administrative and supporting body to implement measures in accordance with the Digital Government Development Plans, as required by Sections 6 and 10 of the DPASDA. As regards the data governance of public information policy, Sections 7 and 8 require the DGDC to make policies on data governance of the public sector and implement the relevant measures. In addition, all government agencies are required by Section 12 to produce governmental data at the departmental level to be in line with and integrated with the data governance framework. The detailed policies and action plans were set out in the third-phase Digital Government Development plan (2020-2022).[26] As mentioned above, the DGDC issued the Announcement on Data Governance for Government 2020 as the first explicit policy and legal framework with a

---

[17] See The Thai Constitution 2017, Sections 65, 142, 162, 270, 275

[18] National Strategy Secretariat Office, *National Strategy 2018-2037 : A Short Version*.

[19] *Id.* This agenda aims to "to reform and enhance the country's governmental administrative services based on the principle of"government of the people for the people and the common good of the nation and the happiness of the public at large.

[20] Office of the National Economic and Social Development Board Office of the Prime Minister, *Summary of The Twelfth National Economic and Social Development Plan 2017-2021*.

[21] Ministry of Information and Communication Technology, *Digital Thailand Pocket Book (EN)*.

[22] Digital Government Development Agency, 'The Digital Government Development Plan of Thailand for the 3-year period 2016-2018'.

[23] Digital Government Development Agency, 'History of (the Draft) of the Digital Government Development Plan of Thailand for the years 2017-2021'.

[24] Digital Government Development Agency, 'History of of the Digital Government Development Plan of Thailand for the years 2020-2022'.

[25] Digital Government Development Agency, 'The Digital Government Development Plan of Thailand for the years 2023-2027'.

[26] Digital Government Development Agency, *The Digital Government Development Plan 2020-2022 as Published in Royal Gazette*.

view to increasing openness and access as part of data governance, especially in the public sector.

2.2.1.1 The public sector

In this section, we discuss laws that make public data accessible. First, we examine policies that mandate proactive disclosure. Then, we turn to 'reactive' laws that enable data to be shared upon a specific action, such as a citizen's request.

2.2.1.1.1 Proactive data disclosure in the public sector

As discussed above, the first laws to address transparency of data are the OIA and the 1997 Thai Constitution, which are the consequence of the violent political confrontations between the National Peace Keeping Council (the junta) and Thai people in May 1992. Currently, the Office of the Official Information Commission regulates, oversees, and monitors how governmental agencies perform in relation to the disclosure of official information. It also has a power to issue relevant regulations, guidelines, measures, and practices.[27]

The OIA is guided by the idea that "disclosure is the principle; secrecy is the exception".[28] Notably, just 10% of government-held public information is readily accessible to the public (proactively), with the remaining 90% disclosed only upon request (reactively).

The legal principles and policies deriving from the OIA can be summarized as follows.[29] First, all government agencies and public officials are required to comply with all requirements imposed by this law in order to safeguard the right to access public information, as the exercise of political rights and freedom of expression is essential for a healthy democracy. As a consequence, all government agencies are required to compile data catalogs of the public information they possess and make them available to the public through the Government Data Catalog website (https://gdcatalog.go.th/).[30] Second, a clear distinction is made between what information should be made available to the public (the principle) and what information should be withheld (the exceptions prescribed in Sections 14 and 15 of the OIA). Under the Government Data Catalog Guideline Version 2, government data is classified into five categories: Open, Private, Confidential, Secret, and Top Secret. The last three categories align with those

[27] Office of the Official Information Commission, 'Office of the Official Information Commission - Missions'.

[28] Office of the Official Information Commission, 'Office of the Official Information Commission Newsletter'.

[29] Office of the Official Information Commission, *Summary of Key Points of the Official Information Act B.E.2540*.

[30] Director of the Office of the Official Information Commission (Thailand), Jompon Pitaksantayothin, interview, 27 October 2023.

defined by the OIA and by the Official Information Commission regarding government secrecy, in order to avoid confusion with the Commission's existing practices. However, it is important to note that the Government Data Catalog Guideline Version 2 currently available online is marked as a draft.[31] The grounds of exception include national security, public order and safety, the rights and reputation of others, and personal data. Third, all government agencies and public officers should ensure that the majority of information should be publicly available, subject to the PDPA, and information that falls within the scope of exception should comprise a small portion. According to the cabinet resolution of 29 April 2011, all information covered by Sections 7 and 9 of the OIA must be made publicly available on the websites of all government agencies[32][33].[34] Last, as required by Section 33 paragraph 2, all government agencies and public officers have to allow the Office of the Official Information Commission or anyone assigned by the Commission to access and assess the information in question, regardless of whether it

[31] 'DGA Community Standard GOVERNMENT DATA CATALOG GUIDELINE REVIEW'.

[32] The Official Information Act 2540 (1997), Section 7 reads "A State agency shall at least publish the following official information in the Government Gazette (1) the structure and organization of its operation; (2) the summary of important powers and duties and operational methods; (3) a contacting address for the purpose of contacting the State agency in order to request and obtain information or advice; (4) by- laws, resolutions of the Council of Ministers, regulations, orders, circulars, Rules, work pattern, policies or interpretations only insofar as they are made or issued to have the same force as by-laws and intended to be of general application to private individuals concerned; (5) such other information as determined by the Board. If any information which has already been published for dissemination in sufficient number is published in the Government Gazette by making reference to such prior published material, it shall be deemed to comply with the provisions of paragraph one."

[33] The Official Information Act 2540 (1997), Section 9 reads "Subject to section 14 and section 15, a State agency shall make available at least the following official information for public inspection in accordance with the rules and procedure prescribed by the Board: (1) a result of consideration or a decision which has a direct effect on a private individual including a dissenting opinion and an order relating thereto; (2) a policy or an interpretation which does not fall within the scope of the requirement of publication in the Government Gazette under section 7 (4); (3) a work-plan, project and annual expenditure estimate of the year of its preparation; (4) a manual or order relating to work procedure of State officials which affects the rights and duties of private individuals; (5) the published material to which a reference is made under section 7 paragraph two; (6) a concession contract, agreement of a monopolistic nature or joint venture agreement with a private individual for the provision of public services; (7) a resolution of the Council of Ministers or of such Board, Tribunal, Commission or Committee as established by law or by a resolution of the Council of Ministers; provided that the titles of the technical reports, fact reports or information relied on in such consideration shall also be specified; (8) such other information as determined by the Board. If any part of the information made available for public inspection under paragraph one is prohibited from disclosure under section 14 or section 15, it shall be deleted, omitted or effected in such other manners whatsoever so as not to disclose such part of the information. A person, whether interested in the matter concerned or not, has the right to inspect or obtain a copy or a certified copy of the information under paragraph one. In an appropriate case, a state agency may, with the approval of the Board, lay down the rules on the collection of fees therefor. For this purpose, regard shall also be had to the making of concession given to persons with low incomes, unless otherwise provided by specific law. The extent to which an alien may enjoy the right under this section shall be provided by the Ministerial Regulation."

[34] Permanent Secretary of the Ministry of Interior, *Report on the Implementation in Accordance with the Official Information Act B.E. 2540 in the Fiscal Year 2010*.

is publicly disclosable or not. To sum up, the OIA and the cabinet resolution of 29 April 2011 have made the majority of public information in the possession of government agencies (especially those on the lists in Sections 7 and 9) available on the websites of individual government agencies. To date, there has been no study assessing the effectiveness of the cabinet resolution regarding compliance with Sections 7 and 9 of the OIA. Not only does the Official Information Commission under the OIA play a significant role in proactive data sharing, but so does the DGA, a public organization whose mission is to establish an effective digital government in accordance with the DPASDA. As previously stated, Section 59 of the Thai Constitution mandates the disclosure of any public data or information possessed by governmental agencies. In addition, it must ensure convenient access to such data or information. In 2015, the Thai government initiated its Open Government Data project by commissioning the Electronic Government Agency (EGA) to compile a list of types of public information that need to be disclosed, and then ordering all government agencies to provide the required public information on the list for uploading to data.go.th.[35] EGA was under the administration of the Ministry of Digital Economy and Society until 2018, when it was renamed DGA and its administration was transferred to the Office of the Prime Minister. This website is aimed to be "[d]eveloped under the concept of being the central point for accessing open government data, allowing citizens to conveniently and rapidly access government data at all times. The published dataset should be in a structured format such as CSV, XLS, XLSX, XML, or JSON to ensure it is fully machine-readable. Additionally, data sets and metadata can also be managed."[36] [37]

This one-stop information website contains information pertinent to culture, law and justice, education, economy and finance, public health, official statistics, agriculture, social welfare, transportation and logistics, politics, science and technology, and local and regional affairs among other topics. It is still extremely active, with 3,878,375 users and 14,920,495 downloads as of 9 October 2023.[38]

The National Statistical Office of Thailand (NSO) also plays a crucial role in the country's data governance framework.[39] Under Section 6 of the Statistics Act B.E. 2550 (2007), the NSO is responsible for preparing, collecting, and creating national statistics.[40] Furthermore, as stipulated by Section 8(5) of the DPASDA and a Cabinet

---

[35] ThaiPublica, *Prayut Ordered the Electronic Government Agency (EGA) to Specify the Dataset That Every Government Agency Must Disclose to Reinforcing Anti-Corruption Measures. Preliminary Actions Include 'Procurement and Budget Uses*.

[36] Digital Government Development Agency, 'Q&A - Open Government Data of Thailand'.

[37] Digital Government Development Agency, 'Welcome - Open Government Data of Thailand'.

[38] Digital Government Development Agency, 'Welcome - Open Government Data of Thailand'.

[39] National Statistical Office, 'National Statistical Office Website'.

[40] Statistics Act B.E.2550 (2007).

resolution from 7 May 2019, all government agencies are required to collaborate with the NSO, a division of the Ministry of Digital Economy and Society, to create data catalogs focused on statistical and directory services.[41] These statistics are then made publicly available on catalog.nso.go.th, covering a range of topics including logistics, energy, consumption, science and technology, demography, social welfare, religion, and culture. Currently, 752 sets of statistical data are accessible through this platform.

Importantly, apart from dealing with open data or statistical data, the NSO has been appointed by DGDC as the national registrar for all types of government data catalogs. Meanwhile, the DGA manages data.or.th, the central platform for open data, as specified by the DPASDA.

In practice, however, most government agencies have so far posted data catalogs for open data only. This is because all government agencies are driven by KPIs set out by the Office of the Public Sector Development Commission (OPDC). In the first phase of this initiative (2021-2023), the primary objective was to build open data resources. The KPI for this phase measured the number of open data sets cataloged on the NSO website and made available on data.or.th or agency-specific sites, following DGA's data governance guidelines.

