INSTITUTO
UNIVERSITÁRIO
DE LISBOA

EU Personal Data Protection Standards Beyond Its Borders: An Analysis of the European External Governance through GDPR on Data Protection Laws in the ASEAN Region

Sofia Mira Pereira Jesus Gomes

Master in International Studies

Supervisor:
PhD Luís Nuno Valdez Faria Rodrigues, Full Professor, ISCTE - University Institute of Lisbon

Sofia Martins Geraldes, PhD in History, Security and Defence Studies, ISCTE - University Institute of Lisbon

September, 2024

SOCIOLOGIA
E POLÍTICAS PÚBLICAS

Department of History

EU Personal Data Protection Standards Beyond Its Borders: An Analysis of the European External Governance through GDPR on Data Protection Laws in the ASEAN Region

Sofia Mira Pereira Jesus Gomes

Master in International Studies

Supervisor:
PhD Luís Nuno Valdez Faria Rodrigues, Full Professor, ISCTE - University Institute of Lisbon

Sofia Martins Geraldes, PhD in History, Security and Defence Studies, ISCTE - University Institute of Lisbon

September, 2024

Acknowledgments

The journey of completing this dissertation has been both rewarding and challenging. While I was privileged enough to devote my full attention to it, there were moments when I doubted my ability to succeed. Fortunately, I was surrounded by people who never allowed me to spiral into self-doubt and consistently helped me put things in perspective. To all of them, I express my deepest gratitude.

First and foremost, I would like to thank my advisor, PhD Luís Nuno Valdez Faria Rodrigues, for his guidance throughout this journey. I extend my sincere thanks to my co-supervisor, PhD Sofia Cristina Martins Geraldes, for striking the perfect balance between challenging me to excel and providing much-needed reassurance. Her guidance and constructive feedback were instrumental in refining both my ideas and the quality of this work.

To my family, your unwavering love and belief in me have been my greatest source of strength. A special appreciation goes to my sisters, whose own journeys through graduate studies, under far more challenging circumstances, have been a constant source of inspiration. To my mother, your support has been the foundation upon which all my efforts were built. Your strength and encouragement have been my greatest motivators.

To my friends, your relentless support, infectious laughter, and the joyful moments we shared helped sustain me. Your belief in my abilities convinced me that my dreams were within reach, even during moments of doubt.

A special mention goes to my boyfriend, Yevgeniy, for your endless patience, kindness, and constant companionship. Your support has been a cornerstone of my journey, and I am deeply grateful to have had you by my side every step of the way.

Lastly, I dedicate this work to all those who believed in me, even when my own confidence wavered. May this dissertation serve as a reminder that with determination, perseverance, and the support of a caring community, no challenge is insurmountable.

Resumo

Numa era em que a governação de dados está a moldar cada vez mais as dinâmicas globais e a sua regulamentação tornou-se um ponto de discórdia entre as grandes potências, a União Europeia (UE) tem-se vindo a posicionar como uma autoridade neste contexto. Esta dissertação analisa a influência do Regulamento Geral de Proteção de Dados (RGPD) da UE nos quadros jurídicos de proteção de dados na região da Associação de Nações do Sudeste Asiático (ASEAN), com particular foco em Laos, Singapura e Tailândia. O principal objetivo é avaliar até que ponto os princípios do RGPD foram incorporados nos sistemas jurídicos destes países e analisar os fatores subjacentes a essa influência.

Assente no quadro conceptual da *Governação Externa Europeia*, o estudo explora os mecanismos pelos quais a UE exerce influência regulatória para além das suas fronteiras, com destaque para a *competição*, *aprendizagem*, *emulação* e *socialização.* Através de uma análise temática dedutiva, os dados são sistematicamente categorizados e interpretados, permitindo uma avaliação da adoção do RGPD nos países selecionados.

Os resultados revelam variações significativas no grau de integração do RGPD na região da ASEAN, com cada país a apresentarem níveis variados de convergência regulatória. O estudo conclui que os mecanismos funcionalistas – nomeadamente a competição e a aprendizagem – são os principais impulsionadores da influência do RGPD, em comparação com os mecanismos normativos – como a emulação e a socialização. Esta investigação contribui para uma compreensão mais profunda das complexidades envolvidas na difusão das normas regulatórias europeias, especialmente no domínio da governação internacional da proteção de dados.

Palavras-chave: Proteção de Dados, União Europeia, RGPD, Governação Externa Europeia, ASEAN.

Abstract

In an era where data governance is increasingly shaping global dynamics and its regulation has become a point of contention among major powers, the European Union (EU) has positioned itself as a leading authority in data protection standards. This dissertation investigates the influence of the EU's General Data Protection Regulation (GDPR) on data protection frameworks in the ASEAN region, with a particular focus on Laos, Singapore, and Thailand. The primary aim is to evaluate the extent to which GDPR principles have been incorporated into the legal systems of these countries and to analyze the drivers behind this influence.

Grounded in the conceptual framework of *European External Governance*, the study examines the mechanisms through which the EU exerts regulatory influence beyond its borders, emphasizing *competition, learning, emulation*, and *socialization*. A deductive thematic analysis is employed to systematically categorize and interpret data, allowing for an assessment of GDPR adoption across the selected countries.

The findings reveal significant variations in the degree of GDPR integration within the ASEAN region, with each country exhibiting varying levels of regulatory convergence. The study concludes that functionalist mechanisms – particularly competition and learning – are more prominent drivers of GDPR influence, compared to normative mechanisms such as emulation and socialization. This research contributes to a deeper understanding of the complexities involved in the diffusion of European regulatory standards, particularly in the realm of international data protection governance.

Keywords: Data Protection, European Union, GDPR, European External Governance, ASEAN.

General Index

Index of Tables

Acronyms

ADIX	ASEAN Digital Index
AEC	ASEAN Economic Community
AFTA	ASEAN Free Trade Area
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations/ Associação de Nações do Sudeste Asiático
CCC	Civil and Commercial Code
CJEU	Court of Justice of the European Union
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEG	European External Governance
EU	European Union
EUR	Euro
EUSFTA	EU-Singapore Free Trade Agreement
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IT	Information and Technology
LAK	Lao Kip
Lao PDR	Lao People's Democratic Republic
Laos' LEDP	Laos' Law on Electronic Data Protection

LDC	Least Developed Countries
MCC	Model Contractual Clauses
MCI	Ministry of Communications and Information
MDES	Ministry of Digital Economy and Society
MPE	Market Power Europe
NCPO	National Council for Peace and Order
NSEDP	National Socio-economic Development Plan
OECD	Organization for Economic Co-operation and Development
PDPA	Personal Data Protection Act
PDPC	Personal Data Protection Commission/ Committee
RGDP	Regulamento Geral de Proteção de Dados
SCC	Standard Contractual Clauses
SGD	Singapore Dollar
SME	Small and Medium-sized Enterprise
TELMIN	Telecommunications and IT Ministers Meeting
THB	Thai Baht
UE	União Europeia
UN	United Nations
UNDP	United Nations Development Programme
US	United States
USD	United States Dollars
WP29	Article 29 Data Protection Working Party

Introduction

In an era of rapid globalization and technological advancement, data has become essential to modern society, prompting urgent calls for effective regulation that balances economic potential with individual privacy protection. The European Union (EU) has emerged as a global leader in data protection, with the General Data Protection Regulation (GDPR) being recognized as the most comprehensive and stringent data protection framework in the world. Nonetheless, ongoing geopolitical tensions surrounding data governance, coupled with divergent regulatory approaches from other major powers, such as the United States (US) and China, contribute to a fragmented regulatory landscape.

In light of this, this research seeks to evaluate the extent to which the European Union is a significant and influential actor in the global data protection landscape. The ASEAN region serves as an interesting region to examine the influence of the EU's General Data Protection Regulation (GDPR), due to its strategic position as a contested space among major global powers, its rapidly growing digital economy, heightened concerns over data security, and recent regulatory developments, which underscore its rising prominence in global data governance. To explore the GDPR's influence, the study focuses on three ASEAN Member States – Laos, Singapore, and Thailand – chosen for their recent adoption or updates of comprehensive data protection laws following the GDPR's introduction, and the availability of these legal texts in English.

The central research question guiding this investigation is: **How has the EU's GDPR influenced the development of data protection laws in ASEAN countries?**

To address this question and achieve the research objectives, the research is framed within the conceptual framework of European External Governance, which provides a lens for interpreting how the European Union extends its regulatory influence beyond its borders. A deductive thematic analysis is employed to systematically categorize and interpret the data, facilitating a thorough evaluation of GDPR adoption across the selected countries. The dissertation is further organized into three chapters, ensuring a comprehensive exploration of the research question.

