2020

Exploring Thailand's PDPA Implementation Approaches and Challenges

Damrongsak Naparat
Chiang Mai University, damrong.naparat@cmu.ac.th

Exploring Thailand's PDPA Implementation Approaches and Challenges

Research-in-progress

Damrongsak Naparat
Faculty of Business Administration
Chiang Mai University
Chiang Mai, Thailand
Email: damrongsak.naparat@cmu.ac.th

Abstract

Thailand's Personal Data Protection Act (PDPA) will come into full force in 2021. Sharing many similarities with the General Data Protection Regulations (GDPR), the PDPA could similarly severely affect private and public organisations that have to deal with personal data and its privacy in the same way that the GDPR has. While existing literature on the GDPR provides some initial information about how organisations could apply the GPDR implementation methods to the PDPA implementation process, little is known about what organisations are doing to comply with the PDPA. This research aims to bridge this gap. The objective of this research is 1) to gain an in-depth understanding of how large public and private organisations in Thailand are implementing the PDPA; 2) to determine the necessary steps that organisations must take to meet compliance; 3) to identify the challenges faced by large organisations in seeking to comply with the GDPR.

Keywords PDPA, GDPR, privacy, implementation, challenges

1. Introduction

The growth of the internet and social media has introduced new security challenges and risks. A growing mountain of personal data collected by private and public organisations has raised concerns for individuals and governments. The European Union (EU), in 2018, introduced the General Data Protection Regulations (GDPR) to replace the EU Data Protection Directive adopted in 1995. The GDPR initiative aims to keep up with the privacy requirements necessary for the new digital landscape (Tikkinen-Piri et al. 2018).

Following the trend set by the GDPR, Thailand's Personal Data Protection Act (PDPA) was passed in 2019 and became effective on 28 May 2019. The PDPA has many similarities with the GDPR, and shares the same principles. Businesses that already comply with the GDPR would find it easy to comply with the PDPA.

Most of the PDPAs operational provisions relating to the rights of the original owners of the data, should have come into full force on 27 May 2020. Such provisions include the obligations of the data controller; data processes; relevant entities; and the penalties for non-compliance. The Thai government agreed to postpone the enforcement date for most of the provisions of the PDPA by one year, which would give public and private sectors enough time to implement the PDPA in the respective organisations. The main reason for the delay stems from the financial burden on the organisations during the coronavirus pandemic (Bangkok Post 2020). However, the complexity of the PDPA implementation process and lack of public awareness could be hidden facets of this delay.

When the GDPR became active across EU countries in 2018, it introduced many changes and challenges to organisations. For example, organisations now have to review their processes and procedures to ensure that they comply with the GDPR requirements on personal data collection and the processing of personal data (Almeida Teixeira et al. 2019). The GDPR brings changes not only to processes and procedures in the organisations but also to organisation culture and employee mindsets (Freitas and Mira Da Silva 2018). According to the results of various surveys between 2016 and 2018, it takes several years for organisations in the EU to gain a proper understanding and to create sufficient employee awareness of the GDPR. Still, many organisations do not see the GDPR as their priority (Almeida Teixeira et al. 2019). The results from these surveys indicate two important things: 1) The GDPR implementation is very complex and time-consuming, 2) it requires a great deal of attention and resources to successfully implement the GDPR, since it will mean radical changes across organisations, so full compliance with the GDPR is not realistic within a short time-frame (Sirur et al. 2018).

The implementation of the PDPA in Thailand could go down the same route, and it would face the same challenges. For example, the PDPA could affect the private and public sectors in the same way that the GDPR has. The delay of the PDPA implementation within organisations indicates that there have been challenges relating to its implementation. However, sufficient research on the PDPA implementation still lacks, especially in the context of a large organisation, which would be subjected to PDPA implementation. Also, there is a lack of empirical research to explain how large organisations have successfully implemented the PDPA. This study aims to bridge these gaps by 1) seeking to understand how large and complex organisations have implemented the PDPA, 2) identifying what the challenges are in terms of implementing the PDPA, and 3) identifying mechanisms used by these organisations.