Starting from the second phase (2024), the KPIs have shifted focus to encourage data sharing among government agencies. Key agencies are now expected to share "master data" with other agencies, and the KPI will reward data sets that are beneficial across multiple agencies. This shift reflects a broader objective: data governance as a tool for inter-agency collaboration and resource-sharing, rather than an end in itself.

As far as data openness on websites of government agencies is concerned, the 2021 Government Website Standard Handbook issued by EGA sets guidelines for the content that government agency websites should include.[42] It specifies that a government agency website should provide information such as the organization's history or background, aims and vision, information about the CEO, and relevant laws and regulations.

As a part of proactive approaches to government open data, two other initiatives are worth mentioning. First, the Office of the National Anti-Corruption Commission (NACC) conducts an annual Integrity and Transparency Assessment (ITA), with open data as one of its criteria. The NACC specifies which types of government information must be publicly accessible according to the OIA and government policy. DGA has advocated for integrating its open data standard into these datasets to enhance public accessibility through machine-readable formats. Additionally, DGA has recommended that agencies

[41] National Statistical Office, 'Introduction to Government Data Catalogs'.

[42] Electronic Government Agency, *Government Website Standard : Version 2.0*.

conduct public surveys to understand the demand for open data. If agencies release data based on this demand, they can claim this as fulfilling the ITA's open data requirement.

Another major initiative is the Law Portal, launched by the Office of the Council of State in partnership with DGA. This online platform provides access to all legislations and related decrees, allowing users to search and cross-reference laws, decrees, and subordinate regulations.[43]

Interestingly, there is no open access mandate for scholarly literature imposed by either governmental agencies or private funders. Open access is based on voluntariness and collaboration between the Ministry of Higher Education, Science, Research, and Innovation and educational institutions. The main scheme is the ThaiLIS Digital Collection (TCD), which serves as a repository of dissertations, theses, and research reports from numerous colleges and universities nationwide. ThaiLIS is supported by the Ministry of Higher Education, Science, Research, and Innovation.[44] Thailand also has an academic journal database, Thai Journals Online (ThaiJO), which is supported by Thailand Science Research and Innovation (TSRI), an agency under the Ministry of Higher Education, Science, Research and Innovation, National Electronics and Computer Technology Center, Thai-Journal Citation Index Center, Thammasat University and King Mongkut's University of Technology Thonburi.[45] With regard to geo-informatics, the Ministry of Natural Resources and Environment is the main government agency responsible for making this information available. It can be accessed via data.go.th.[46]

2.2.1.1.2 Reactive data disclosure in the public sector

The OIA is also the principal piece of legislation governing reactive data disclosure. Under this law, public information in the possession of government agencies can be divided into three categories: namely, information that is proactively made available to the public (which makes up only 10%, as discussed in the proactive data openness section above); information that falls within the scope of exception and thus cannot be disclosed (Sections 14 and 15 of the OIA); and information that is not within the scope of the first two (Section 11 of the OIA). The final category refers to public information that is disclosed upon request, which accounts for 90% of all public information.[47] Currently, significantly more data is disclosed reactively than proactively. Reactive

[43] Office of the Council of State, 'Law Portal'.

[44] Ministry of Higher Education, Science, Research and Innovation, 'ThaiLIS Digital Collection'.

[45] Thai Journal Online, 'ThaiJo2.1'.

[46] Digital Government Development Agency, 'Geographic Information Services - Open Government Data of Thailand'.

[47] Director of the Office of the Official Information Commission (Thailand), Jompon Pitaksantayothin, interview, 27 October 2023.

disclosure of data is subject to exceptions set forth in Article 15 of the OIA. These exceptions include cases where disclosure would cause damage to national security, interstate relationships, national economic and financial stability, impede the enforcement of other laws, endanger life or safety, or violate privacy. Additionally, under the PDPA, the disclosure of personal data without the consent of the data subject is prohibited.

2.2.1.2 The private sector

There is no uniform policy or framework regarding data and content openness in the private sector. Moreover, data and information of private companies and organizations can be disclosed through the legal frameworks of the OIA and the PDPA. For companies that are not public, the Department of Business Development has a duty to make publicly available information regarding company registration, financial statements, shareholder registration, and business collateral registration (on the department's website). Likewise, the public can access information on charitable and non-profit organizations by using the OIA. However, this is subject to the PDPA. For public companies, Article 24/1 of the Securities Exchange Act, 1992, requires the Securities and Exchange Commission (SEC) to disclose information concerning the issuance or offering for sale of securities, the companies issuing or offering securities, securities companies, the Securities Exchange, over-the-counter centers, organizations related to the securities business, or information relating to any violations and penalties imposed on violators. This includes any other information obtained in the performance of duties under this Act, such as current information, financial statements, and reports on the financial status and operating results of public companies that offer shares to the public (as required by Article 56).

2.2.1.2.1 Trade agreements

At present, Thailand has bilateral free trade agreements with six different countries, namely Australia, Chile, India, Japan, New Zealand, and Peru.[48] With regard to open access to law and open data relating to macro-economics, according to Article 7 of the Framework Agreement on Closer Economic Partnership between the Government of the Republic of Peru and the Government of the Kingdom of Thailand, both Thailand and Peru are required to "ensure that [their] laws, regulations and basic economic data are made available, for example via the Internet, in such a manner as to enable the other Party to become acquainted with them. Upon request from the other Party, a Party will endeavour to promptly provide information and respond to questions pertaining to any actual or proposed measure referred to in paragraph 1".[49] In addition, certain trade agreements require Thailand to have personal data protection measures in place.

[48] Official Website of the International Trade Administration, 'Thailand - Country Commercial Guide'.

[49] SICE, 'Trade Agreements: Peru - Thailand Free Trade Agreement'.

2.2.2 Open standards and software

This section focuses on how Thai government agencies – such as DGA and DGDC – ensure consistency in data format, quality, and interoperability. Despite this, the use and promotion of open-source software remain underdeveloped and underfunded.

2.2.2.1 The public sector

In Thailand, a ministerial or departmental announcement is a type of secondary legislation that a department can issue within the scope allowed by an act. By virtue of the DPASDA, the DGDC issued the Announcement on Data Governance for Government on 12 March 2020 [Digital Government Development Agency[50]].[51] It serves as the foundation for policies and legal measures that explicitly address data governance. The announcement states clearly that the Thai government's data governance serves as a set of principles and guidelines for all government agencies to follow in order to develop systems that effectively manage and integrate discrete and disparate pieces public information, as well as safeguard them with reliable data security mechanisms.[52] Besides the announcement, DGA also issued the Data Governance for Government Handbook version 1.0 in 2018. It provides essential information about data governance in the form of the core concepts, definitions, framework of data governance, data rules, metrics and success measures, data quality and security assessments as well as case studies of Australia, South Korea and the United Kingdom as good models of data governance.[53] In 2020, DGDC also issued the Announcement on Disclosure of Public Sector Information in Digital Format to the Public and the 2020 Handbook.[54] The aim of this announcement is to mandate all government agencies to make the information in their possession ready for public availability and free of charge. The handbook accompanying the announcement provides a set of guidelines to ensure standardization in how data is made accessible, usable, and shareable. It also specifies the file formats used to store and exchange data, ensuring the data can be accessed and used without proprietary constraints, with an expectation that the information will be circulated and utilized for wider benefits and interests. Furthermore, the announcement requires the establishment of a central information center, which will serve as a liaison and facilitator between various government agencies in order to make public information available to the public.[55] The handbook contains details regarding the nature of information that is disclosed, the criteria that should be taken into

[50] 'Digital Government Development Agency - Homepage'.

[51] Announcement of Digital Government Committee on Data Governance.

[52] Announcement of Digital Government Committee on Data Governance.

[53] Announcement of Digital Government Committee on Data Governance.

[54] Announcement on Disclosure of Public Sector Information in Digital Format to the Public.

[55] Announcement on Disclosure of Public Sector Information in Digital Format to the Public.

account when evaluating whether public information is ready to be made available, the procedure for making information publicly available, the designated center for public information, and potential applications of public information.[56]

In 2023, DGA issued the Data Governance for Government Handbook version 2.0 The second version incorporates several modifications and supplementary content. These include updating definitions to align more closely with the present circumstances, providing more details on data governance and information categorization, modifying the criterion for assessing data quality, incorporating guidance on how to implement a data governance framework in practice, and supplementing the first edition with clearer, step-by-step instructions to assist individual government agencies. The second announcement is on Data Quality Assessment Framework for Government Agencies 2023.[57] Its handbook aims to provide a framework and tools for assessing the quality of public information in relation to data management, monitoring, and control. Its main purpose is to provide users of public information with the assurance that the data is accurate, reliable, and of sufficient quality to be utilized for precise policy and operational decision-making, as well as accurate analysis. The third announcement is on Recommendations for Writing Data Management Policies.[58] The primary purpose of this announcement and its handbook is to serve as a template for a data management model that individual government agencies can refer to in developing their own data governance guidelines, aligning with the data policies they have publicly declared.

The last one is the Announcement on Government Data Catalog and Registration Guidelines 2023.[59] There are two handbooks accompanying this announcement. The Handbook on Government Data Catalog provides information to the government agencies' technical and non-technical teams regarding the creation of data catalogs (with metadata) that can be supplied to the central database of public information. The Handbook on Government Data Registration aims to furnish guidance that will establish a standardized framework for the registration process of diverse data catalogs.

In 2012, EGA published the first version of the Government Website Standard Handbook with an expectation to establish a uniform criterion that different government agencies could implement on their respective organizational websites.[60] This handbook contains information regarding: 1. government website contents; 2. government data exchange

---

[56] Announcement on Disclosure of Public Sector Information in Digital Format to the Public.

[57] Ruangchawee, 'ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง
มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (มรด. 5'.

[58] Ruangchawee, 'ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง
มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (มรด. 4-1'.

[59] Ruangchawee, 'ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง
มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ (มรด. 3-1'.

[60] Electronic Government Agency, *Government Website Standard*.

(i.e., how to integrate public information from various websites into a one-stop-service platform or application.); 3. information security; 4. recommended features (i.e., web designs and displays, languages (Thai and English), fonts (the Thai government requires government agencies to use 13 open-source fonts developed by Software Industry Promotion Agency on their websites. Additionally, these fonts have also been promoted for use in the private sector,[61] web navigation system, pop-ups and tool tips, web analytic tools, naming of files and directories, hyperlinks; [62] and 5. Phases of Online Service Development.[63]

In 2021, the Government Website Standard Version 2.0 was released. The second version of the handbook, like the first version, draws from existing open standards such as WCAG 2.0[64]. It contains information on 8 issues: 1. website domain names; 2. basic organizational information of a government agency; 3. organizational policies on open government data; 4. services provided by a government agency; 5. public participation (such as public relations, social interaction, public hearing and online surveys); 6. recommended features; 7. website security; and 8. relevant policies (such as website policy, privacy policy, and website security policy).[65] DGA motivates agencies to adopt data governance practices through incentives and KPIs. One key incentive is the annual Digital Government Award, led by the Prime Minister, which recognizes government agencies that excel in advancing their digital maturity, with specific categories for achievements in open data and data governance. The OPDC's KPI serves as a mandatory benchmark, requiring top-performing agencies to align with DGA's data-related standards and to actively promote data usage. DGA not only establishes and promotes these standards and guidelines but also provides training for government employees. However, DGA is not a regulatory or enforcement body; each government department is responsible for implementing and adhering to the recommended standards and guidelines.