Chapter One fulfills three main purposes by providing contextual background, demonstrating the study's relevance and contribution, and outlining the conceptual and methodological frameworks.

Firstly, begins by tracing the evolution of data privacy and examining the EU's role in global data protection, highlighting its central, yet contested, position in shaping international standards. Furthermore, it focuses on the development of data protection laws within the

ASEAN region, presenting it as a valuable region to assess the influence of the EU's General Data Protection Regulation (GDPR) beyond the EU's borders.

Secondly, this chapter introduces the research goals and the contribution of this study, namely by demonstrating the relevance and the innovation of analyzing the EU's pivotal role in shaping and influencing data protection regulations beyond EU borders. Specifically, the EU's GDPR influence on the development of personal data protection laws within the Association of Southeast Asian Nations (ASEAN).

Thirdly, this chapter identifies and justifies the research design, including the conceptual and methodological frameworks. The study adopts the European External Governance (EEG) framework, which allows for a tighter control for power asymmetries and a less Eurocentric analysis of the EU's influence beyond its borders. Additionally, the study adopts a qualitative approach, applying deductive thematic analysis based on predefined themes, such as key elements of the GDPR and the mechanisms underlying the EU's External Governance.

Chapter Two addresses one of the primary objectives of the study, which is to investigate the degree to which the EU's GDPR has been integrated into the domestic personal data regulations of ASEAN countries.

This chapter begins by providing an overview of the GDPR, including its historical evolution and distinctive features, laying the foundation for a framework of key elements used to analyze GDPR adoption. The second part of the chapter explores the broader context of data protection in ASEAN, analyzing the underlying factors driving regulatory development. This contextual analysis sets the stage for a detailed examination of Laos, Singapore, and Thailand, to assess whether and how they have incorporated GDPR principles into their domestic data protection legislations.

Chapter Three focuses on the second main objective of the study, which is to investigates the mechanisms that determine the extent of the GDPR's influence on domestic regulations within ASEAN. Drawing on the European External Governance framework, the chapter assesses how competition, learning, emulation, and socialization have influenced the adoption of GDPR standards in Laos, Singapore, and Thailand. By analyzing each country individually, the chapter seeks to identify which mechanisms were most influential in shaping data protection laws and whether any barriers hindered the adoption of GDPR principles.

By examining the EU's influence on data protection regulation in ASEAN, this research contributes to broader discussions on global data governance, and the role of the EU as a global actor in the digital age.

Chapter 1 – State of the Art, Research Goals, Methodological and Conceptual Framework

1.1. State of the Art – Studying the influence of the EU data protection regulation in the ASEAN region

This sub-chapter focuses on the importance of studying data regulation, particularly the influence of the European Union's General Data Protection Regulation (GDPR) in the ASEAN region. It starts by discussing the significance of data in modern society and the need for regulation, followed by a historical overview of global personal data protection laws. The EU's regulatory evolution, from the Data Protection Directive (DPD) to the GDPR, is highlighted, emphasizing its role in shaping international data protection standards. The chapter also explores recent data protection developments in ASEAN, given the region's growing digital economy and new regulatory frameworks.

Data, often compared to "oil" in the digital era[1], is now considered a critical asset due to its transformative impact on business and technology. Just as oil transformed industry during the third industrial revolution, data now drives innovation and is crucial for the digital economy, significantly influencing digital services, e-commerce, and advancing technologies such as Artificial Intelligence, machine learning, and predictive analytics. This data revolution marks a significant shift in society, changing how we live, work, and interact (Gao, 2023; World Economic Forum, 2011). Historically, technological advancements have prompted reevaluations of privacy laws, and the current data revolution continues this trend, leading to an expansion of individual rights to protect personal privacy from external intrusions (Sharma, 2019).

One of the earliest articulations of personal privacy was formulated by Sir Edward Coke in 1604, emphasizing that individuals have the right to privacy within their homes. This notion faced challenges with the emergence of print media, prompting Samuel Warren and Louis Brandeis to coin the phrase "the right to be left alone" in 1890, highlighting the need for solitude amid increasing public observation due to modern technology (Sharma, 2019; Warren & Brandeis, 1890).

The right to privacy gained formal international recognition with the 1948 United Nations Declaration of Human Rights (United Nations General Assembly, 1948) and the 1950 European Convention on Human Rights (Council of Europe, 1950), both influenced by the misuse of personal data during World War II, particularly against Holocaust victims. By the

[1] The term was introduced by the British mathematician Clive Humby in 2006 during his presentation titled "Data is the new oil!" at an Association of National Advertisers conference (Palmer, 2006).

1970s Europe and the United States paved the way for the first privacy laws, with Sweden leading the charge in 1973 (Sharma, 2019; Greenleaf, 2017).

Nevertheless, it was not until 1980, that the OECD introduced non-binding guidelines for privacy protection and cross-border data flow, which played a crucial role in standardizing data protection across national jurisdictions despite their lack of legal enforceability (Phillips, 2018; OECD, 1980). This was soon followed by the Council of Europe's Convention 108 in 1981 (Council of Europe, 1981), the first legally binding international privacy instrument, which built on similar principles (Greenleaf, 2012). Together, these documents are regarded by Corning (2024) and Greenleaf (2018, 2014) as the first generation of data protection principles[2] that have influenced numerous comprehensive data privacy laws globally.

In the 1990s, the harmonization of data privacy laws accelerated in Europe with the enactment of the European Community's Data Protection Directive (DPD) (Official Journal of the European Communities, 1995), marking the second wave of data privacy legislation (Corning, 2024; Bennett, 2018; Greenleaf, 2018). The DPD introduced comprehensive privacy principles that were more rigorous than the OECD guidelines and aligned with the Council of Europe's standards, establishing strong European standards for data privacy[3] that influenced global practices and pressured other countries to adopt similar laws during the 1990s and 2000s (Corning, 2024; Greenleaf, 2018, 2017) Consequently, this period saw a worldwide convergence of policies (Bennett, 2018; Greenleaf, 2018; Birnhack, 2008) and a general 'trading up'[4] of regulatory standards (Bradford, 2012; Vogel, 1997).

However, by the end of the first decade of the 21st century, the EU DPD was coming under several pressures. Multinational businesses were frustrated by inconsistent interpretations of data protection principles and the lack of interoperability across Europe (Bennett, 2018). Moreover, alternative approaches to the Directive emerged such as the

[2] For a detailed analysis of the first generation of data protection principles see, for instance: Greenleaf (2014, 2012).

[3] Greenleaf (2012) identifies the ten most distinctive European standards for data privacy as follows: Establishment of an independent Data Protection Authority; Provision for individuals to enforce their data privacy rights through the courts; Restrictions on exporting personal data to countries lacking adequate privacy protection standards; Requirement that data collection be minimized to only what is necessary for the specified purpose; General mandate for fair and lawful processing of personal data, not just its collection; Obligations to notify and, in certain cases, perform prior checks on specific types of data processing systems; Requirement for the destruction or anonymization of personal data after a designated period; Additional safeguards for specific categories of sensitive data; Limitations on automated decision-making and the right for individuals to understand the logic behind automated data processing; Provision for individuals to opt out of the use of their personal data for direct marketing purposes.

[4] The concept of 'trading up' was first introduced by Vogel (1995 apud Vogel, 1997) and refers to the phenomenon where international trade and globalization lead to the adoption of higher regulatory standards across different countries. Vogel argues that in a globalized market, multinational corporations and powerful economic actors, often based in countries with stringent regulations, influence other countries to elevate their regulatory standards to remain competitive and gain access to lucrative markets. Later, Bradford (2012) builds on this assumption to explain the EU's unique ability to unilaterally set global standards, a phenomenon known as the *Brussels Effect*.

Privacy Framework initiated by the Asia-Pacific Economic Cooperation (APEC) in 2005 (Asia-Pacific Economic Cooperation, 2005). Additionally, there was an urgent need to modernize European data protection to stay relevant in the global digital economy (Corning, 2024; Bennett, 2018).

Thus, in 2012, the European Commission proposed the General Data Protection Regulation (GDPR) to enhance citizen protection, foster innovation in the European Single Market, and modernize EU data practices for the digital age, with the regulation being enacted in 2016 and full compliance required by 2018, marking the beginning of the third wave of privacy laws (Corning, 2024; Bennett, 2018; European Commission, 2012).