The results of this study will provide guidelines for implementing the PDPA, as well as reveal mechanisms that organisations are using to overcome the challenges they face during the implementation process.

2. Literature Review

2.1 Thailand Privacy and Data Protection Act (PDPA)

The PDPA, following the trend of the GDPR, aims to regulate the lawful collection, use, or disclosure of personal data, that can directly or indirectly identify a natural person (Greenleaf and Suriyawongkul 2019). The Act was published in the Government Gazette on 27 May 2019, and should have come into effect, with the full force of the law, on 28 May 2020. The Act has been postponed to May 2021, when the government reassessed the situations as a result of the COVID-19 pandemic (Bangkok Post 2020).

The PDPA covers both the private and public sectors. Of Asian countries, only Thailand and The Philippines have data privacy laws that also cover the public sector. Exemptions, made by decree are few, especially for the private sector. This Act, however, will not cover the use of data for private and family purposes, data collected for media, artistic or literary uses, and data collected in the public

interest. Credit bureaus and their members, state agencies with duties to protect public security (i.e. financial security, protect against money laundering, forensic science purposes, or for cybersecurity) are also on the exemption lists.

The PDPA's principles are heavily informed by the EU's GDPR. For example, the data minimisation principle, consent requirements for data collection, restrictions on personal data processing, and right to request deletion ('right to be forgotten'). The PDPA also requires the appointment of data protection officers (DPOs), with an exception for 'small-sized businesses' (Greenleaf and Suriyawongkul 2019). Breaching the PDPA will result in administrative fines, with maximum fines ranging from 500,000 baht (approx. US$ 16,000) to 5 million baht (approx. US$160,000), depending on the nature of the breach (Greenleaf and Suriyawongkul 2019). However, this is a 'low maxima' by international standards, but will severely affect some local businesses, especially during the COVID-19 pandemic, where finance is a primary concern for businesses.

2.1. PDPA Implementation – Lesson Learned from the GDPR

The literature on implementing the PDPA is scarce or non-existent, and with no peer-review articles. This is obvious, because the PDPA is very new, and many businesses operating in Thailand do not yet know about it. However, since the GDPR has significantly influenced the PDPA, research on the GDPR implementation is encouraged, and should provide useful information to help understand how organisations could successfully implement the PDPA.

A review of the research on the GDPR implementation shows that there are different approaches to putting the GDPR into action. While some papers propose comprehensive guidelines, containing a number of steps, different researchers suggest various steps to implementing the GDPR. For example, Boban (2018) lists four broad steps, including 1) establish an implementation programme; 2) specify a realistic timeline and assign people to tasks; 3) prioritise compliance recommendations; and 4) conduct ongoing reviews and continuously improve the implementation programme. Another approach, for example, Tzolov (2018), proposes using a family of ISO frameworks, including ISO 9001:2015, ISO 27000, and ISO 31000 as a guideline for GDPR implementation. The framework would include seven steps: 1) understand the business, 2) analyse the data flow, 3) conduct analysis for the compliance, 4) prepare for GDPR implementation, 5) perform an impact assessment, 6) verify compliance, and 7) consult the supervisory authority. Polkoskwi (2018) argues for even more detail with 23 steps an organisation could take to reach compliance.

Regardless of the approach taken by different authors, implementation steps can be classified into the following sets of activities:

2.1.1. Understanding the Regulations and Obligations

Lack of understanding of the regulations is one of the challenges in implementing the GDPR. Management and legal departments typically do share common ground (e.g., in terms of approach and vocabulary). These shortcomings hinder progress and prevent organisations from identifying ways to comply (Labadie and Leggier 2019). However, understanding the regulations and its obligations can be difficult, because the GDPR does not specify guidelines regarding its implementation, and does not prescribe which particular technologies to use. In the case of the PDPA, the regulations impose strict obligations on organisations operating in Thailand, but further information that allows the organisations to assess their obligations is not yet available (Greenleaf and Suriyawongkul 2019).