---

[61] National Science and Technology Development Agency, '13 Standard Fonts from Software Industry Promotion Agency (SIPA)'.

[62] It is important to note that all of these should be consistent with the standard of Web Content Accessibility Guidelines 2.0 (WCAG 2.0) introduced by World Wide Web Consortium (W3C), an international standard on accessibility for persons with disabilities.

[63] Electronic Government Agency, *Government Website Standard*.

[64] The Ministry of ICT (the former name of the Ministry of Digital Economy and Society) issued the Thai Web Content Accessibility Guideline (hereinafter "TWCAG") in 2010. The TWCAG 2010 aims to encourage website developers in both public and private sectors to create websites which meet the standards set out in the WCAG 2.0. Content and user interface elements should be perceivable. User interface and navigation should be operable, ensuring keyboard accessibility and allowing sufficient time for user interaction. The operation of the user interface and information must be understandable, maintaining clear and consistent navigation and readability of text. Content should be robust for reliable interpretation by various user agents, including assistive technologies. Hypertext Markup Language (HTML) should be at least HTML 4.01 and XHTML 1.0 versions.

[65] Electronic Government Agency, *Government Website Standard : Version 2.0*.

In 2012, the Act on Carrying Out of Public Service via Electronic Means B.E. 2565 (APSEM) was passed [ActCarrying2022]. In essence, the law grants citizens the right to access all government services and related information online. It mandates that government agencies provide these electronic services in line with standards approved by the cabinet. Failure to comply may lead to charges of neglect of duty for the responsible government officers, as outlined in Article 157 of the Criminal Code. In addition, the law also empowers the OPDC to monitor all government agencies every 15 days and to report to the cabinet every two months on those agencies that have not implemented the required measures.

The OPDC, Office of the Council of State, Electronic Transactions Development Agency (ETDA), and DGA issued two Handbooks on Carrying Out of Public Service via Electronic Means. One edition is designed for novices, while the other is intended for more experienced government agencies [Digital Government Development Agency[66]].[67] These handbooks provide guidelines regarding submission/receipt of petitions or cases, contacting government agencies, sending/receiving electronic documents, presenting evidence, and the preparation and verification of licenses. Importantly, they also set standards for the format of electronic documents to be in PDF, JPEG and BMP. Furthermore, in the case that certification is necessary, the document in question needs to be certified by the National Root Certification Authority of Thailand.[68]

DGDC also issued another major standard called TGIX with the aim of standardizing data format and data exchange protocol between government agencies. TGIX contains both semantic and technical standards. The semantic standards for natural (Thai) personal data and address (location) data are already promulgated, with more planned to be approved by DGDC soon.

2.2.2.2 The private sector

Similar to the public sector, Sections 7 and 10 of the Electronic Transactions Act (No.4) B.E. 2562 (2019) requires private companies and organizations to recognize and treat digital data or documents in the same way as hard copies.

2.2.2.3 Free and Open-Source Software

The NECTEC is active in promoting open-source software, such as Linux and OpenOffice.org.[69] In the private sector, Thailand has the Open-Source Education and Development Association (OSEDA) which aims to promote the study and development

[66] *E-Book Guidelines for Initial*.

[67] Digital Government Development Agency, *E-BOOK-Guidelines-for-Standard.pdf*.

[68] National Root Certificate Authority of Thailand, 'Thailand National Root Certification'.

[69] NECTEC, 'NECTEC : Thailand : National Electronics and Computer Technology Center'.

of open-source software.[70] Unfortunately, at the moment, the Thai government does not give enough importance to the development of open-source software.

2.3 Decreasing openness/access

This section examines legal frameworks that restrict data access, often citing national security, as seen in the Computer-Related Crime Act and Official Secrets Rules. Further limitations arise from disinformation laws, and data localization and retention requirements. It also reviews the Personal Data Protection Act (2019), which aligns with constitutional privacy rights but faces implementation challenges due to ambiguous guidelines and limited enforcement capacity in both the public and private sectors.

2.3.1 National security and public order

Section 52 of the 2017 Thai Constitution makes it obvious that the Thai government has a responsibility to *inter alia* protect national security and public order. This clause allows the Thai government to conduct intelligence operations. Furthermore, under the 2017 Thai Constitution, constitutional rights and liberties may be restricted or limited by law for the protection of national security and the preservation of public order. The right to freedom of expression (Section 34), freedom of travel (Section 38), and civil assembly (Section 44) are, for instance, subject to the protection of national security and the maintenance of public order. It is not surprising that, in Thailand, national security and public order appear to be of particular significance. Though Section 59 requires the Thai government to make public information accessible and available, it also specifies that the obligation to disclose public information does not apply to information related to national security and state secrets.

Section 14(3) of the Computer-Related Crime Act (No.2) B.E.2560 (2017) prohibits the entry of computer data deemed to constitute a national security or terrorism-related offence. It is worth noting that the information that falls under the purview of this provision does not need to be false (disinformation). Even information that is true and accurate can be restricted on the grounds that it threatens national security or that publishing it would amount to a terrorism-related offence.

In addition, the Rule on Maintenance of Official Secrets B.E. 2544 (2001), the secondary legislation passed by the virtue of Section 16 and Section 26 paragraph 5 of the OIA, lays down a practical framework of how to categorize and treat different types of "official secrets". Under this Rule, official secrets, i.e., public information not subject to be the disclosure requirement of the OIA [Section 5 of the Rule on Maintenance of Official Secrets B.E. 2544 (2001)], are classified into three different groups, namely confidential, secret, and top-secret information [Section 12 of the Rule on Maintenance of Official Secrets (2001)]. Confidential information refers to classified information that,

[70] SIPA, 'SIPA Technology Meetup 2016 #6'.

if disclosed in whole or in part, would cause damage to the interests of the state [Section 5 of the Rule on Maintenance of Official Secrets (2001)]. Secret information means classified information that, if disclosed in whole or in part, would cause serious damage to the interests of the state [Section 5 of the Rule on Maintenance of Official Secrets (2001)]. Lastly, top-secret information refers to classified information that, if disclosed in whole or in part, would cause the most serious damage to the interests of the state [Section 5 of the Rule on Maintenance of Official Secrets (2001)]. According to the Rule on Maintenance of Official Secrets (No.2) B.E. 2561 (2018), heads of government agencies (such as individual heads of departments, provincial governors, Bangkok governor, directors or general managers of state enterprises, and the chief executive officers of organizations – for example, the Attorney General, the Secretary-General of the Office of the Judiciary, the Secretariat of The House of Representatives, and the Chairperson of the Lawyer Council of Thailand) have the power to determine the classification level of specific information within their respective organizations.[71] They are also required to provide justifications for labelling information categories (i.e., types of particular pieces of information such as civil-related, military-related, public health-related, financial and economic information) and classification levels (i.e., a confidential, secret or top-secret level). Notably, Section 16 of the Rule on Maintenance of Official Secrets (2001) was not amended by the Rule on Maintenance of Official Secrets (No.2) (2018). This classification and categorization are vital for protecting sensitive information and ensuring that it is handled properly in accordance with the nature, characteristics, and impact of its disclosure or leakage. Moreover, the National Intelligence Agency has responsibility for the security and preservation of civil-related official secrets,[72] the Armed Forces Security Center is responsible for military-related secrets,[73] and the Special Branch Bureau of Royal Thai Police is responsible for police-related secrets[74] [Section 11 of the Rule on Maintenance of Official Secrets (No.2) (2018)].

The final piece of legislation to be discussed here is the National Intelligence Act B.E.2562 (2019). The data and information derived from intelligence operations is technically "public information". However, such public information is of a sensitive nature, and its disclosure or leakage could have detrimental effects on national security and public order. Therefore, information derived from intelligence operations is typically classified as a state secret and is not made public.

[71] The Rule on Maintenance of Official Secrets (No.2) B.E. 2561.

[72] National Intelligence Agency, 'National Intelligence Agency'.

[73] Armed Forces Security Center, 'Armed Forces Security Center'.

[74] Special Branch Bureau - Royal Thai Police, 'Special Branch Bureau - Royal Thai Police'.

2.3.1.1 Disinformation

In Thailand, Section 14 (1) and (2) of the Computer-Related Crime Act (No.2) B.E.2560 (2017) are two main provisions to combat disinformation. Section 14(1) makes it a criminal offence for a person to "dishonestly or by deception, [enter] wholly or partially distorted or false information or content in the form of computer data into a computer system in a manner likely to cause damage to the general public…".[75] Section 14(2) also criminalizes the entry of "false computer data into a computer system in a manner which is likely to cause damage to the protection of national security, public safety, economic safety of [Thailand], infrastructures which are for public benefit; or to cause panic to the general public".[76] It can be concluded that in Thailand, internet-based disinformation that may cause harm to the general public, vital national security and infrastructure, or panic among the populace is subject to criminal penalties. Furthermore, in 2019, the Ministry of Digital Economy and Society established the Anti-Fake News Center Thailand with the dual purpose of disseminating information regarding disinformation, and serving as a platform for the public to report instances of disinformation.[77]

2.3.1.2 Data localization

At present, Thailand does not have a specific law that requires non-personal data to be stored, processed, or handled within the country's border. However, the PDPA has a regulation on the transfer of personal data outside Thailand (for details see below). Additionally, the Ministry of Digital Economy and Society has commissioned the Office of National Digital Economy and Society to study and propose a Cloud-First Policy, which in turn commissioned the Thailand Development Research Institute (TDRI) to come up with a report and recommendations including data sovereignty and data residency policy proposals. But there is no concrete policy or specific law for data localization yet.

2.3.1.3 Data retention

There are two main laws which regulate data retention: Computer-Related Crime Act (No.2) B.E.2560 (2017) and the PDPA. An Internet service provider is required by the Computer-Related Crime Act (No.2) B.E.2560 (2017) to retain traffic data (which refers to any data related to computer system communications, including details about the communication's origin, destination, route, time, date, size, duration, type of service used, or other relevant information regarding the computer system's communication) for at least 90 days from the date the data entered the computer system. Failure to comply with this requirement can be punishable with an administrative fine not

[75] Computer-Related Crime Act B.E.2550 (2007).