While building upon prior regulations and guidelines, the GDPR introduced several key innovations in the protection of personal data. Notably, it expanded its territorial scope to apply beyond EU borders, broadened the definition of personal data and included data processors within the regulatory framework. The GDPR also granted individuals enhanced rights, such as the right to data portability and the right to be forgotten, alongside imposing stricter consent requirements. To ensure strict accountability, the GDPR mandated that controllers conducted Data Protection Impact Assessments (DPIAs) and required both controllers and processors to adhere to *privacy by design* and *by default* principles. Moreover, the regulation strengthened the role and powers of supervisory authorities, mandated the appointment of Data Protection Officers (DPOs), required timely data breach notifications, and introduced substantial administrative fines for non-compliance (Carrillo & Jackson, 2022; Bennett, 2018; Synopsys, 2018; Deloitte, 2017; SeeUnity, 2017). Chapter 2 provides an in-depth analysis of these innovations and their rationale in meeting evolving data protection needs.

According to Greenleaf and Cottier (2018), regions outside Europe are increasingly adopting EU-inspired data protection standards, particularly the more stringent '3rd generation' standards set by the GDPR. Greenleaf (2018) and Greenleaf and Cottier (2018) highlight early examples in Asia and Africa of advanced data protection standards; these include Malaysia implementing data portability, Indonesia recognizing the 'right to be forgotten', Mauritania and Niger adopting stricter consent requirements, the Republic of Guinea mandating the appointment of Data Protection Officers, Thailand introducing regulations with extraterritorial implications and Korea enforcing 4% administrative fines.

However, despite agreement among various scholars that there has been a global convergence of data privacy protection standards, and recognizing the EU as the most influential entity in establishing these global standards (Corning, 2024; Bennett & Raab, 2020; Bennett, 2018; Greenleaf, 2018; Birnhack, 2008), some authors caution that a universal data

governance framework remains elusive[5] (Lin, 2024; Gao, 2023; World Economic Forum, 2023; Arner et al., 2021; Obendiek, 2021).

The fragmentation of global data governance frameworks arises from the divergent approaches adopted by the three major economies – the US, the EU, and China – intensified by technological, economic and geopolitical competition (Lin, 2024; Gao, 2023; Arner et al., 2021). Each of these three major economies has established distinct regulatory frameworks and perspectives on personal data, conceptualizing it variously as a fundamental right, an economic asset, or a matter of national security (Gao, 2023).

In the European Union, personal data is regarded as a fundamental right[6] that includes privacy, autonomy, transparency, and non-discrimination, leading to strict protections for individuals and significant obligations for private entities and Member States (Gao, 2023; Aaronson & Leblond, 2018; McDermott, 2017). Meanwhile, in the United States, personal data is seen as an economic asset, leading to a trade-centric approach with minimal cross-border restrictions and limited privacy guidance. The US lacks a comprehensive privacy law, relying instead on sector-specific legislation[7] and self-regulation (Gao, 2023; Aaronson & Leblond, 2018). In contrast, China's approach to personal data emphasizes national security[8], employing stringent domestic laws, including mandatory data localization, to maintain social stability, reinforce Communist Party authority, and promote growth in knowledge-based sectors like artificial intelligence while reducing foreign competition (Gao, 2023; Aaronson & Leblond, 2018).

Within this context of regulatory fragmentation, Gao (2023) astutely emphasizes the vital importance for States of mastering data governance, as it not only positions them at the forefront of digital transformation, but also significantly impacts their influence in global affairs. As personal data governance becomes more politically significant and contentious, regulatory conflicts are shaping transnational data governance and influencing the frameworks adopted by other nations. The major economies – the US, the EU, and China – capitalize on their substantial market shares and early investments to position themselves as leaders in data

[5] The objective of this study is not to explore neither the reasons, nor the consequences, behind the absence of a universal data governance framework. For a detailed discussion on this topic, see: Lin (2024), Gao (2023), Arner et al. (2021), and Obendiek (2021).

[6] The General Data Protection Regulation (Official Journal of the European Union, 2016) is consistent with Article 8(1) of the Charter of Fundamental Rights of the European Union (Official Journal of the European Communities, 2000) and Article 16(1) of the Treaty on the Functioning of the European Union (Official Journal of the European Union, 2012), both of which assert everyone's right to the protection of their personal data.

[7] Some examples are the HIPAA - regulates sensitive patient health information -, FCRA - regulates information collected by consumer reporting agencies -, and VPPA - regulates the disclosure of VHS rental records (Borner, 2023).

[8] As per Article 10 of China's Personal Information Protection Law, it is explicitly forbidden for organizations or individuals to unlawfully collect, use, process, or transmit personal information that jeopardizes national security or public interests (China Briefing, 2021)

regulation, thereby exerting pressure on smaller nations with limited capabilities in data-driven sectors to align with their dominant regulatory frameworks (Gao, 2023; Aaronson & Leblond, 2018). In the evolving global scenario, where a growing number of countries are formulating regulations on personal data – with 162 already having data privacy laws as of 2023 (Greenleaf, 2023) – the inquiry into the regulatory model these regulations will or have already adhered to becomes increasingly significant.

This question holds significant importance within the ASEAN region due to its internal dynamics and its strategic relevance for the US, the EU and China. The relationships between ASEAN and the major international powers have evolved substantially, with China becoming a Strategic Partner in 2003, the United States in 2015[9], and the European Union in 2020. These partnerships underscore a profound commitment to multifaceted cooperation, particularly in areas like the digital economy and cyber-security (European External Action Service, 2024; ASEAN, 2023; Lin, 2023; The White House, 2023). Moreover, as of 2022, China emerged as ASEAN's largest trading partner, with the United States and the European Union following. In Foreign Direct Investment, the United States ranked first, the European Union third, and China fourth (ASEAN Secretariat, 2023),

The strategic importance of the ASEAN region is further highlighted by the rapid expansion of ASEAN's digital economy. In 2020, it grew to approximately 150 billion USD and is projected to reach 1 trillion USD by 2030 (Lee, 2024; Nasution, 2021). Despite the digital economy constituting only 7% of ASEAN's Gross Domestic Product (GDP) – compared to 16% in China, 27% in the European Union-5[10], and 35% in the United States (Tobing, 2022) – ASEAN is poised to become a global leader in the digital economy. Notably, five ASEAN Member States[11] are anticipated to rank among the top 20 fastest-growing digital economies by 2026 (Hawcock, 2022).

Furthermore, the region is one of the most data-rich areas globally, driven by widespread internet accessibility. However, this prosperity is tempered by significant vulnerabilities, as the ASEAN region faces heightened risks of cyberattacks and personal data breaches. In 2022, the Asia-Pacific region, which includes ASEAN, was the most targeted region globally, accounting for 31% of all cyberattacks (Positive Technologies, 2023). This situation is exacerbated by relatively weak security infrastructure, making numerous computers highly susceptible to large-scale attacks (Nasution, 2021; EU-ASEAN Business Council, 2020).

[9] Both China and the US have updated their relationship with ASEAN to a Comprehensive Strategic Partnership in 2021 and 2022, respectively. Nevertheless, it is difficult to establish a clear distinction between a Comprehensive Strategic Partnership and a Strategic Partnership. For further understanding see, for instance: Lin (2023) and Ha (2021).
[10] France, Germany, Italy, Spain, and the United Kingdom
[11] Vietnam (1st), Indonesia (4th), Philippines (9th), Singapore (18th), and Thailand (19th)

In light of these developments, data protection and governance in Southeast Asia have witnessed a noteworthy transformation in recent years. This shift is exemplified by the establishment of key frameworks such as the ASEAN Framework on Personal Data Protection (2016) and the Framework on Digital Data Governance (2018), which underscore the importance of facilitating seamless data flow within ASEAN while fostering a dynamic data ecosystem conducive to innovation and economic expansion.

Building upon these regional frameworks, several countries in the ASEAN region have enacted or updated their privacy laws. Laos implemented its privacy legislation in 2017 (Lao People's Democratic Republic, 2017), followed by Thailand in 2019 (Kingdom of Thailand, 2019), Indonesia in 2022 (Yuriutomo, 2023), and Vietnam in 2023 (Le Ton, 2023). Singapore amended its privacy law in 2020 (Republic of Singapore, 2020). In 2022, Malaysia proposed a Draft Bill to revise its 2010 Personal Data Protection Act, though it remains pending due to the dissolution of Parliament (Christopher & Lee Ong Law Firm, 2023; Ping, 2023). The Philippines has been working on amendments since 2022, but as of 2023, they have yet to be passed (Mundin, 2023). Additionally, Cambodia (Cohen et al., 2023), Brunei (DLA Piper, 2024), and Myanmar (Allen & Gledhill, 2022) have expressed intentions to develop comprehensive personal data protection laws, though none have been enacted so far.

Therefore, among the ASEAN countries, five have established comprehensive[12] laws on data protection - Laos, Thailand, Indonesia, Vietnam, and Singapore -, while three have introduced bills focusing on specific areas of protection - Cambodia, Brunei, and Myanmar. Additionally, two countries are awaiting the enactment of amended comprehensive legislation - Malaysia and the Philippines.