2.1.2. Build Awareness Across an Organisation

Complying with the PDPA should become a top priority for an organisation. Awareness-raising includes building awareness for data subjects; and employees involved in collecting, processing, and storing personal and sensitive data. According to Almeida Teixeira et al. (2019), an organisation should be aware of the existence and content of the relevant regulations and understand how the privacy regulations are relevant to their company. The sooner organisations become aware of the regulations and start their preparation to meet compliance, the more likely they will be able to achieve compliance.

2.1.3. Perform an Audit of Data and Processes

To comply with the PDPA, an organisation needs to audit the data, internal processes, and procedures to find out to what extent the PDPA applies to them. The organisation must analyse the personal data that they own and apply appropriate data management to protect the data (Almeida Teixeira et al. 2019). The audit should include the auditing of the data protection system, and there should be a constant monitoring of the system (Tzolov 2018). Frameworks like ISO 27001 (Lopes et al. 2019) and

ISO 9001:2015 (Tzolov 2018) can be used as an internal guideline for auditing data, developing processes and infrastructure, and for meeting compliance.

2.1.4. Appoint DPO and Necessary Positions

The next activity is to appoint the Data Protection Officer and officers to carry out other roles (i.e., project manager (PMs) and Data Administrator (DA)). Specified in the PDPA (s. 41), an organisation (except for 'small size' businesses and specific state agencies) must appoint the DPO (Greenleaf and Suriyawongkul 2019), who will play crucial roles in PDPA implementation. Research suggests that the DPO (in the context of GDPR implementation) should monitor the compliance of the GDPR, and be a contact point between the organisation and Supervisory Authorities (Almeida Teixeira et al. 2019). The appointment of the DPO also demonstrates that an organisation takes GDPR seriously and recognises data as its main assets (Zerlang 2017). Nonetheless, identifying a designated and qualified DPO can be challenging since it is hard to recruit and retain people with the required skills (Khan 2018).

2.1.5. Identify Gap for Compliance

Gap identification reveals the areas (e.g., processes, data flows, systems) that must be improved, and allows organisations to pinpoint areas where they might violate their PDPA obligations - hence they can resolve those violations and issues. Gap analysis requires IT professionals who know the software systems handling the personal data; data privacy experts; legal experts; and compliance experts who can assess the practice, identify risks, and provide advice to ensure compliance (Ayala-Rivera and Pasquale 2018).

2.1.6. Create Measures for Compliance and Minimise Risks

Organisations would be required to create necessary measures for compliance. These measures include establishing security mechanisms to protect personal data, create risk management plans, use secure infrastructure and advanced security features (Gabriela et al. 2018). Other measures could be devised to address and remedy the gaps identified earlier, and, ultimately, to ensure compliance.

2.1.7. Employee Training

Employee training is necessary since it creates awareness about the PDPA, and educates the staff involved in the personal data processing operation (c.f. Tikkinen-Peri et al. 2018). It also emphasises the importance of awareness building at the individual level. Organisations may provide various types of employee training, such as training before starting work, on-the-job training, optional training, and training about changes in data protection laws/procedures (Polkowski 2018). A training session should help employees to follow internally determined rules, and hence minimise risks to the personal data (Magnusson and Iqbal 2017).

2.1.8. Establish Policies, rules and recommendations

Privacy policies must be clear with regard to the data subject as well as to employees of the organisation. According to the GDPR, organisations are required to inform data owners about their data privacy policy. The policy should contain details about how personal data is collected, processed, used, stored, and deleted. Internal rules and recommendations are for employees to follow. Rules and recommendations for employees must be explicit and can be in great detail to ensure the compliance with the GDPR (Polkowski 2018).