[76] Computer-Related Crime Act B.E.2550 (2007).

[77] Ministry of Digital Economy and Society, 'Ministry of Digital Economy and Society Opens Anti-Fakenews Center'.

exceeding THB 500,000. It does not have extra-territorial applicability. In addition, it must store the user's data, for identification purposes, for at least 90 days after expiration date of a service [Section 26 of the Computer-Related Crime Act (No.2) B.E.2560 (2017)]. The PDPA makes it compulsory for data controllers to specify the period of data retention (in accordance with the purpose of the personal data collection) and inform data subjects prior to or during the consent request [Section 23(3) of PDPA]. In addition, data controllers have a duty to delete or destroy personal data after the data retention period has expired [Section 37(3) of PDPA]. It should be noted that PDPA does not provide leeway for data controllers to retain data indefinitely.

Interestingly, data retention is related to the archiving regulation set out by OIC and National Archives of Thailand. As OIC and other laws regarding government data or information deal with information in the form of paper documents, treating data largely means opening or destroying the whole document. On the other hand, data mentioned in the DPASDA, the Computer Crime Act and the PDPA deal with each data set and data field as a unit regardless of its physical form.

2.3.2 Privacy Protection of personal data and taxpayer information

2.3.2.1 Protection of individual rights and personal information

Provisions in the Thai Criminal Code related to the disclosure of private information and secrets decrease data openness. Section 322 makes it a criminal offence for a person to "[break] open or [take] away the closed letter, telegram or any document belonging to the other person so as to ascertain or to disclose its contents, if such act to be likely to cause injury to any person".[78] Section 323 focuses on secrets deriving from duties or occupations. It is a criminal offence for a person who "knows or acquires a private secret of another person by reason of his functions as a competent official or his profession as a medical practitioner, pharmacist, druggist, midwife, nursing attendant, priest, advocate, lawyer or auditor, or by reason of being an assistant in such profession, and then discloses such private secret in a manner likely to cause injury to any person".[79] Under Section 324, a person is subject to criminal punishment if "on the ground that oneself having the duty, professing to call the trust, having known or acquired the secret according to industry, discovery or scientific invention, disclosing or using such secret for the benefit of oneself or other person".[80] Section 325 makes the aforementioned offences compoundable offences. These provisions are based on traditional criminal offences aiming to protect certain types of secrets, and came into

[78] Thailand Criminal Law Text.

[79] Thailand Criminal Law Text.

[80] Thailand Criminal Law Text.

effect several decades prior to the introduction of data transparency (OIA, PDPA) and the framework of data governance in the public sector (DPASDA).

As far as personal data protection is concerned, in 2010 the ETDA issued the Announcement on the Guideline of Government Agency's Personal Data Protection.[81] This guideline applies only to government agencies. In essence, it requires government agencies to handle people's personal data in a proper manner, including through the limited collection of personal data, identification of purposes of personal data collection and storage, prohibition of the use and disclosure of personal data in ways that are different from the purposes of personal data collection, the requirement of data security, notification of the storage of personal data to data subjects and the liabilities of data controllers. Interestingly, certain provisions of this announcement bear resemblance to those specified in the PDPA. The 2010 Announcement was a predecessor of the PDPA, whose application was limited to government agencies.

As regards personal data protection in general, Section 32 of the 2017 Thai Constitution guarantees the right to privacy and the protection of personal data. The PDPA is consistent with this constitutional guarantee. As discussed previously, the draft of personal data protection law was one of six ICT-related drafts introduced in the late 1990s. However, while the Electronic Transactions Act B.E.2544 (2001) and the Computer-Related Crime Act B.E.2550 (2007) came into effect, the personal data protection law was still in the legislative process. In December 2018, the Bill on Personal Data Protection was proposed to the National Legislative Assembly by the military junta at the 91/2561 Assembly; and the PDPA was promulgated and came into effect in February 2019.[82] However, due to concerns that the public and private data controllers and processors might not be at the technical and technological capacity required, as well as due to the COVID-19 pandemic, the full enforcement of the PDPA was postponed until 1 June 2022.[83] According to the Thai government, the postponement of the enforcement of the PDPA will ensure that people's right to privacy and personal data as guaranteed by the 2017 Thai Constitution will be properly protected, reduce and limit injuries caused by violations of personal data, make the collection, storage, use, and dissemination of personal data meet international standards (especially the GDPR of the EU), ensure legal measures that are in line with other countries are in place, and increase transparency and good governance in relation

[81] The Announcement of the Electronic Transactions Commission on the Policy and Practices Guidelines for the Protection of Personal Data of State Agencies.

[82] Digital Government Development Agency, 'History of of the Digital Government Development Plan of Thailand for the years 2020-2022'.

[83] Prachachat Online, *Postponement of the Enforcement of the Personal Data Protection Act by Another 1 Year*.

to personal data[84] .[85] As with other countries' personal data protection laws, the PDPA stipulates that personal data cannot be collected, processed, used, or disclosed without the data subject's consent. However, it should be noted that Section 4 provides exceptions to the applicability of the PDPA.[86] This means that in certain circumstances personal data can be lawfully collected, processed, and disclosed without consent.

The PDPC issued the Guideline for Requesting Consent, which provides guidance on various matters, including the process by which a data controller may request consent from a data subject, the specific information that ought to be presented to the data subject during the consent request process, and the appropriate course of action in response to consent revocation[87] It should be noted, however, that this principle is subject to certain exceptions, including national, financial, or public safety, trial and adjudication, etc.

---

[84] Office of the Personal Data Protection Commission, 'Benefits from the Personal Data Protection Act B.E.2562'.

[85] Prachachat Online, *Postponement of the Enforcement of the Personal Data Protection Act by Another 1 Year*.

[86] Section 4 This Act shall not apply to:

(1) the collection, use, or disclosure of Personal Data by a Person who collects such Personal Data for personal benefit or household activity of such Person only;

(2) operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity;

(3) a Person or a juristic person who uses or discloses Personal Data that is collected only for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest;

(4) The House of Representatives, the Senate, and the Parliament, including the committee appointed by the House of Representatives, the Senate, or the Parliament, which collect, use or disclose Personal Data in their consideration under the duties and power of the House of Representatives, the Senate, the Parliament or their committee, as the case may be;

(5) trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure;

(6) operations of data undertaken by a credit bureau company and its members, according to the law governing the operations of a credit bureau business. The exceptions to apply all or parts of the provisions of this Act to any Data Controller in any manner, business or entity, in a similar manner to the Data Controller in paragraph one, or for any other public interest purpose, shall be promulgated in the form of the Royal Decree.

The Data Controller under paragraph one (2), (3), (4), (5), and (6) and the Data Controller of the entities that are exempted under the Royal Decree in accordance with paragraph two shall also put in place a security protection of Personal Data in accordance with the standard.

[87] Personal Data Protection Committee, 'Guidelines for Obtaining Consent from the Owner of Personal Data in Accordance with the Personal Data Protection Act B.E. 2562'.

According to PDPC's Announcement on the Appointment of a Data Protection Officer under Section 41 (2) of the Personal Data Protection Act B.E. 2562 in 2023,[88] the data controller and data processor who have activities involving the collection, use, or disclosure of personal data on a large scale (over 100,000 individuals) are required to appoint their own data protection officers. This provision is applicable to the data controller and data processor who collect, use, or disclose personal data for the purpose of behavioral advertising through search engines or online social media platforms.

As far as AI and personal data are concerned, the PDPA is the primary legislation that safeguards individuals' personal data in Thailand. It does not include any specific provisions related to web scraping or AI training. However, Section 4(3) of the Act specifies that it does not apply to the use of personal data collected solely for activities related to mass media, fine arts, or literature, provided these activities adhere to professional ethics or serve the public interest. This suggests that web scraping and the extraction of personal data already available from such activities are not regulated by the PDPA. However, the use of personal data on a large scale to train AI, which does not fall within the scope of Section 4(3), appears to contravene the PDPA. Importantly, the Personal Data Committee and the legislative body have not issued an announcement or guidelines to specifically address the use of personal data to train AI yet. It remains to be seen whether the PDPA Committee or the Thai court will address this in the future.

It is noteworthy that Thailand's obligation to implement legal measures for protecting personal information and data is stipulated in several trade agreements. Specifically, this requirement is detailed in Article 1106.1 of the Australia – Thailand Free Trade Agreement, Articles 10.7 and 11.7 of the Peru – Thailand Free Trade Agreement, and Article 10.5 of the Thailand – New Zealand Closer Economic Partnership Agreement.

2.3.2.2 Transfer of personal data to foreign countries

Section 28 of the PDPA regulates the transfer of personal data from Thailand to other countries. This provision requires the destination country or international organization to have "adequate" data protection standards and also implement appropriate safeguards to protect personal data while it is being transferred and stored outside of Thailand. In December 2023, the Personal Data Committee issued the Announcement on the Criteria for Protecting Personal Data Sent or Transferred Abroad.[89] Section 5 of the announcement requires the Personal Data Committee to consider two main factors. The first pertains to whether the country or international organization receiving personal

[88] Announcement: Establishment of a Data Protection Officer (DPO) Under Section 41(2) of the Personal Data Protection Act B.E.2562.

[89] Announcement of the Personal Data Protection Committee on the criteria for the protection of personal data transmitted or transferred to foreign Countries under Section 28 of the Personal Data Protection Act B.E. 2562.

data has legal measures or mechanisms aligned with the PDPA. This involves specific requirements for the data controller, including the need to have suitable security and personal data protection measures, the capability to implement measures safeguarding the rights of data subjects, and an effective remedy.

The second factor pertains to whether the country or international organization has a regulatory body responsible for personal data protection with the power to enforce legal or regulatory measures for data protection. Under Section 6 of the announcement, the data controller seeking to send or transfer personal data abroad can file a request to PDPC for an evaluation of the "suitable safeguards to protect personal data" in the foreign country or international organization. Alternatively, the Office of PDPC also has the authority to initiate the evaluation without a formal request from the data controller. Interestingly, the announcement and the website of the Office of the Personal Data Committee have not yet provided details regarding the necessary documents, the procedural steps, or the expected waiting period.

2.3.2.3 The PDPA, search engines, AI developers, and journalism

Search engines are currently subject to the legal framework of the PDPA as part of the communications, telecommunications, computer, and digital sectors.[90] Legally speaking, all requirements prescribed under the PDPA — such as obtaining the data subject's consent, the duties and responsibilities of data controllers and processors, and the rights of data subjects — are applicable to search engines operating in Thailand.