Overall, existing literature underscores that in our increasingly data-driven world, data is profoundly transforming everyday life. This transformation necessitates regulations that facilitate unrestricted data flow while simultaneously protecting individual privacy rights. The European Union has established itself as a leading authority in formulating stringent data protection standards. However, achieving policy convergence with the EU's framework remains a complex challenge due to the fragmentation of global data governance and the differing regulatory approaches of major powers, including the United States, the EU, and China, all of which shape transnational data governance dynamics.

This study does not seek to resolve the ongoing debate regarding the development of a universal data governance framework; instead, it will focus on evaluating whether the EU is a significant influence in shaping personal data regulations beyond its borders. The decision to focus on the EU, rather than other global leaders in data governance, is based on Europe's long-standing role in shaping key international data standards. Notable examples include the

[12] In the context of this study, "comprehensive" refers to laws that are not specific to a particular sector

OECD guidelines and Convention 108, both of which originated in Europe and have been pivotal in establishing global data protection frameworks. Additionally, the EU is recognized for having the most comprehensive and stringent data protection regulations globally, making it a crucial actor in the field.

The ASEAN region serves as an ideal region to examine the influence of the EU's GDPR for two primary reasons. First, it is a contested space among major global powers, providing a neutral ground for assessing influence. Second, ASEAN's rapidly expanding digital economy, pressing data security concerns, and recent regulatory developments highlight its growing importance in the context of data protection.

1.2. Research Question, Goals and Contribution

This sub-chapter presents the research question, objectives, and the study's contributions to the literature on global data governance, with an emphasis on the EU's pivotal role in shaping and influencing data protection regulations beyond EU borders. The study will specifically examine the EU's General Data Protection Regulation (GDPR) and its influence on the development of personal data protection laws within the Association of Southeast Asian Nations (ASEAN).

Thus, this study aims to answer the following research question:

How has the EU's GDPR influenced the development of data protection laws in ASEAN countries?

To thoroughly address this question, it is necessary to unpack and understand both the extent of the EU's GDPR influence and the mechanisms through which this influence occurs. Consequently, two sub-questions arise:

1. **To what extent have the EU's GDPR key elements been incorporated into the domestic personal data laws of ASEAN countries?**

   This sub-question requires analyzing whether the distinctive features and novelties of the GDPR are present in the personal data protection laws of ASEAN countries.

2. **What are the mechanisms through which the EU GDPR is incorporated into the laws of the ASEAN countries?**

   This sub-question involves examining the processes and channels through which the EU data protection standards are transferred to ASEAN countries.

This research provides a significant contribution to the study of international data regulation by offering a novel perspective, both in terms of conceptualization and operationalization.

Regarding conceptualization, this study introduces an innovative approach to analyzing the extent to which GDPR elements have been incorporated into ASEAN countries' data protection laws. Building on the precedent set by previous studies (Carrillo & Jackson, 2022;

Bennett, 2018), the research selects key elements that are distinctive to the GDPR and embody its core principles. These elements will be further detailed and developed in Chapter 2. Moreover, instead of focusing solely on isolated provisions adopted from the GDPR, the study provides a comprehensive assessment of the overall influence of the GDPR's key components on other regulatory systems.

In terms of operationalization, this study presents several innovative approaches. It intentionally moves away from traditional foreign policy analyses of the EU's role as an international actor, recognizing that conventional approaches often neglect the agency of those impacted by EU foreign policy. Additionally, this research does not align with established theories on the EU as a Global Actor like Normative Power Europe (Manners, 2002) or Market Power Europe (Damro, 2011), due to the deficiencies in these approaches, which are discussed in the sub-chapter 1.3.1. Instead, this study employs the *European External Governance* (EEG) framework This approach, rooted in international relations and comparative politics, challenges the notion of the EU as a unitary state actor, favoring an institutionalist perspective on EU external relations (Lavenex & Schimmelfennig, 2009). Further details are discussed in sub-chapter 1.3.1.

Additionally, this study innovatively applies the EEG framework in a context where it has not been commonly used – namely, in analyzing countries geographically distant from the EU. Traditionally, the EEG framework has been applied to the EU's immediate neighborhood or regions where the EU holds particular bargaining leverage. This novel approach allows for a less Eurocentric analysis of the EU's influence and offers a more nuanced consideration of power hierarchies.

This broader application of the EEG framework is particularly relevant in the context of the ASEAN region, which has been chosen for two primary reasons. First, since 2016, ASEAN has experienced a significant increase in the creation or revision of data protection laws, a trend closely linked to the enactment of the GDPR. Second, given ASEAN's geographical distance from the EU and its strong ties with other global powers such as the US and China, the EU's capacity to influence regulations in ASEAN is not a foregone conclusion. Thus, applying the EEG framework to the ASEAN region challenges conventional beliefs regarding the EU's global influence and offers important insights into the broader effects of the GDPR on global data protection practices.

1.3. Research Design

This sub-chapter will provide a comprehensive overview of the conceptual framework underpinning the study, elaborating on the key concepts that inform the research and their operationalization. It will also meticulously outline the methodology selected, including the

research design, data collection methods, and analytical techniques employed, to ensure a robust and rigorous investigation of the research question.

1.3.1. Conceptual Framework

The European Union is frequently characterized as a significant actor within the international system, yet it is distinct from traditional actors, such as States and International Organizations (Bretherton & Vogler, 2013; Cmakalová & Rolenc, 2012; Delaere & Van Schaik, 2012). This uniqueness has spurred the development of various conceptual frameworks to analyze the EU's role as a global power, focusing on its essential characteristics fundamental nature and unique attributes (Damro, 2015; 2012; 2011). This approach was grounded in the belief, articulated by Manners, that *"the most important factor shaping the international role of the EU is not what it does or what it says, but what it is"* (2002, p.252).

In the early 1970s, Duchêne introduced the concept of civilian power to define the European Union's distinctive approach to international politics, which relies on economic, diplomatic, and cultural tools rather than military force to promote a rule-based governance model (apud Schimmelfennig, 2010). Manners (2002) later built on this with the idea of Normative Power Europe, arguing that the EU's influence stems from its ability to shape global norms around peace, freedom, and human rights through ideational factors rather than military or material incentives, reflecting its unique historical context and political-legal structure (Manners, 2009). Damro (2011; 2012) countered that the single market is fundamental to the EU's identity, asserting that its influence is primarily driven by the size of its internal market, regulatory power, and interest group pressures.

However, as noted by Schimmelfennig (2010), the debates surrounding the EU's identity pose significant challenges for studying its external influence for several reasons. First, these debates are partly influenced by the EU's self-portrayal, which is both descriptive and prescriptive, indicating that its identity may be constructed rather than accurately reflecting its true influence. Second, the multidimensionality of these debates – encompassing the means, ends and impact – misleadingly implies that the EU operates in a coherent and linear manner, where its objectives consistently align with its methods and outcomes; in reality, the EU may pursue civilian goals, such as regional stability, through military means. Finally, the EU's goals and methods in global politics are dynamic, varying over time, across different countries and regions, and policy fields, making them difficult to capture with uniform labels or to attribute solely to the EU's ontological quality. (Lavenex & Schimmelfennig, 2009).

Therefore, as Smith aptly noted, *"We should instead engage in a debate about what the EU does, why it does it, and with what effect, rather than about what it is"* (apud Schimmelfennig, 2010, p.6). To move beyond the essentialist debate over the EU's core

identity and focus on the procedural analysis of how the EU engages in rule projection, this study adopts the conceptual framework of *European External Governance* (EEG) (Lavenex, 2014).

Initially, the research agenda of *European External Governance* focused primarily on the impact of European integration and governance on the Member States of the European Union, a process defined as Europeanization (Schimmelfennig, 2010). According to Radaelli, Europeanization involves the *"processes of (a) construction, (b) diffusion, and (c) institutionalization of formal and informal rules, procedures, policy paradigms, styles, 'ways of doing things,' and shared beliefs and norms, which are first defined and consolidated in the making of EU decisions and then incorporated into the logic of domestic discourse, identities, political structures, and public policies"* (2004, p. 3).

Over time, however, EEG evolved to encompass "*the expansion of EU rules beyond EU borders*" (Lavenex & Schimmelfennig, 2009, p. 807). Consequently, several studies broadened the scope of Europeanization to include "quasi-Member States" such as Norway and Switzerland, as well as candidate States for EU membership (Schimmelfennig, 2015; Tonra, 2015). More recently, this research has extended beyond membership candidates to include discussions about the EU's immediate neighborhood (Dimitrova & Dragneva, 2009; Petrov, 2006; Christiansen et al., 2000) and even more distant countries (Rousselin, 2012).