2.1.9. Impact Assessment

Organisations must conduct a Data Protection Impact Assessment (DPIA) when a type of processing is likely to result in a high risk to the rights and freedoms of a person (Tikkinen-Piri et al. 2018). According to Tzolov (2018), the purpose of having an impact assessment is to minimise the risk using risk management methodology, which demonstrates that data processing complies with the regulations. Risks assessment should be used to identify risks for the rights and freedom of data subjects, risks of security breaches, and data loss. Tzolov (2018) recommends the use of the ISO 31000 framework to help recognise risks and risk levels. The ISO 9001 framework can be used to mitigate those risks. By performing an impact assessment, the organisation needs to have a proposal containing measures to improve data protection; organisation policies; training; and a residual risk assessment.

2.1.10. Review and Verification of Compliance

Devised data processing and data protection should be monitored regularly. The current state of data protection should be reported to the person in charge, such as the Data Administrator (DA). (Polkowski

2018). Besides auditing and monitoring the implementation, organisations should regularly review to verify compliance (Tzolov 2018).

2.1.11. Use Proper Tools

PDPA implementation can be complicated and time-consuming. Use of proper tools can help with the implementation. Small and medium-sized organisations can use readily available and simple software like Microsoft Word to do documentation and custom tools made in Microsoft Excel to perform risk analysis (Polkowski 2018). More sophisticated tools can also be used, for example, to monitor risk in data exchanged online, and to analyse threats and malware that might breach data storage and data processing infrastructures (Horák et al., 2019).

2.2. Challenges in PDPA Implementation

While the PDPA is anticipated to be beneficial to individuals and organisations in the public and private sectors, similar to the GDPR, the implications for organisations regarding regulatory compliance are that they could face severe difficulties and many challenges.

The first challenge stems from a lack of awareness of the regulations and obligations that organisations need to abide by. Many GDPR readiness surveys (see Addis and Kumar 2018; Ayala-Rivera and Pasquale 2018) point to the same kind of challenge - that many organisations were not aware of the GDPR or did not know how it would affect their organisation. This lack of awareness, both at the organisation and the individual level, could slow the implementation process, and eventually leads to a delay or an incompletion of the implementation (Almeida Teixeira et al. 2019).

The second challenge is that the PDPA implementation could demand a great deal of resources such as time, money, and people to meet the deadline before the regulations become fully active on 26 May 2021. Research shows that budgets required for GDPR compliance could reach $50 million for a single organisation (Sirur et al. 2018). As a result of the coronavirus pandemic, and the global economic downturn, financial resource could be limited. Moreover, while every large organisation is obliged to appoint a DPO, recruiting and maintaining a qualified person can be challenging (Khan 2018). Moreover, given that there is less than a year left for implementation (before 26 May 2021), time is the enemy for organisations that have not yet started their implementation processes, or are still in the process of implementing it. As Sirur et al. (2018) put it, “feasibility in short time-scales [is] not guaranteed” (p. 94).

The third challenge is understanding the regulations. To have a common understanding of the regulations across an organisation is difficult. Managements and law departments could have different views of the same regulations (Labadie and Leggier 2019). The fourth challenge regarding the regulations is that certain parts of the PDPA are not finalised. There are many rules and exemptions of the PDPA that the Personal Data Protection Committee (PDPC) need to come to their decisions. Much necessary information about the PDPA has not yet become available to the public (Greenleaf and Suriryawongkul 2019).

3. Research Design

The objectives of this research are 1) to gain an in-depth understanding of how large public and private organisations in Thailand are implementing the PDPA; 2) to determine the necessary steps that organisations need to take to meet compliance; and 3) to identify the challenges faced by large organisations in seeking to comply with the GDPR, and logging ways in which they are overcoming these challenges.

This research asks the following questions: 1) What are the steps taken by large organisations to successfully implement the PDPA? 2) What are the challenges the organisations have faced when implementing the PDPA? and, 3) What are the mechanisms the organisations use to overcome the challenges?