As of now, there are no official legal documents or guidelines from PDPC specifically addressing how PDPA requirements apply to search engines. This results in ongoing ambiguity regarding how search engines collect and process personal data, including the legality of scraped personal data. Furthermore, although Section 33 of the PDPA introduces the right to be forgotten, enabling individuals to request the deletion or anonymization of their personal data from search engine results, there is no official guidance on its implementation, leaving the issue unresolved.[91]

Nonetheless, in 2022, Google Cloud (not the search engine business) published a white paper outlining its compliance with the Thai Personal Data Protection Act. The paper emphasized Google Cloud's commitment to providing its services in alignment with the PDPA and to working with its customers to ensure that all services and their usage conform to the Act's requirements.[92]

---

[90] Plumkoson et al., 'การคุ้มครองสิทธิในการถูกลืมบนระบบอินเทอร์เน็ต'.

[91] Plumkoson et al., 'การคุ้มครองสิทธิในการถูกลืมบนระบบอินเทอร์เน็ต', 374.

[92] Google, *Thailand Personal Data Protection Act*.

As far as journalists are concerned, Section 4(3) clearly states that the PDPA does not apply to the activities of mass media and journalism carried out in accordance with professional ethics or for the public interest. Thus, journalists and news agencies are still allowed to collect, use, and disclose personal data in the name of public interest, such as in cases of crime, corruption, etc.

Regarding the use of personal data to train AI, as in the case of search engines, AI developers are subject to all legal requirements set forth in the PDPA. However, there are not yet any specific legal regulations or official guidelines from the PDPC.

2.3.2.4 Protection of taxpayer information

Under Section 10 of the Thai Revenue Code, the disclosure of taxpayer information is strictly restricted. Revenue officials who obtain information about taxpayers or related individuals through their official duties are barred from sharing such details with others or making them public, unless the requester is legally permitted to access the information.[93]

While the Official Information Act of 1997 promotes transparency by affirming that government-held information should generally be accessible, with confidentiality as an exception, this principle is not absolute. Specific types of information are shielded from disclosure when release could potentially harm national security or infringe on important private interests. For instance, taxpayer-related information – recognized as personal data – is explicitly protected and excluded from disclosure under the Act.[94] Nonetheless, according to the last sentence of Section 10, taxpayer information may be disclosed if permitted by other laws – for example, when such disclosure is made under a court judgment or order, explicitly authorized by statute, carried out in the public interest, or undertaken as part of the data controller's official duties in exercising state authority.

2.3.3 Intellectual property law and data

This section explores the legal issues concerning data and copyright laws, including a discussion on AI.

2.3.3.1 Copyright law in Thailand

The Copyright Act (No.5) B.E. 2565 (2022), the Patent Act (No. 3) B.E. 2542 (1999), the Trademark Act (No.2) B.E. 2543 (2000), and the Trade Secret Act B.E. 2545 (2002) have certain provisions which prohibit the disclosure of data to the public.[95]

---

[93] Chanataradhamma, 'Personal Data Protection Standards of Publicly Available Information of Tax'.

[94] Chanataradhamma, 'Personal Data Protection Standards of Publicly Available Information of Tax'.

[95] Announcement on Disclosure of Public Sector Information in Digital Format to the Public.

As far as copyright and research are concerned, Section 32 (1) of the Copyright Act provides an exemption for using copyrighted work for research on the condition that such research is not for profit.

The Copyright Act does not specifically address web scraping. As a result, general copyright principles apply. This implies that web scraping activities that extract copyrighted content without the permission of the copyright owners, and does not fall under the exceptions outlined in Section 32 of the Act (such as personal use, research, academic purposes, teaching, school examinations, criticism, or news reporting), could be considered a violation of copyright. It is important to note that, at present, neither the Department of Intellectual Property (DIP) nor the Central Intellectual Property and International Trade Court have provided any guidance on the use of copyrighted material to train AI yet.

Notably, however, Sections 43/1 and 43/5 offer exemptions for search engines ("those who provide services of computer data location tools"), if they meet the following conditions:

"(1) the service [providers provide] services of locating computer data on the internet without knowing, or having a reasonable ground to know, that the computer data are infringing and expeditiously removes the reference or link to the computer data claimed to be infringing from the computer system or network or disables access to the reference or link to such computer data upon obtaining knowledge or notification of such copyright infringement;

(2) the service [providers do] not receive a financial benefit directly from the copyright infringing activity if the [service providers have] the right and ability to control such copyright infringing activity; and

(3) the service [providers make] available a means for receiving notifications, and provide information on the name, address, telephone number and electronic mail address, for contacting purposes, of the service [providers] or the person designated to receive notification, in a location easily accessible".[96]

2.3.3.1.1 Copyright law and AI

The DIP makes it clear that it does not recognize the copyright of work purely generated by AI. However, it may recognize such work if it is generated by AI with the involvement or interference of a human creator.[97] Nevertheless, the DIP and the Central Intellectual

[96] Copyright Act (No.5) B.E.2565 (2022).

[97] Thansettakij, 'The Department of Intellectual Property emphasizes that works created by AI 'cannot be registered for copyright.'

Property and International Trade Court have not provided any comments regarding copyrighted work used to train AI yet.

In my opinion, the infringement of copyright occurs when someone uses other people's copyrighted work without permission for commercial or profit-making purposes. However, the key consideration is that the violating work must be an exact copy or an altered version of the copyrighted work. In this case, AI simply relies on copyrighted work for training to "generate new work" that has distinctive features of its own and differs significantly from the original work. The use of copyrighted work to train AI may not violate copyright as long as the output has unique characteristics that differ from the original..[98]

According to TDRI, the private sector sees the potential and welcomes the opportunities provided by using big data to train AI, and vice versa, using AI to manage big data.

2.4Learnings

2.4.1 Policy frictions and trade-offs

The key friction in Thailand's data governance lies between the legal obligation to disclose public information and the laws that permit government agencies to withhold information based on national security concerns and the protection of personal data. Section 41 of the 2017 Thai Constitution guarantees the right to access public information held by government agencies, while Section 59 mandates the Thai government to disclose public data and ensure easy access to it. The OIA is instrumental in requiring government departments and organizations to make public information available.

However, several laws create exceptions to this rule. Notable among these are the Rules on Maintenance of Official Secrets (2001 and 2018), the PDPA, and the Revenue Code, which prohibit the disclosure of confidential taxpayer information. As a result, tax revenue data is generally not shared with other agencies, except where it is permitted by other laws (for example, through a court order, statutory authorization, public interest, or the performance of official duties involving state authority). As a result, the general principle of information disclosure under the OIA and the constitutional rights to public access are constrained by these exceptions, particularly on grounds of national security and privacy protection.

In terms of trade-offs, although the 2017 Thai Constitution guarantees the right to access public information held by government agencies and obligates the government

[98] Thailand Development Research Institute (TDRI), 'When using AI to manage Big Data for surveying the Thai job market.'

to disclose such data, Section 25 stipulates that this right can be restricted to protect state security or prevent the violation of others' rights. The Rules on Maintenance of Official Secrets (2001 and 2018) and the PDPA permit government agencies to withhold information on the grounds of national security and privacy protection. Consequently, the right to access public information must yield to the need to protect national security and privacy rights.

2.4.2 Good practices and potential learnings

As mentioned in the Data Governance for Government Handbook accompanying the 2020 Announcement, Thailand appears to recognize data governance models in Australia, South Korea, and the United Kingdom as good practices and sources for potential learning.

At the national level, both the Office of the Official Information Commission and DGA provide online and offline training and workshops for government agencies and the private sector.

2.4.3 Policy development and capacity challenges

According to information from the Director of the Office of the Official Information Commission (Thailand), the first prominent challenge in relation to data governance in the public sector is that the categorization of information prescribed in the OIA differs from that set in the Announcement on Data Governance for Government 2020 (issued under the DPASDA). Under the 2020 Announcement, information is classified into four groups: public information, personal information, national security-related information, and official secrets. However, under the OIA, there are three types of official information: (1) information that must be made publicly available (e.g. through online data catalogues), (2) undisclosed information, and (3) information that may be disclosed upon request. This discrepancy creates uncertainty for government agencies when categorizing the data in their possession, as they are required to comply with both frameworks.

Furthermore, under the 2020 announcement, all government agencies are required to create data catalogs of the information they hold. DGA and the Office of the Public Sector Development Commission (OPDC) are currently pushing for the registration of these catalogs to enable data exchange across government agencies, which is expected to lead to the release of more types of government data. Additionally, the disclosure of official documents without revealing sensitive, secret, or personal data can be achieved through techniques such as data masking and anonymization. DGA is currently drafting a standard for anonymization, which is pending approval by the Digital Government Development Promotion Committee (DGDP).

However, many government agencies have not thoroughly reviewed their documents. They tend to rely on brief summaries to generate data catalogs, resulting in documents

with diverse content being grouped together due to similar summary descriptions. Consequently, public data catalogs often fail to accurately reflect the diversity and specific details of the original documents. Given the volume and variety of government records, it is not surprising that the number of catalogs is lower than it should be. Moreover, since the available catalogs contain only condensed summaries rather than full information, individuals may have difficulty locating specific details or identifying documents in their requests. As a result, some requests are rejected by government agencies due to their ambiguity.

Another problem is that current data catalogs do not include full lists of the documents they cover. Some of the listed documents may be classified. Even when individuals know that the information they seek is contained in a particular catalogue, they may be unaware that it cannot be disclosed. Their requests may then be rejected on these grounds. This has led to a breakdown of trust between the public and government agencies. For example, consider a person seeking information on public building project budgets in their village. They know this information is in Data Catalog A, but the catalog also contains documents related to classified military budgets. If the person submits a request for Catalog A without realizing it includes classified content, their request may be denied in full. Public officers may assume the requester is asking for access to all included documents. This situation arises because data catalogs do not specify the full list of documents or clearly indicate which ones are public and which are classified.

In the private sector, the main challenge is the lack of clear and detailed guidelines for businesses to comply with the PDPA, despite mandatory compliance. As a result, many businesses are uncertain whether they are meeting legal requirements, especially when adopting unfamiliar data practices. Furthermore, small and medium-sized enterprises are often reluctant to invest in internal data governance systems. The absence of comprehensive guidance from regulatory authorities – particularly PDPC – has left companies unsure whether their systems and tools are legally compliant.

In addition, some interviewees identified the prevailing negative perception of data governance among executives, officers, and practitioners in both public and private sectors as a key barrier to progress. Many still regard data governance as an unnecessary burden, failing to appreciate its importance. Although the law requires them to develop policies and implement data governance measures, the sheer volume of data and documents they manage makes these tasks feel overwhelming. Moreover, both professionals and the general public in Thailand often lack a clear understanding of data governance principles. Knowledge-sharing mechanisms on this topic are also inadequate and ineffective across sectors.

Despite these challenges, the Bank of Thailand (BoT) has successfully adopted data governance policies and standards aligned with national guidelines. In 2023, BoT received the Digital Government Award for Excellence in Data Governance from the

Prime Minister, presented by DGA, demonstrating strong commitment and cooperation from leadership and staff.