Throughout these studies, it has become noticeable that geographical proximity to the European Union plays a crucial role in shaping the impact of EEG. Lavenex (2011) and Schimmelfennig (2010) conceptualize this relationship through the framework of concentric circles, which posits that the EU's influence and the intensity of its relations with neighboring countries diminish as distance from the EU increases. Still, Lavenex (2014, 2011) and Schimmelfennig (2015, 2010) consider that other determinants may trump the geographic logic[13].

These observations raise essential questions on the EEG literature, namely: How does EU influence beyond EU borders occur? What are the mechanisms and processes through which the EU disseminates its rules of governance in the wider international system? Several largely overlapping classifications of *European External Governance* mechanisms have been proposed in the literature (Schimmelfennig, 2015; Lavenex, 2014; Rousselin, 2012; Schimmelfennig, 2010; Schimmelfennig & Sedelmeier, 2004), along with policy diffusion conceptualizations that enrich the discussion (Börzel & Risse, 2012).

[13] Lavenex (2011) acknowledges that the sectoral logic (differentiation of external governance by policy areas) trumps the geographic logic beyond the EU's immediate neighborhood. This sectoral logic gives rise to the functionalist extension driven by socio-economic interconnections and interdependence, on the one hand, and socialization and lesson-drawing with the help of transgovernmental networks, on the other (Lavenex, 2014). In Schimmelfennig opinion (2015, 2010), the most important conditions cutting across the concentric circles of Europeanization are market share and supranational regulation.

For instance, Schimmelfennig and Sedelmeier (2004) categorize mechanisms of Europeanization along two primary dimensions: the source of influence – which can be EU-driven or domestically driven – and the underlying institutional logic – which can be consequential or appropriateness-based. The *logic of consequences* assumes that actors select behaviors that maximize their utility given the circumstances, while the *logic of appropriateness* posits that actors choose behaviors deemed appropriate according to their social roles and norms. Under the *logic of consequences*, the EU directly influences through an *external incentives model*, which primarily uses conditionality; the EU sets rules and conditions, rewarding compliance and sanctioning non-compliance. In contrast, under the *logic of appropriateness*, EU influence occurs through *social learning*, where States are persuaded to adopt EU rules they perceive as legitimate and aligned with their identification with the EU, or through *lesson-drawing*, where States adopt rules expecting them to effectively address domestic policy challenges.

Schimmelfennig (2010) further reinforces this study but introduces a key distinction within the *logic of consequences* between *conditionality* and *externalization*. *Conditionality* is a direct mechanism of external governance, where the EU influences other actors' cost-benefit analyses by setting governance rules as conditions for rewards or sanctions. *Externalization*, on the other hand, is an indirect mechanism where the EU's impact on external actors' cost-benefit calculations occurs without active promotion of its governance model. Instead, the EU's presence as a market and regional governance system generates externalities that influence other actors, often in unintended or unforeseen ways.

Börzel and Risse (2012) expand the framework of EEG by introducing the *logic of arguing* alongside the existing logics of consequences and appropriateness. They define arguing as the process of reason-giving and challenging the legitimacy of norms, characterizing it as a scenario where actors seek to persuade one another. They distinguish between persuasion, which advocates for ideas as legitimate or true through rational discourse, and socialization, where ideas are communicated via an authoritative model.

Lavenex (2014) further enriches the study of EEG by contrasting it with EU foreign policy, asserting that the latter is characterized by cohesive, coordinated interactions among states at the intergovernmental level, employing hierarchical mechanisms such as *conditionality* and *legal authority* to exert coercive control over non-Member States. In contrast, defines EEG as a functionalist extension that operates transnationally, marked by decentralized, sectoral interactions, and identifies its mechanisms as *learning*, *socialization*, *emulation*, and *competition*, drawing on existing literature.

In line with Lavenex, Rousselin (2012) advocates for an EEG framework that prevents predetermined EU dominance and conditionality imposition. This revised framework introduces new assumptions about rule importers' domestic preferences, which include

incentive-driven choices (maximizing rewards or minimizing sanctions), value-driven choices (prioritizing legitimacy), and solution-driven choices (focusing on the effectiveness of rules in addressing domestic issues).

Given the significant overlap among these conceptual frameworks, this study chooses to adopt mechanisms that integrate both direct and indirect approaches while distinguishing between instrumental and normative rationales. The study excludes the logic of persuasion defined by Börzel and Risse (2012), as distinguishing between persuasion and socialization can be challenging. The study opts to focus solely on socialization, as defined by scholars like Schimmelfennig (2010) and Schimmelfennig and Sedelmeier (2004), who consider persuasion as integral to the socialization process[14]. Moreover, as highlighted by Lavenex (2014), Rousselin (2012), and Börzel and Risse (2012), countries situated further from the EU and without aspirations for EU membership do not experience the influence of conditionality or significant hierarchical dynamics. Consequently, this study excludes coercion, conditionality and legal authority as relevant mechanisms.

Therefore, this study opts for the following conceptual framework:

Table 1 - European External Governance Mechanisms.

	Direct mechanisms	Indirect mechanisms
Instrumental logic		**Competition** (incentive-driven preferences)
		Learning (solution-driven preferences)
Normative logic	**Socialization**	**Emulation** (value-driven preferences)

Competition stands out as the predominant mechanism supporting the diffusion of market regulations. The EU's sheer economic presence is recognized to exert significant influence, bolstered by its regulatory enforcement capabilities and advocacy efforts by interest groups that transform economic pressures into political demands (Damro, 2015, 2012, 2011).

[14] "*Socialization encompasses all EU efforts to disseminate European governance by persuading external actors of the underlying ideas and norms*" (Schimmelfennig, 2010, p.9).

Moreover, Bradford (2012) argues that the EU's impact is amplified when it imposes stringent rules[15] of inelastic targets[16], such as consumer markets.

Nevertheless, global standards only become established when adhering to a single standard outweighs the benefits of exploiting weaker regulations in more lenient jurisdictions. Consequently, third countries align with EU legislation not due to direct EU demands, but because their businesses and regulators anticipate adverse consequences if they do not comply, prompting them to select rules offering the highest rewards or the lowest sanctions (Lavenex, 2014; Schimmelfennig, 2015, 2010; Rousselin, 2012). This phenomenon, described by Bradford (2012) as the *de facto Brussels Effect*, is reinforced as export-oriented firms lobby their governments to adopt similar standards, thereby implementing a *de jure Brussels Effect*.

In contrast to competition, *learning* arises from domestic dissatisfaction with the status quo. It begins when actors encounter specific political or economic challenges that necessitate institutional change (Schimmelfennig & Sedelmeier, 2004). While competition involves compliance with rules for incentives, learning is driven by the search for effective solutions to these problems. Thus, actors explore institutional alternatives that best fit their specific circumstances (Börzel & Risse, 2012; Rousselin, 2012). Schwartz (2019) notes that the EU's highly transplantable legal model enhances this learning mechanism, as it is often adopted due to its ease of enactment and comprehensiveness.

Socialization and *emulation* mechanisms both involve actors aligning with EU rules because they perceive them as legitimate or normatively superior (Lavenex, 2014; Schimmelfennig, 2010). This perception is central to Manners' (2002) argument about the EU's exemplary role and the influence of transnational actors in norm diffusion. Schwartz (2019) further notes that EU data protection laws have gained significant recognition. The public discourse on consumer privacy has evolved dramatically, leading many important institutions and individuals in non-EU jurisdictions to acknowledge the merits of EU-style data protection. However, while *socialization* suggests direct EU efforts to persuade other countries of its normative values (Schimmelfennig, 2010), *emulation* depends more on a country's pre-existing beliefs and practices. Therefore, a country's perception of the EU's legitimacy may depend on

[15] Bradford (2012), notes that strict regulation is more prevalent in high-income countries because wealthier nations can afford to prioritize consumer protection over corporate profitability. However, variations exist even among affluent countries regarding their willingness to engage in regulatory intervention. To function as a global regulator, a state must uphold stringent domestic standards, a principle exemplified by the EU, which reflects its policymakers' aversion to risk and commitment to a social market economy.

[16] Bradford (2012) explains that inelastic targets refer to consumer groups that cannot easily relocate to regions with looser regulatory standards, forcing companies to adhere to existing regulations to operate within the EU's single market. Unlike mobile capital, consumer markets are less flexible By prioritizing consumer market regulations, the EU has established itself as a global standard-setter, creating regulations that remain robust against market forces and capital mobility.

how closely EU norms align with its own values and practices (Lavenex & Schimmelfennig, 2009).