3.1. Data Collection

We will collect data from the following organisations to represent the private and public sectors (see Table 1):

Sector	Organisation	Examples of Personal/Sensitive Data
Public	The Ministry of Interior	Thai citizen data including name, home address, biometric data, blood group, race, religion, and national ID.
	The Revenue Department	Personal data of taxpayers, individual income, tax payment records.
	Government Saving Bank	Employees' personal data, customers' personal information, bank accounts, payments and services records, recorded data for Know-Your-Customer (KYC).
	Three research universities	Employees' personal data, students' personal data, students' family data academic records, research subjects' data.
Private	Three commercial banks	Employees' personal data, customers' personal data, bank accounts, payments and services records, recorded data for Know-Your-Customer (KYC).
	Three life/health insurance companies	Employees' personal data, customers' personal data, health data.

Table 1. A list of organisations for data collection

We have chosen these organisations because:

1. These organisations have to deal with a large amount of personal and sensitive data. The PDPA poses significant challenges to these organisations, because they have to handle large quantities of various personal information.
2. These organisations are large organisations, meaning they have more than 100 employees or their annual revenue is more than 500 million baht (approx. US$16,000,000) per year (for the service sector business).
3. These organisations are accessible for data collection.

Data will be collected using in-depth semi-structured interviews and related documents to allow data collaboration and triangulation. Semi-structured interviews will be conducted with top-level management (e.g., CIO, DPO), project managers, PDPA steering committees, and working groups. The interview will be used to gain an understanding of:

- an organisation's strategic direction towards PDPA compliance;
- PDPA policies;
- PDPA implementation and deployment plans;
- challenges and issues before, during, and after PDPA implementation, and how the organisation overcame the challenges.

The interviews with informants who perform different roles in the PDPA implementation processes should minimise the 'elite bias' problem (c.f. Miles and Huberman 1994). The interview guide, building around the 11 GDPR implementation steps and challenges reviewed in the previous section, will aid the interviews to ensure that the researchers focus on the objective of this study.

Each interview will be one-on-one (unless the participants prefer the group interview). While the number of informants is not a primary indicator for data collection in qualitative research (as compared to variance-based research where the sample size is crucial), we aim to interview at least 24 informants

(at least two informants per organisation) or when the collected data is saturated. Data is considered saturated "when gathering more data sheds no further light on the properties of [the] theoretical category" (Charmaz 2008, p. 167). Each interview will last around 60-90 minutes. The interviews will be audio/video recorded with permission from the informants and file-notes will be taken. We will use the snowball technique (Wohlin 2012) to identify informants. The technique should allow the recruitment of key informants who are genuinely involved in the implementation of the PDPA in their organisation; hence insightful information can be gathered.

For additional sources of information, data will be gathered from project documents and related information such as an organisation's policies related to personal data, standard operation procedures for protecting personal data, information security policies/measures and practices, etc.

3.2. Data Analysis

Interviews will be transcribed and collated with other collected documents. We will use the 'open coding' technique (see Charmaz 2008) to identify themes, activities, tasks and conditions that emerged from the data. Next, we will use 'axial coding' to create relationships between themes/activities/tasks to form processes. Also, the axial coding will reveal relationships between conditions and processes. These coding steps should allow us to understand how organisations implement the PDPA under some specific conditions; how organisations maneuver their PDPA implementation processes, and overcome challenges or issues that could hamper the success of the implementation.

Interviews and documents will be analysed immediately after each interview. Data analysis should be conducted as a researcher gathers the data (Chamaz 2008), allowing a researcher to work with the data while it is still fresh. Moreover, further questions, which allow us to gain a deeper understanding of the topic, can emerge from the previous analysis. We will use a 'line-by-line' coding technique to scrutinise the data. Line-by-line coding is suitable for identifying actions (Chamaz 2008), which is deemed appropriate for our research objective and questions. Furthermore, we will do memo writing (see Charmaz 2008) during our analysis to force ourselves to think deeply, be more critical and more analytical when analysing the collected data.

We will use qualitative data analysis software (QDAS) to assist in the analysis. This includes performing open/axial coding on different types of media such as transcripts, recordings, and VDOs, as well as recording our analysis memos.