In summary, both the public and private sectors must allocate time, budgets, and personnel to meet legal data governance requirements. Investments in appropriate tools and technologies are essential, and staff must receive proper training to manage large volumes of data effectively. These remain significant challenges for the implementation of data governance in Thailand.

3 Sectoral deep dives

This section delves into the application of data governance across key sectors. In the public health sector, the National Health Security Office attempts to balance openness and privacy but faces limited capacity and unclear policy direction. In the financial sector, the Bank of Thailand has promoted open banking and digital statement sharing, although overlapping laws and inconsistent interpretations of the PDPA hinder effective data sharing.

3.1 Data governance in the national public health sector

The Ministry of Public Health plays a significant role in making policies on data governance in the public health sector. In March 2022, the Ministry of Public Health issued its Ministerial Order No. 378/2565 to commission its Information and Communication Technology Center to regulate the ICT infrastructure in relation to digital data of public health, especially data security (Health CIRT).[99] It also announced the Information Security Management System Policy to ensure data security by providing a guideline and training for public health personnel.[100] At the national level, in September of the same year, Anutin Charnvirakul, the then Ministry of Public Health, announced the policies on public health, one of which was the development of a digital health data system with the aim of integrating scattered health data into a big national database, allowing people to access health-related information about, for example, how to prevent diabetes or types of food that can boost immunity, and access public health services and treatments across different health-care providers.[101] This was followed by the (Draft) Action plan for Thailand's digital health system 2023-2027, with the goals of fostering good data governance, building an ecosystem for digital health data, integrating pertinent health data, and improving data security for sustainable

[99] No.378-2565 Ministry of Public Health's Order on Delegating Responsibilities to Agencies to Control and Supervise Critical Information Infrastructure in the Public Health Sector.

[100] Ministry of Public Health, 'MOPH Data Center Service'.

[101] Ministry of Public Health, 'Ministry of Public Health's Focal Policies 2023'.

digital data for public health.[102] The document mentions that one of the aims is to increase the decentralization of the public health service, making it available to the wider public. However, it mainly addresses administrative decentralization and does not provide any details on how this can be achieved. It reads more like an aspiration rather than actionable information for policy implementation.

This report considers the NHSO and private hospitals as representatives of the public and private healthcare sectors respectively.[103]

The NHSO is a public organization that is responsible for policy-making and implementation in relation to the promotion of the health care system under universal health coverage, ensuring that all people who live in Thailand have access to health care. Among other goals, it aims to achieve and implement an effective information system for communications, an evidence-based system of health care delivery, beneficiary registration facility, and a monitoring and evaluation system".[104]

Importantly, while the NHSO gave an interview, all private hospitals that the researcher approached declined to participate in the interview, due to internal policies. However, the researcher could interview a legal consultant specialized in providing legal advice to private hospitals and familiar with legal requirements in relation to data governance [Director of Digital Information Support Department, National Health Security Office (Thailand), Jompon Pitaksantayothin[105]].[106]

3.1.1 Laws and policies

The laws and policies which the NHSO has to comply with can be divided into 4 categories as follows:

• The first group is relevant to the implementation and operation of the NHSO, which includes the 2017 Thai Constitution, the Official Information Act 2540 (1997), DPASDA and the APSEM B.E. 2565 (2022).

• The second group is about information exchange and disclosure, which includes DPASDA, the Recommendation on ICT Standard for Electronic Transactions by the ETDA, and Open Government Data Guideline 2020 by DGDC.

---

[102] Ministry of Public Health, '"(Draft) Thailand's 5-Year Digital Health System Implementation Plan (B.E. 2566-2570)'.

[103] National Health Security Office, 'National Health Security Office'.

[104] National Health Security Office, 'Philosophy Background'.

[105] Interview, 26 October 2023.

[106] Legal Consultant who is Specialized in Data Management and Protection, interview, 30 October 2023.

• The third group is about personal data protection which includes the Official Information Act B.E.2540 (1997), the PDPA and the Announcement on the Guideline of Government Agency's Personal Data Protection 2010 by the ETDA.

• The final group is about secret protection, which includes the National Intelligence Act B.E. 2562 (2019) and the Rule on Maintenance of Official Secrets (No.2) B.E. 2561 (2018).

For the majority of private hospitals, the relevant laws with regard to data governance that they have to comply with are the Social Security Act B.E. 2533 (1990) and the Workmen's Compensation (No. 2) Act B.E. 2561 (2018), which make them liaise with the Social Security Office, and the PDPA, which requires them to have data governance system to protect personal data of the patient.

3.1.2 Policy gaps and frictions

Similar to other government agencies, the NHSO is required by the Official Information Act 1997 to make public information in its possession accessible to the public. However, it is also obligated by the PDPA to protect what it considers personal data of individuals. The situation is further complicated by a general lack of understanding of the PDPA, leading most public health agencies to hesitate in disclosing information, even when such disclosure is not prohibited by law. This misunderstanding makes it complicated and time-consuming for the public or other government agencies to request information. The policy of promoting information disclosure under the Official Information Act 1997 is at odds with how most government agencies interpret the PDPA, which may be incorrect.

As for private hospitals, they generally do not face issues with policy conflicts, as they are not subject to the Official Information Act of 1997. They only need to comply with the PDPA.

3.1.3 Policy objectives, trade-offs, and their recognition

The NHSO recognizes the competing objectives of accessibility and privacy, as required by laws concerning official information and personal data protection. However, it does not have a clear strategy to resolve this conflict. Currently, it is attempting to comply with both laws as much as possible. In most cases, it has to give priority to the protection of personal data.

Private hospitals are not required to disclose information in their possession, as the Official Information Act of 1997 does not apply to them. They only need to comply with the PDPA. Therefore, the trade-off between accessibility and privacy protection is not an issue for them.

3.1.4 Good practices and potential learnings

As the NHSO is a government agency, it adopts DGA's Data Governance for Government as best practice. The officers of the NHSO have been sent to participate in both online and offline training sessions organized by DGA. There are a few examples in the healthcare sector of open data sharing and data exchange. During the COVID-19 pandemic, the Department of Disease Control, MOPH, reported the COVID-19 cases daily with the data anonymized. Data on home isolation and community isolation patients were also shared with emergency medical service providers and hospitals for efficient patient transfer, using the DGA-RC standard agreed upon among related government agencies. Other examples include the open datasets on road accident fatalities, which include anonymized individual details and GPS location of the accidents.

There are no specific best practices in the private healthcare sector. The officers of private hospitals have the opportunity to participate in workshops or training sessions offered by both private and governmental organizations, such as private companies and public and private universities.

3.1.5 Policy development and capacity challenges

The NHSO faces several capacity challenges at the moment. The first one is that different public health government agencies maintain identical information in various systems and formats. Additionally, certain pieces or sets of data are not complete, accurate, up-to-date and therefore not ready to be used. Furthermore, due to insufficient (or weak) data security mechanisms, certain officers can access particular sets of information which are not relevant to them. Different sets of information are still scattered in different government agencies' possession, as the integration of information has not been achieved in practice yet.

In addition, although the Thai government has issued several policies on data governance, most of them are not systematic and clear, making it difficult for relevant officers to implement in practice. The budgets on procurement of technical tools are limited. The NHSO lacks technicians and officials who have expertise in data management systems and policy analysis to create a framework for data governance. The organizational executives do not give enough importance to data governance within their departments. There is a lack of comprehensive data management strategy. Furthermore, there is a lack of processes or mechanisms to ensure that government agencies adhere to laws and policies. Although all parts and levels of the public sector are required to give importance to data governance and should devote more time and budgets to pursue this goal, at present, a number of government agencies have not yet truly and fully recognized these matters.

For private hospitals, the major concern is how to satisfy the requirements imposed by the PDPA, especially with regard to the request for consent. Despite the fact that the Data Protection Committee has issued a guideline regarding the process of obtaining consent, most hospitals remain uncertain whether their internal procedures adhere to the legal obligations. For example, after receiving consent from a patient, a hospital may be uncertain as to whether it is necessary to request for consent again before connecting its patient database to external organizations, such as an insurance company or the Pao Tang App (a Thai government-adopted e-service and wallet). Furthermore, there is confusion regarding what qualifies as consent (such as a consent given through a telephone), and how long the consent will be valid. In addition, they do not know who manages the personal data of the patient after consent is revoked. To sum up, most private hospitals lack detailed and clear guidelines from law enforcement to comply with policies and legal obligations imposed on them.

Moreover, they lack in-house officers who can handle personal data effectively. As a result, they have to pay outsourcing companies and law firms for legal advice and computer system settings. Even after receiving legal advice and computer system settings, they lack the ability to operate the systems. Moreover, when new problems or difficulties arise, they have to request assistance from the law firms again. Most officers are already engaged in routine duties. They do not have time to and interest in learning about personal data protection, which is new and out of the scope of their main responsibilities. As a consequence, although they receive training, they are unwilling to devote themselves to learning. Finally, most private companies see this as additional and unnecessary costs. Thus, they do not want to invest in this area.

3.2 Data governance in the national banking and financial sector

At the national level, the Bank of Thailand (BoT) plays the main role in making policies, regulations, and guidelines regarding data governance for the bank and the financial sector. In 2021, BoT issued its Guideline on Data Governance[107] with an aim to promote the effective use of financial data to develop and improve financial products and services while protecting the personal information of clients against all potential risks. In addition, the bank's Regulation on Information Technology Risk, which aims to ensure that both bank and non-bank payment service providers *inter alia* have proper IT risk management plans to tackle cyber threats, was also issued in the same year.[108] Furthermore, BoT also promotes open banking and open data in the form of digital bank statements. Open banking allows clients to manage their personal financial data

[107] Bank of Thailand, 'Bank of Thailand's Policy Guidelines on Data Governance'.

[108] Bank of Thailand, 'Bank of Thailand's Criteria for Supervising and Overseeing Information Technology Risks in Accordance with Laws Related to Payment Transactions'.

through digital channels with convenience, especially with regard to the consent given to the banks to send their data to third-parties (such as FinTech companies or government agencies) under good data governance and the principle of secret protection.[109] As regards digital banking, BoT encourages commercial banks to provide a service which makes it possible for a bank statement issued by one bank to be sent digitally to another bank directly with a high level of security and verification. Financial service customers can use a mobile banking app to request bank statement data from their own bank and send it directly to another bank that has requested the bank statement from them.[110]

3.2.1 Public sector: Bank of Thailand (BoT)

3.2.1.1 Laws and policies

According to information from the Deputy Director of Data Management and Analytics Department, BoT's data governance is subject to various laws and policies, most of which are similar to those which regulate other government agencies. The laws and policies in relation to data openness include the Official Information Act 2540 (1997), DPASDA, and the Announcement on Data Governance for Government 2020. For the law and policies concerning the protection of personal information and state secrets, the bank has to comply with the Rule on Maintenance of Official Secrets (No.2) B.E. 2561 (2018) and the PDPA.[111] However, as a regulatory body, the bank also has power to promote plans for openness of financial data and issue regulations on data governance and information technology risk with which private financial institutions have to comply.