In conclusion, this conceptual framework synthesizes the key mechanisms identified in the literature on European External Governance, which explain how the EU exerts influence beyond its borders. By focusing on competition, learning, socialization, and emulation, it provides a comprehensive lens through which to examine the diffusion of the EU's GDPR in ASEAN countries.

1.3.2. Methodology

This study adopts a qualitative research approach and employs a deductive thematic analysis, a specific type of document analysis, as a systematic method to examine the influence of the EU's General Data Protection Regulation beyond its jurisdiction, specifically its influence on the development of personal data protection laws in the ASEAN region. This method involves selecting, analyzing, and interpreting data by categorizing it into predefined themes (Proudfoot, 2023; Armstrong, 2022). This methodological choice enables targeted exploration of key areas of interest, facilitating in-depth analysis of the phenomenon of regulatory adoption (Atlas.ti, n.d.).

The research is structured into two distinct phases, each addressing specific sub-questions aligned with the study's objectives.

The first phase, covered in Chapter 2, investigates the extent to which ASEAN countries have incorporated the EU's GDPR key elements into their domestic laws on personal data protection, addressing the first sub-question of this study. Primary sources, specifically the GDPR and the personal data laws of ASEAN countries, serve as the main documents analyzed for this purpose. To provide a comprehensive and nuanced analysis, secondary sources such as academic articles and supplementary guidelines related to these regulations are also utilized.

Due to the fact that updated comprehensive data protection laws exist in only five of the ten ASEAN countries, and with only three of these being available in English, the study narrows its focus to a selected sample: the Lao People's Democratic Republic (PDR), Singapore, and Thailand.

The study systematically evaluates the integration of key GDPR elements – our predefined themes – into the legislation of Laos, Singapore, and Thailand, to determine the extent to which these GDPR standards are reflected in ASEAN laws. The selected key elements include broadened definitions of personal data, rights to data portability and to be forgotten, stricter consent requirements, expanded territorial scope, inclusion of data processors within the regulatory framework, adherence to *privacy by design* and *privacy by default* principles, enhanced role of supervisory authorities, conduction of Data Protection Impact Assessments

(DPIAs), mandatory appointment of Data Protection Officers (DPOs), notification of data breaches, and substantial administrative fines.

While not exhaustive of all GDPR innovations, these selected elements encapsulate the core features of Europe's advanced data privacy approach. They are distinguishable by their novelty and direct representation of GDPR principles, making verification straightforward. Chosen for their clarity and relevance, these elements serve as benchmarks for assessing how well GDPR standards have been incorporated into ASEAN legal frameworks. By checking whether these obligations are reflected in the domestic laws of the ASEAN countries studied, we can gauge the extent of GDPR influence.

Annexes A to L systematically present the key elements of the GDPR in a series of tables. Each table is organized into four columns, corresponding to the regulations of the EU, Lao PDR, Singapore, and Thailand. This format enables a clear comparison of the similarities and differences among the key elements. The tables provide direct transcriptions of the relevant articles and sections from the regulations, without any preliminary interpretation. A detailed analysis and interpretation of these provisions are conducted in Chapter 2.

In the second phase of the study - Chapter 3 -, the focus shifts to exploring the mechanisms through which the EU GDPR is integrated into ASEAN regulations, directly addressing the second sub-question defined in the study's objectives. This part of the study utilizes a combination of primary sources – including international trade databases, and official documents, speeches, and press releases from ASEAN, the countries under analysis (Lao PDR, Singapore, and Thailand), as well as EU institutions – as well as secondary sources, including media articles and academic literature.

The analysis seeks to identify information relevant to the predefined themes derived from the conceptual framework established through literature synthesis. This framework emphasizes aspects such as *competition*, *learning*, *emulation*, and *socialization*, drawing on key contributions from the literature on *European External Governance*, including the works of Lavenex (2014), Börzel and Risse (2012), Rousselin (2012), and Schimmelfennig (2010).

The selected concepts provide a multidimensional perspective on EU rule transfer by considering both the EU's unilateral efforts and the agency of rule importers. They differentiate between functionalist and normative logics, allowing for the inclusion of rationalist approaches that view actors as strategic utility-maximizers and constructivist approaches that consider how internalized identities influence choices (Schimmelfennig & Sedelmeier, 2004). Overall, this conceptual framework is comprehensive enough to encompass all relevant mechanisms through which the EU can influence rule adoption in third countries, while also offering a clear and targeted approach for data analysis.

Chapter 2 – The incorporation of EU's GDPR into the domestic data protection laws of ASEAN countries

This chapter addresses the first su-research question posed in sub-chapter 1.2: To what extent have the EU's GDPR key elements been incorporated into the domestic personal data laws of ASEAN countries?

This chapter is divided into two parts. In the first part, we introduce an overview of the EU's General Data Protection Regulation, providing an historical evolution and highlighting its novel elements and distinctive characteristics. This contextualization sets the foundation for developing a framework of *key elements* which will be used in subsequent sections to analyze the incorporation of the GDPR into the domestic regulations of ASEAN countries in a nuanced manner. The second part of this chapter analyzes the data protection regulatory framework in ASEAN countries, aiming to provide a broad understanding of regulatory developments in this region. It then focuses on specific countries – Lao PDR, Singapore, and Thailand – to determine whether and how they incorporate the key elements of the GDPR into their domestic regulations.

Both sections of this chapter are supplemented by Annexes A to L, which provide direct transcriptions of relevant articles and sections from the regulations. These annexes are designed to facilitate a clear and comparative visual analysis of the regulations.

2.1. Overview of the GDPR and key elements

The General Data Protection Regulation (GDPR), known as the world's most stringent privacy law (Greenleaf, 2021; Rustad & Koenig, 2019), is rooted in Europe's extensive history of privacy protection, beginning with the 1950 European Convention on Human Rights (Council of Europe, 1950), which established the right to respect for private life. This fundamental right has been the basis for the European Union's continuous legislative efforts to safeguard privacy (Wolford, n.d.).

In response to the technological advancements of the 1990s and the rise of the internet, the European Union adopted the 1995 European Data Protection Directive to update its data protection framework. This directive established minimum privacy and security standards across EU Member States, which implemented it through national laws (Wolford, n.d.). Together with Convention 108[17], it laid the groundwork for the GDPR (Greenleaf, 2012;

[17] Opened for signature in 1981, the Convention 108 was the first legally binding international instrument for data protection. It requires parties to incorporate its principles into domestic legislation to uphold fundamental human rights concerning personal data processing. The official document of the

Wolford, n.d.), introducing key provisions such as the establishment of independent Data Protection Authorities, individual enforcement of privacy rights, restrictions on data exports, data minimization, and obligations for fair processing. It also mandated notifications for certain data processing, required data destruction or anonymization after a specified period, provided safeguards for sensitive data, limited automated decision-making, and granted individuals the right to understand processing logic and opt out of direct marketing (Hustinx, 2014, Greenleaf, 2012).

At the beginning of the second millennium, concerns about the effectiveness of the Directive prompted assessments of its implementation and the potential need for amendments. The primary issues identified included the inconsistent application of the Directive across Member States and its inability to remain relevant in light of rapid technological advancements (Hustinx, 2014; Robinson et al., 2009). In response to these challenges, the European Commission presented a comprehensive set of proposals in 2012 aimed at overhauling the EU's 1995 data protection framework. These proposed reforms sought to adopt a human rights-centered approach, with the objectives of strengthening individual rights, enhancing enforcement mechanisms, improving the internal market's functioning, and addressing emerging global data protection challenges (European Commission, 2020a; European Commission, 2012). After several years of extensive consultation and drafting, the General Data Protection Regulation (GDPR) was adopted in 2016 and came into effect in 2018, thereby significantly expanding and fortifying the legal framework originally established by the Data Protection Directive.

The subsequent sections will analyze the innovative elements introduced by the General Data Protection Regulation (GDPR). Scholars such as Carrillo and Jackson (2022) and Bennett (2018) highlight these elements as distinctive features that can serve as critical criteria for evaluating the regulation's impact and effectiveness.

2.1.1. Broadened Personal Data Definition

At the heart of the General Data Protection Regulation (GDPR) is the concept of personal data, which covers any information that can identify a living individual, directly or indirectly. The GDPR expands the definition of personal data beyond traditional identifiers like name and address to include information such as IP addresses, geolocation data, biometric data, and cultural and social identity markers[18] (Corning, 2024).

The expanded definition was introduced to clarify and more precisely delineate what qualifies as identifiable information in response to modern technological advances. While some

Convention 108 can be accessed through the link: https://rm.coe.int/1680078b37. For a more in-depth analysis of the Convention, see, for instance: Greenleaf (2012)

[18] General Data Protection Regulation 2016, art. 4(1); recs. 26, 27

data types were already informally considered personal, their official inclusion in the law came after thorough legal debate. This ensures that data previously treated as personal is now formally recognized and regulated (Purtova, 2018; Kefron, 2016).