4. Conclusion

This study builds on the existing literature about the GDPR implementation process. It seeks to gain an in-depth understanding about ways in which organisations comply with the privacy regulations, and the PDPA in particular. We anticipate that the results of this study can be used as PDPA implementation guidelines for many organisations (especially in Thailand). Mechanisms to overcome the challenges identified by this study will also assist organisations in their implementation of the PDPA, within a limited time frame.

5. References

Addis, M. C., and Kutar, M. 2018. "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness.," in *UKAIS*, p. 29.

Almeida Teixeira, G., Mira da Silva, M., and Pereira, R. 2019. "The Critical Success Factors of GDPR Implementation: A Systematic Literature Review," *Digital Policy, Regulation and Governance* (21:4), pp. 402–418.

Ayala-Rivera, V., and Pasquale, L. 2018. "The Grace Period Has Ended: An Approach to Operationalise GDPR Requirements," in *2018 IEEE 26th International Requirements Engineering Conference (RE)*, August, pp. 136–146.

Bangkok Post. 2020. "Most Parts of PDPA to Be Deferred by a Year," https://www.bangkokpost.com/business/1920972/most-parts-of-pdpa-to-be-deferred-by-a-year.

Boban, M. 2018. "Protection of Personal Data and Public and Private Sector Provisions in the Implementation of the General EU Directive on Personal Data (GDPR)," *Economic and Social*

Development: Book of Proceedings, Varazdin Development and Entrepreneurship Agency (VADEA), pp. 161–169.

Charmaz, K. 2008. "Grounded Theory as an Emergent Method," *Handbook of Emergent Methods* (155), p. 172.

Freitas, M. D. C., and Mira da Silva, M. 2018. "GDPR Compliance in SMEs: There Is Much to Be Done," Journal of Information Systems Engineering & Management (3:4), p. 30.

Gabriela, G., Cerasela, S. E., and Alina, C. A. 2018. "The EU General Data Protection Regulation Implications for Romanian Small and Medium-Sized Entreprises," *Ovidius University Annals (Economic Sciences Series)* (18:1), pp. 88–91.

Greenleaf, G., and Suriyawongkul, A. 2019. "Thailand – Asia's Strong New Data Protection Law," SSRN Scholarly Paper No. ID 3502671, SSRN Scholarly Paper, Rochester, NY: Social Science Research Network, 24 September.

Horák, M., Stupka, V., and Husák, M. 2019. "GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ARES '19, New York, NY, USA: Association for Computing Machinery, 26 August, pp. 1–8.

Khan, J. 2018. "The Need for Continuous Compliance," *Network Security* (2018:6), pp. 14–15.

Labadie, C., and Legner, C. 2019. *Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR*, presented at the Proceedings of the 14th International Conference on Wirtschaftsinformatik (2019), 24 February.

Lopes, I. M., Guarda, T., and Oliveira, P. 2019. "Implementation of ISO 27001 Standards as GDPR Compliance Facilitator," *Journal of Information Systems Engineering & Management* (2:4),

Modestum Publications, pp. 1–8.

Magnusson, L., and Iqbal, S. 2018. "Implications of EU-GDPR in Low-Grade Social, Activist and NGO Settings," *International Journal of Business and Technology* (6:3), pp. 1–7.

Miles, M. B., and Huberman, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*, sage.

Polkowski, Z. 2018. "The Method of Implementing the General Data Protection Regulation in Business and Administration," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, , June, pp. 1–6.

Sirur, S., Nurse, J. R., and Webb, H. 2018. "Are We There yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pp. 88–95.

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. 2018. "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies," *Computer Law & Security Review* (34:1), pp. 134–153.

Tzolov, T. 2018. "One Model For Implementation GDPR Based On ISO Standards," in *2018 International Conference on Information Technologies (InfoTech)*, September, pp. 1–3.

Wohlin, C. 2014. "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering," in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, EASE '14, New York, NY, USA: ACM, 38:1–38:10.

Zerlang, J. 2017. "GDPR: A Milestone in Convergence for Cyber-Security and Compliance," *Network Security* (2017:6), pp. 8–11.

Copyright