There is a recent collaboration between the bank and DGA in implementing the "Open Finance" policy, which transfers data from various government sources to facilitate loan application for people lacking access to financial services. The main concept is to utilize individual consent to obtain their personal data currently in possession of government agencies. The service has been launched to obtain individual water usage or electricity usage and bill payment information from Metropolitan and Provincial Electricity Authority and Metropolitan and Provincial Waterworks Authority, and send it to financial institutions to consider that individual for loan approval. This policy is planned to be expanded to all other personal data held by government agencies.

3.2.1.2 Policy gaps and frictions

There are some conflicts of policies and legal requirements among different government agencies in the financial sector. Firstly, the DPASDA requires government agencies to share and connect databases among the government agencies in the

[109] Bank of Thailand, 'Open Banking and Its Benefits for Thai People'.

[110] Bank of Thailand, 'dStatement Service (Digital Bank Statement)'.

[111] Deputy Director of Data Management and Analytics Department, Bank of Thailand, interview, 20 October 2023.

financial sector in general. However, due to specific pieces of legislation which aim to restrict the disclosure of financial data – for example, the Financial Institution Business Act B.E. 2551 (2008)[112] and the Credit Information Business Act B.E. 2545 (2002)[113] – certain organizations, such as the National Credit Bureau,[114] are not allowed to disclose or share financial information with other government agencies.[115] Secondly, although BoT is subject to the OIA, which requires making public information accessible to the public, the PDPA prevents it from disclosing information that can be considered personal data.

3.2.1.3 Policy objectives, trade-offs and recognition

BoT recognizes the trade-offs and must comply with the laws that restrict the disclosure of financial and personal data, as discussed above.

3.2.1.4 Good practices and potential learnings

BoT regards its Data Governance Guideline as a model of good practice for financial institutions. It also encourages its officers to attend the workshops and training programs organized by the DGA.

3.2.1.5 Policy development and capacity challenges

One of the most important challenges that BoT faces is the undeniable fact that data governance is highly abstract and difficult to understand. As a consequence, like in the public health sector, most officers feel that it is a burdensome addition to their routine duties. Additionally, although there has been some investment in technical tools, technologies and human resources, it seems that the bank still lacks a one-stop-service platform that would enable it to implement data catalog registration, data search, right to access information management, the monitoring mechanisms to follow and evaluate impacts caused by the changes of data governance-related laws and policies, and the proper evaluation process of quality of data.

As required by the DPASDA and the Announcement on Data Governance for Government 2020, all government agencies in the financial sector have to prepare and create data catalogs. As a result, the Thai government in general and BoT in particular have invested more in both financial and human resources. Moreover, it is a time-consuming and difficult task to set a practical framework and to raise awareness of the importance of data governance in individual organizations.

---

[112] Financial Institutions Business Act B.E.2551 (2008).

[113] Credit Information Business Act B.E. 2545 (2002).

[114] National Credit Bureau, 'National Credit Bureau'.

[115] It should be noted that the National Credit Bureau is a private company. However, it has both public and private financial institutions as its shareholders.

The inadequate understanding of the PDPA poses certain obstacles. Most government agencies and other relevant organizations are uncertain about the types of data and the extent to which such data can be disclosed and shared with other agencies. As a result, in practice, the PDPA is typically used as an excuse for refusing to share such information at the beginning. BoT, despite being a regulatory body with legal authority, also experiences this issue. Its requests for certain information in the possession of other departments have occasionally been rejected by those departments as they were unsure whether the requested information could be disclosed. Erring on the side of caution, they prefer to reject the requests initially, and provide information only if the bank shows them evidence, such as specific legal provisions, judgements or ministerial regulations, orders, or announcements.

3.2.2 Private sector: Private banks

Individual private financial institutions that were approached refused to be interviewed due to internal policies. However, the researcher could interview a legal consultant specialized in providing legal advice to private hospitals and familiar with legal requirements in relation to data governance.

3.2.2.1 Laws and policies

The main piece of legislation that requires private banks in Thailand to collect and submit personal financial information of their clients to the National Credit Bureau is the Credit Information Business Act B.E.2545 (2002). For the protection of personal information, they have to adhere to the PDPA. In addition, they have to comply with BoT's guidelines on data governance and the regulation on IT risk management. Interestingly, certain commercial banks, for example Siam Commercial Bank and Kasikorn Bank have their own organizational policies, some of which address the transparency and data openness for shareholders and clients[116] .[117]

3.2.2.2 Policy gaps and frictions

The main policy gap arises from the PDPA. Under this law, personal financial information is not considered as sensitive data. Thus, it is not handled with special protection as is the case for health-related data (despite the fact that it is also a very important type of information especially to financial institutions and their clients). In addition, as regards data security, Section 37(1) requires banks to "provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of [personal data]".[118] However, there are no detailed criteria or evaluation guidelines for the banks to know whether the systems they are

[116] Siam Commercial Bank Public Company Limited (SCB), 'Policy on the Supervision and Management of Business Operations of Siam Commercial Bank Public Company Limited (SCB)'.

[117] Kasikorn Bank, 'Transparency and Data Disclosure - Kasikorn Bank'.

[118] Personal Data Protection Act B.E. 2562 (2019) (English Version).

using are regarded as “appropriate security measures” or not. This makes them uncertain whether their implementation of their organizational or internal data security systems is in line with the legal requirements.

3.2.2.3 Policy objectives, trade-offs and recognition

Commercial banks are not obligated to disclose the information they hold, as the Official Information Act of 1997 does not govern them. Their only requirement is to comply with the PDPA. Consequently, the balance between accessibility and privacy protection is not a concern for them.

3.2.2.4 Good practices and potential learnings

They regard BoT’s guideline on data governance and the regulation on IT risk management as good practices.

3.2.2.5 Policy development and capacity challenges

Although commercial banks do not want to violate the law, especially the PDPA, compliance with the legal requirements imposed by this law also means additional investments and costs. Furthermore, as mentioned above, the law simply requires them to implement personal data protection measures, and there is no detailed guideline or criteria for the financial sector yet. As a result, banks are concerned that the measures they are implementing may not be “appropriate” enough in the eyes of the regulatory body (especially PDPC).

Like most private hospitals, the majority of commercial banks are trying to comply with legal regulations. Nevertheless, most of them have to depend on external law firms for legal counsel and on IT companies to establish computer systems for them, imposing an additional financial burden on them. As regards accessibility, they simply comply with the laws. This means that, due to personal data protection law, in most cases, they will not allow access to information. They will permit access only when required to adhere to other laws or comply with law enforcement authorities’ orders. The issue of interoperability was not mentioned by the interviewee, and no publicly available information on this matter could be found during data collection for this report.

4 Summary of findings

4.1 Commonality & divergences in data governance architecture

In the public sector, the Thai government has established a unified standard for the collection, processing, sharing, disclosure, and access to public data held by government departments and agencies. This initiative is guided by the DPASDA, with the DGA overseeing its implementation. However, these efforts are influenced by other laws

aimed at safeguarding national security, such as the Rules on Maintenance of Official Secrets of 2001 and 2018, as well as protecting privacy rights, particularly under the Personal Data Protection Act of 2019. In contrast, private companies and organizations lack a similarly clear and unified framework, and they are primarily governed by laws like the Personal Data Protection Act of 2019.

For public data sharing, Thailand's main platform is the Open Government Data of Thailand (data.go.th), which offers access to public data from various government departments and organizations. Additionally, the National Statistical Office of Thailand (https://www.nso.go.th/) plays a key role in managing and providing access to public information. Among developed countries, Thailand considers Australia, South Korea, and the United Kingdom as good models of data governance. Furthermore, the Personal Data Protection Act of 2019 is significantly influenced by the EU's GDPR, especially the core principles regarding consent, the duties of data controllers and processors, the rights of data subjects, and the establishment of a supervisory authority.

4.2 Frictions within policies

Section 41 of the 2017 Thai Constitution guarantees the public's right to access information held by government agencies, while Section 59 obligates the Thai government to disclose any public data or information and ensure easy access to it. To support these constitutional provisions, the Official Information Act of 1997 plays a crucial role by requiring government departments and organizations to make public information available to the public.

However, there are several laws that create exceptions to this general rule. Notable among these are the Rules on Maintenance of Official Secrets of 2001 and 2018, as well as the Personal Data Protection Act of 2019. As a result, the broad principles of information disclosure outlined in the 1997 Act and the constitutional rights regarding public access to information are constrained by these exceptions, particularly on the grounds of national security and privacy protection.

4.3 Trade-offs among data governance objectives

Although the 2017 Thai Constitution guarantees the right to access public information in the possession of government agencies and requires the government to disclose any public data or information, Section 25 makes it clear that to protect the security of the State or prevent the violation of the rights of other persons, the right to access public information can be restricted. The Rules on Maintenance of Official Secrets of 2001 and 2018 (national security), as well as the Personal Data Protection Act of 2019 (right to privacy), allow government agencies to deny disclosure on the grounds of national security and personal data protection.

Therefore, the right and freedom to access public information held by government agencies involve a trade-off with the protection of national security and the right to privacy.

4.4 Innovations in data governance regimes

An innovation worth mentioning is the DPASDA. It provides legal and practical frameworks for data governance in the public sector. By virtue of this law, DGA is authorized to issue announcements and guidelines (handbooks) on data governance.

However, apart from this, there is no evidence of legal or policy innovation regarding data governance in Thailand, nor is there evidence suggesting that Thailand has learned from other developing countries.

4.5Policy development processes

Thailand had several data-related laws in place before the introduction of data governance for governmental departments, aiming to both promote data openness and restrict access to data for privacy, national security, and crime prevention. These laws include the Thai Constitution, the OIA, the Computer-Related Crime Act (No.2) B.E.2560 (2017), the PDPA, and the Rule on Maintenance of Official Secrets. However, the landscape of data governance significantly changed with the promulgation of the DPASDA.

The DPASDA mandates that all governmental agencies and departments prepare and implement measures to create data catalogs of public information and data in their possession. These catalogs must be entered and integrated into a centralized data platform to make them available to the public online. DGA is responsible for setting guidelines and standards for the creation and integration of these data catalogs and website portals. Despite the DPASDA, many governmental departments still face several challenges in meeting the data governance requirements set by DGA or complying with laws passed several decades ago. Additionally, there was limited public participation in the legislative process, and while the public could express opinions on more recent laws like the DPASDA through the government’s online platform, these opinions did not significantly influence the final content of the law.