Moreover, the GDPR delineates specific categories of sensitive personal data, such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometric data, health information, and information concerning an individual's sexual orientation[19]. These categories warrant enhanced protection, due to the significant risks their processing poses to fundamental rights and freedoms[20]. For instance, biometric data, including fingerprints and facial recognition, is increasingly used in access control systems and various applications, raising significant privacy concerns and emphasizing the need for strict safeguards (Kefron, 2016).

The GDPR also encourages the use of *pseudonymization*, which refers to personal data that can no longer be attributed to a specific data subject[21] without additional information. This pseudonymized data may be processed, provided that technical and organizational measures are in place to ensure it cannot be attributed to a specific individual[22] (Bennett, 2018).

Therefore, to fully incorporate the cornerstone concept of the GDPR, the selected countries' national laws must have an understanding of personal data that extends beyond traditional identifiers, clear delineation of sensitive data categories, and policies for handling pseudonymized information.

2.1.2. Right to Data Portability

The General Data Protection Regulation (GDPR) introduces new privacy rights for data subjects, including the right to data portability. This right enables individuals to receive their personal data in a structured, commonly used, and machine-readable format, and to transfer it directly to another controller where technically feasible. For example, individuals can use this right to switch between services like iTunes and Spotify, bringing their data and usage history with them (EPSU, 2019). However, data portability applies only when the original data controller[23] based the processing on either consent or the performance of a contract, and when the data is processed through automated means[24].

[19] General Data Protection Regulation 2016, art. 9; recs. 10, 51-54
[20] General Data Protection Regulation 2016, rec. 51
[21] According to Article 4(1) of the General Data Protection Regulation (Official Journal of the European Union, 2016), a *data subject* is defined as an "*identified or identifiable natural person*"
[22] General Data Protection Regulation 2016, art. 4(5); recs. 26, 28-29
[23] According to Article 4(7) of the General Data Protection Regulation (Official Journal of the European Union, 2016), a *data controller* is a "*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*"
[24] General Data Protection Regulation 2016, art. 20; recs. 68, 73

This reform serves two primary purposes. It enhances individuals' control over their personal data to build trust in how their information is handled. Additionally, it encourages the free flow of data and fosters competition by lowering switching costs, enabling start-ups and smaller companies to compete with larger digital firms and attract consumers with privacy-friendly solutions (Carrillo & Jackson, 2022; European Commission, 2015).

To determine the extent to which this right has been incorporated into the national laws of the selected countries, it is necessary to identify whether the right is explicitly recognized and established within their legal frameworks.

2.1.3. Right to be Forgotten

Another significant right established by the General Data Protection Regulation (GDPR) is the right to erasure, also known as the right to be forgotten. This right stems from the 2014 Court of Justice of the European Union (CJEU) ruling in Google Spain SL v Costeja, Case C-131/12. In this landmark decision, the CJEU recognized the right to be forgotten, inferred from the rights to erasure and blocking of data outlined in Directive Article 12(b) and the right to object in Article 14(a). The Court held that if certain information is deemed "*inadequate, irrelevant, no longer relevant, or excessive*" for the purposes of data processing by a search engine operator, the related information and links must be removed from search results (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014, point 94).

This ruling has been explicitly incorporated into the GDPR, codifying the right to erasure. Under the GDPR, individuals can request the deletion of their personal data when certain conditions are met, such as when the data is no longer needed, consent is withdrawn, the individual objects to processing, or the data has been unlawfully processed. The GDPR also enforces strict notification requirements for the erasure or restriction of personal data processing[25] (Carrillo & Jackson, 2022).

Thus, to evaluate the incorporation of this right into the national laws of the selected countries, it is essential to verify whether the right is explicitly acknowledged and codified in their legal systems.

2.1.4. Stricter Consent Requirements

The General Data Protection Regulation (GDPR) has substantially raised the standards for determining the lawfulness of data processing, particularly by introducing stricter consent requirements to ensure that consent functions as a more effective safeguard for data protection rights (Carrillo & Jackson, 2022; Carolan, 2016). This is especially crucial in the realm of online

[25] General Data Protection Regulation 2016, art. 17; recs. 59, 65-66

data protection, where traditional legal frameworks for consent have often fallen short, as individuals frequently do not fully comprehend the nature or scope of what they are consenting to (Carolan, 2016).

Under the GDPR's revised consent provisions, consent must be freely given, specific, informed, and clearly expressed as the data subject's genuine intent. Consent is not deemed freely given if the data subject lacks a real choice or faces negative consequences for refusing or withdrawing consent[26]. Besides, practices such as silence, pre-ticked boxes, or inactivity do not meet the criteria for valid consent (Bennett, 2018).

Importantly, under the GDPR, individuals have the right to withdraw their consent at any time[27], a principle that ensures data subjects can revoke consent as easily as they provide it. This right is essential for evaluating compliance with the GDPR's stringent standards and serves as a key indicator of whether a jurisdiction has effectively implemented these rigorous consent requirements (Carrillo & Jackson, 2022).

2.1.5. Expanded Territorial Scope

The General Data Protection Regulation (GDPR) marks a transformative shift in data protection by extending its jurisdiction beyond the EU's borders. This change responds to the challenges posed by the Internet, which has facilitated cross-border data transfers, and the questionable use of such data by companies like Facebook. Issues such as Facebook allowing companies to track user purchases, share this information without consent, and expose private data without warning have underscored the need for stronger regulations (Newcomb, 2018; Gibbs, 2015).

To address these concerns, the GDPR's expanded territorial scope applies to any organization, regardless of location, that offers goods or services to EU residents or monitors their behavior[28] (De Hert & Czerniawski, 2016). This approach closes previous loopholes, ensuring that all entities handling the personal data of EU residents must comply with GDPR standards or face significant penalties, including potential exclusion from the EU market. By extending its reach globally, the GDPR has substantially amplified its influence, reshaping international data protection practices (Corning, 2024; Carrillo & Jackson, 2022).

Accordingly, this element is considered incorporated when ASEAN countries extend their regulatory frameworks to include extraterritorial provisions.

[26] General Data Protection Regulation 2016, arts. 4(11), 7; rec. 42
[27] General Data Protection Regulation 2016, art. 7(3)
[28] General Data Protection Regulation 2016, art. 3

2.1.6. Expanded responsibilities and accountability of Data Processors

The General Data Protection Regulation (GDPR) represents a significant advancement over the Data Protection Directive by extending its scope to regulate data processors – entities that handle data on behalf of controllers[29]. For instance, a marketing company hired by another company to collect email addresses through third-party websites is classified as a data processor (European Data Protection Board, n.d.a.) This expansion addresses the complexities of today's digital landscape, where data collection and storage are ubiquitous. As controllers rely more on processors for personal data management, it is essential to impose legal obligations on both parties to ensure comprehensive data protection (Lobo, 2023).

In light of this, while primary responsibility typically lies with the data controller, the GDPR also imposes specific responsibilities and accountability on processors (Carrillo & Jackson, 2022). This includes conducting processing operations using appropriate technical and organizational measures as instructed by the controller, thereby assisting in GDPR compliance [30]. The controller-processor relationship must be governed by a contract that documents processing operations and methods for handling personal data[31] (European Data Protection Board, n.d.b.)

Additionally, processors are obligated to maintain comprehensive records of processing activities[32], cooperate with data protection authorities[33], promptly report data breaches[34], and appoint a data protection officer (DPO)[35] (European Data Protection Board, n.d.b.). These measures collectively strengthen accountability and transparency in data processing practices under the GDPR.

Therefore, for full integration of this GDPR element, ASEAN countries regulations must acknowledge processors as significant entities and assign them analogous responsibilities.

2.1.7. *Privacy by Design* and *Privacy by Default*

In 2009, the Article 29 Data Protection Working Party[36] (WP29) observed that technological advancements had increased privacy risks and recommended integrating the principle of *privacy by design* into legislative frameworks. This principle involves embedding privacy and data protection into the design of Information and Communication Technologies (ICT).

[29] General Data Protection Regulation 2016, art. 4(8)
[30] General Data Protection Regulation 2016, art. 28; rec. 81
[31] General Data Protection Regulation 2016, art. 28(3)
[32] General Data Protection Regulation 2016, art. 30(2)
[33] General Data Protection Regulation 2016, art. 31
[34] General Data Protection Regulation 2016, art. 33(2)
[35] General Data Protection Regulation 2016, art. 37(1)
[36] Established under the Data Protection Directive, the Article 29 Dara Working Party addressed privacy and personal data protection issues until 25 May 2018, when it was succeeded by the European Data Protection Board (European Data Protection Board, n.d.c.)