Government departments are required to integrate data governance into their tasks, but most face capacity challenges such as a lack of knowledge, insufficient budgets, human resources, technologies, equipment, and willingness. Many are also unsure how to adjust existing operational behaviors to align with the "new" requirements of data governance, leading to a gap between government expectations and the actual capacity of individual departments. In contrast, the private sector, unlike public organizations, lacks clear and sufficient guidelines for effective data governance. As a result, they often attempt to comply with fragmented and disparate legislation, focusing mainly on

what is legally required, particularly concerning personal data protection, without giving true importance to data governance as a whole.

5 References

Announcement of Digital Government Committee on Data Governance (2020).

Announcement of the Digital Government Development Agency - Data Governance of the Public Sector (2020).

Announcement of the Personal Data Protection Committee on the criteria for the protection of personal data transmitted or transferred to foreign Countries under Section 28 of the Personal Data Protection Act B.E. 2562, § ประกาศและคำสั่งสำนักงาน (2023).

Announcement on Disclosure of Public Sector Information in Digital Format to the Public (2020).

Announcement: Establishment of a Data Protection Officer (DPO) Under Section 41(2) of the Personal Data Protection Act B.E.2562 (2023).

Aphornsuvan, Thanet. 'The Search for Order: Constitutions and Human Rights in Thai Political History'. 2001, 1–10.

Armed Forces Security Center. 'Armed Forces Security Center'.

Banisar, David, and Simon Davies. 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments'. *Marshall J. Computer & Info. L.* 18 (1999): 1–112.

Bank of Thailand. 'Bank of Thailand's Criteria for Supervising and Overseeing Information Technology Risks in Accordance with Laws Related to Payment Transactions'. 8 February 2021.

Bank of Thailand. 'Bank of Thailand's Policy Guidelines on Data Governance'. 23 September 2021.

Bank of Thailand. 'dStatement Service (Digital Bank Statement)'. 24 January 2022.

Bank of Thailand. 'Open Banking and Its Benefits for Thai People'. March 2022.

Chanataradhamma, Kanoknun. 'Personal Data Protection Standards of Publicly Available Information of Tax'. Chulalongkorn University, 2021.

Computer-Related Crime Act B.E.2550 (2007) (2007).

Copyright Act (No.5) B.E.2565 (2022) (2022).

Credit Information Business Act B.E. 2545 (2002) (2002).

‘DGA Community Standard GOVERNMENT DATA CATALOG GUIDELINE REVIEW’. 2023.

Digital Government Development Agency. ‘Digital Government Development Agency - Homepage’. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA.

Digital Government Development Agency. *E-Book Guidelines for Initial*. 2023.

Digital Government Development Agency. *E-BOOK-Guidelines-for-Standard.pdf*. 2023.

Digital Government Development Agency. ‘Geographic Information Services - Open Government Data of Thailand’. 2015.

Digital Government Development Agency. ‘History of of the Digital Government Development Plan of Thailand for the years 2020-2022’. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA, 2021.

Digital Government Development Agency. ‘History of (the Draft) of the Digital Government Development Plan of Thailand for the years 2017-2021’. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA, 2021.

Digital Government Development Agency. ‘Q&A - Open Government Data of Thailand’. 2015.

Digital Government Development Agency. *The Digital Government Development Plan 2020-2022 as Published in Royal Gazette*. 2020.

Digital Government Development Agency. ‘The Digital Government Development Plan of Thailand for the 3-year period 2016-2018’. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA, 2016.

Digital Government Development Agency. ‘The Digital Government Development Plan of Thailand for the years 2023-2027’. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA, 2022.

Digital Government Development Agency. ‘Welcome - Open Government Data of Thailand’. 2015.

Elamchamroonlarp, Piti. ‘An Approach for Disclosure of Official Information containing Personal Data’. *Nitipat NIDA Law Journal* 12, no. 1 (2023): 1.

Electronic Government Agency. *Government Website Standard*. 1st ed. 2012.

Electronic Government Agency. *Government Website Standard : Version 2.0*. 2021.

Financial Institutions Business Act B.E.2551 (2008) (2008).

Google. *Thailand Personal Data Protection Act*. Google Cloud Whitepaper. 2022.

Kasikorn Bank. ‘Transparency and Data Disclosure - Kasikorn Bank’. ธนาคารกสิกรไทย, n.d.

Lim, Eric. ‘Black May 1992 – the Last Shot Fired in Anger?’ Tour Bangkok Legacies.

Ministry of Digital Economy and Society. 'Ministry of Digital Economy and Society Opens Anti-Fakenews Center'. 1 November 2019.

Ministry of Higher Education, Science, Research and Innovation. 'ThaiLIS Digital Collection'.

Ministry of Information and Communication Technology. *Digital Thailand Pocket Book (EN)*. n.d.

Ministry of Public Health. '"(Draft) Thailand's 5-Year Digital Health System Implementation Plan (B.E. 2566-2570)'. October 2022.

Ministry of Public Health. 'Ministry of Public Health's Focal Policies 2023'. 29 September 2022.

Ministry of Public Health. 'MOPH Data Center Service'. Ministry of Public Health Data Center Service.

National Credit Bureau. 'National Credit Bureau'.

National Health Security Office. 'National Health Security Office'.

National Health Security Office. 'Philosophy Background'.

National Intelligence Agency. 'National Intelligence Agency'.

National Root Certificate Authority of Thailand. 'Thailand National Root Certification'. 2017.

National Science and Technology Development Agency. '13 Standard Fonts from Software Industry Promotion Agency (SIPA)'. NSTDA.

National Statistical Office. 'Introduction to Government Data Catalogs'. 2020.

National Statistical Office. 'National Statistical Office Website'. 2023.

National Strategy Secretariat Office. *National Strategy 2018-2037 : A Short Version*. n.d.

NECTEC. 'NECTEC : Thailand : National Electronics and Computer Technology Center'.

No.378-2565 Ministry of Public Health's Order on Delegating Responsibilities to Agencies to Control and Supervise Critical Information Infrastructure in the Public Health Sector (2022).

Odering, Jason. 'Library Guides: Southeast Asian Region Countries Law: Thailand'. 2024.

Office of the Council of State. 'Law Portal'.

Office of the National Economic and Social Development Board Office of the Prime Minister. *Summary of The Twelfth National Economic and Social Development Plan 2017-2021*. n.d.

Office of the Official Information Commission. 'History of Office of the Official Information Commission'. 2013.

Office of the Official Information Commission. 'Office of the Official Information Commission - Missions'. 2013.

Office of the Official Information Commission. 'Office of the Official Information Commission Newsletter'. 2013.

Office of the Official Information Commission. *Summary of Key Points of the Official Information Act B.E.2540*. 1997.

Office of the Personal Data Protection Commission. 'Benefits from the Personal Data Protection Act B.E.2562'. n.d.

Official Website of the International Trade Administration. 'Thailand - Country Commercial Guide'. n.d.

Permanent Secretary of the Ministry of Interior. *Report on the Implementation in Accordance with the Official Information Act B.E. 2540 in the Fiscal Year 2010*. 2012.

Personal Data Protection Act B.E. 2562 (2019) (English Version) (2021).

Personal Data Protection Committee. 'Guidelines for Obtaining Consent from the Owner of Personal Data in Accordance with the Personal Data Protection Act B.E. 2562'. n.d.

Plumkoson, Paradee, Auntika Na Pibul, and Varaporn Vanaphituk. 'Protection of the Right to Be Forgotten on the Internet: The Study of Search Engine'. *Rajapark Journal* 16, no. 45 (2022): 45.

Prachachat Online. *Postponement of the Enforcement of the Personal Data Protection Act by Another 1 Year*. 2021.

Ruangchawee, Tanatkris. 'The Announcement of the Digital Government Development Committee regarding the Digital Government Standards on Criteria for Assessing the Quality of Data for Government Agencies (MD5: 2022)'. Digital Government Standard, 27 March 2023.

Ruangchawee, Tanatkris. 'The Announcement of the Digital Government Development Committee regarding the Digital Government Standards on Recommendations for Formulating Policies and Practices in Data Governance (MD4-1: 2022 and MD4-2: 2022)'. Digital Government Standard, 27 March 2023.

Ruangchawee, Tanatkris. 'The Announcement of the Digital Government Development Committee regarding the Digital Government Standards on Recommendations for Guidelines in Establishing Public Sector Data Inventory and Registration Procedures for Public Sector Data Inventory (MD3-1: 2022 and MD3-2: 2022)'. Digital Government Standard, 27 March 2023.

Siam Commercial Bank Public Company Limited (SCB). 'Policy on the Supervision and Management of Business Operations of Siam Commercial Bank Public Company Limited (SCB)'. 17 January 2023.

SICE. 'Trade Agreements: Peru - Thailand Free Trade Agreement'. Foreign Trade Information System, 2022.

SIPA. 'SIPA Technology Meetup 2016 #6'. Open Source Education and Development Association (OSEDA), 2016.

Sombatpoonsiri, Janjira. 'The 2014 Military Coup in Thailand: Implications for Political Conflicts and Resolution'. *Asian Journal of Peacebuilding* 5, no. 1 (2017): 131–54.

Special Branch Bureau - Royal Thai Police. 'Special Branch Bureau - Royal Thai Police'.

Statistics Act B.E.2550 (2007) (2007).

Thai Journal Online. 'ThaiJo2.1: Thai Journal Online'.

Thailand Criminal Law Text.

Thailand Development Research Institute (TDRI). 'When using AI to manage Big Data for surveying the Thai job market.' TDRI: Thailand Development Research Institute, 2 August 2023.

ThaiPublica. *Prayut Ordered the Electronic Government Agency (EGA) to Specify the Dataset That Every Government Agency Must Disclose to Reinforcing Anti-Corruption Measures. Preliminary Actions Include 'Procurement and Budget Uses.* 10 August 2015.

Thansettakij. 'The Department of Intellectual Property emphasizes that works created by AI 'cannot be registered for copyright.' Thansettakij, 30 May 2023.

The Announcement of the Electronic Transactions Commission on the Policy and Practices Guidelines for the Protection of Personal Data of State Agencies (2010).

The Rule on Maintenance of Official Secrets (No.2) B.E. 2561 (2018).

Thuvasethakul, Chadamas, and Thaweesak Koanantakool. 'National ICT Policy in Thailand'. Paper presented at Africa-Asia Workshop : Promoting Co-operation in Information and Communications Technologies Development, Kuala Lumpur and Penang, Malaysia. March 2002.

Yasuda, Nobuyuki. ‘Law and Development from the Southeast Asian Perspective: Methodology, History, and Paradigm Change’. In *Law and Development in East and South-East Asia*. Routledge, 2002.