Although the previous Directive encouraged these measures, implementation had been lacking. WP29 proposed that the new legal framework adopt privacy by design as a core principle, ensuring default privacy protections in ICT products and enhancing enforcement powers for Data Protection Authorities (WP29, 2009). Accordingly, the GDPR introduced this proposal, encouraging data controllers to implement internal policies that reflect the principles of *data protection by design and by default*[37].

Data protection by design involves the proactive integration of effective technical and organizational measures, along with ethical considerations, to ensure privacy. The European Data Protection Authority states that personal data processing using IT systems should stem from a carefully planned design process. *Data protection by default* compels controllers to limit the collection and processing of personal data to what is strictly necessary for each specific purpose, ensuring compliance with legal requirements and transparent communication with data subjects. This approach eliminates the need for individuals to take extra steps to protect their privacy (EPSU, 2019). Key measures of *data protection by design and default* include data minimization, pseudonymization, transparency, enabling data subjects to monitor data processing activities, and enabling controllers to create and improve security features[38].

Furthermore, in the development, design, selection, and utilization of applications, services, and products that involve personal data processing, producers are also encouraged to prioritize data protection from the outset[39]. This means that organizations must restrict data processing to what is essential for their operational tasks, restrict employee access to only necessary personal data, and maintain thorough documentation of their privacy by design practices. Additionally, conducting data protection impact assessments is essential for activities that present higher risks (Heiman, 2020).

Incorporating the principles of *data protection by design and by default* into ASEAN regulations would require these principles to be formally embedded within the laws themselves. This would legally obligate organizations handling personal data to follow these principles, rather than just encouraging or promoting them as optional best practices.

2.1.8. Strengthened tasks and responsibilities of Supervisory Authorities

The General Data Protection Regulation (GDPR) represents a major step forward in data protection, strengthening the role of national supervisory authorities as the primary bodies responsible for overseeing and enforcing the application of EU data protection regulations[40]. This reform was prompted by several legal cases that emerged during the period when the

[37] General Data Protection Regulation 2016, art. 25
[38] General Data Protection Regulation 2016, rec. 78
[39] Ibid 39
[40] General Data Protection Regulation 2016, art. 51

Data Protection Directive was in force, which were brought before the Court of Justice of the European Union. These cases underscored the need for a more comprehensive regulatory framework, particularly in ensuring the independence of supervisory authorities[41] and providing greater clarity regarding their competences and enforcement powers[42]. The GDPR addressed these concerns by harmonizing the functions of supervisory authorities, establishing clear and robust powers, and creating mechanisms for cooperation in cross-border cases (Giurgiu & Larsen, 2016).

While the DPD based the competence of supervisory authorities on national laws, the GDPR mandates that all supervisory authorities adhere to the regulation and have their independence reinforced against both direct and indirect external influences[43] (Giurgiu & Larsen, 2016; GDPR Hub, n.d.). The GDPR also introduces a comprehensive set of clearly defined tasks and powers that apply equally to all European supervisory authorities. These responsibilities include monitoring compliance with the Regulation, handling complaints, advising on data processing matters, and raising public awareness about data protection[44]. Their powers are categorized into three main types[45]: investigatory powers, such as conducting investigations and compelling controllers or processors to provide information; authorization and advisory powers, including the accreditation of certification bodies; and corrective powers, which enable them to impose administrative fines – a function that was previously left to national law. These corrective powers, particularly the ability to issue fines, are among the most forceful and coercive tools available to supervisory authorities (Giurgiu & Larsen, 2016).

Moreover, a notable improvement over the previous Directive was the introduction of the one-stop-shop mechanism, which improves cooperation among supervisory authorities across EU countries, reducing administrative burdens for organizations and aiding individuals in exercising their rights from their home countries (European Data Protection Board, 2021). When data subjects in one EU Member State are significantly impacted by processing activities in another, the local supervisory authority[46] must quickly notify the lead supervisory authority[47], which then determines whether to collaborate with the local authority or let it manage the case independently[48] (Bennett, 2018; Sponselee & Mhungu, n.d.). If consensus cannot be reached,

---

[41] The matter was addressed in the landmark case of *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14, 2015). The full case details can be accessed at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362

[42] The issue was examined in the case of *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Case C-230/14, 2015). The full judgment is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0230

[43] General Data Protection Regulation 2016, arts. 51-54

[44] General Data Protection Regulation 2016, art. 57

[45] General Data Protection Regulation 2016, art. 58

[46] Referring to the supervisory authority of the Member State where the data subject resides.

[47] Referring to the supervisory authority of the Member State where the data controller or processor has its main establishment, which is the location decisions regarding the data processing are made.

[48] General Data Protection Regulation 2016, recs. 127-129

the case is referred to the European Data Protection Board, which issues a binding decision on GDPR interpretation[49] (EPSU, 2019).

For full integration of this GDPR element, ASEAN countries laws would need to establish independent supervisory authorities with comparable responsibilities. However, it is not expected that they adopt a cooperation mechanism akin to the GDPR's one-stop-shop, as this model is designed for the EU's multi-state structure and may not fit ASEAN's regulatory framework.

2.1.9. Data Protection Impact Assessment

The Data Protection Directive mandated that supervisory authorities be notified of all personal data processing activities, which often resulted in administrative and financial burdens without necessarily enhancing data protection. In contrast, the General Data Protection Regulation (GDPR) introduces a mandatory Data Protection Impact Assessment (DPIA) for high-risk processing operations, aimed at evaluating the likelihood and severity of potential risks to individuals' rights and freedoms. High-risk processing operations include those involving new technologies or any processing likely to result in a high risk to individuals' rights and freedoms. Examples include processing sensitive personal data, automated profiling, or large-scale data processing[50] (Carrillo & Jackson, 2022).

A DPIA must be conducted by the controller and should include a description of the processing activities, an assessment of the necessity and associated risks, and the measures implemented to mitigate these risks[51] (Bennett, 2018).

To fully integrate this element, ASEAN countries should require DPIAs in specific situations and ensure consistent conditions for conducting these assessments.

2.1.10. Mandatory appointment of Data Protection Officers

Another significant governance requirement introduced by the General Data Protection Regulation (GDPR) was the mandatory appointment of a Data Protection Officer (DPO) by data controllers and processors under specific circumstances. These circumstances include processing carried out by public authorities (excluding judicial courts) and entities involved in large-scale monitoring or processing of special categories of data[52] (Carrillo & Jackson, 2022; Bennett, 2018).

The Article 29 Data Protection Working Party (WP29) advocated for this provision, recognizing that while the DPD did not mandate the appointment of DPOs, the concept was

[49] General Data Protection Regulation 2016, rec. 136
[50] General Data Protection Regulation 2016, art. 35; recs. 89-90
[51] Ibid 45
[52] General Data Protection Regulation 2016, art. 37(1)

already well established, with many Member States having implemented the practice. The WP29 further emphasized that DPOs serve as a cornerstone of accountability, facilitating compliance with data protection laws and potentially providing businesses with a competitive advantage (WP29, 2017).

A DPO is an individual within an organization – either an internal staff member or engaged through a service contract[53] – responsible for overseeing GDPR compliance, handling data subject inquiries and complaints, providing guidance and training to the organization and its staff, and serving as a liaison with the Supervisory Authority[54] (Secure Privacy, 2024; EPSU, 2019; Borovikov et al., 2017). The DPO must have expert-level knowledge of data protection laws and practices and perform their duties independently[55].

To achieve full integration of this element, ASEAN regulations must establish independent, expert Data Protection Officers with responsibilities equivalent to those outlined in the GDPR.

2.1.11. Notification of Data Breaches

Under the General Data Protection Regulation (GDPR), controllers and processors are subject to a stringent data breach notification regime (Carrillo & Jackson, 2022; Bennett, 2018). The objective of these provisions is to mitigate or prevent physical, material, or non-material damage to natural persons[56] resulting from data breaches or the failure to report them[57].

Controllers are required to notify the supervisory authority promptly, ideally within 72 hours of becoming aware of a personal data breach[58]. The notification must include details such as the nature of the breach, the number of subjects affected, the type of data compromised, the likely consequences, and the measures taken or proposed in response[59]. If the breach poses high risks to individuals' rights and freedoms, controllers must also inform the affected data subjects without undue delay to enable them to take necessary precautions[60]. Conversely, data processors are required only to notify the controller without undue delay upon becoming aware of a personal data breach[61].

Therefore, for full integration of this GDPR element, ASEAN regulations must acknowledge both controllers and processors as responsible for notification and establish similar notification requirements.

---

[53] General Data Protection Regulation 2016, art. 37(6)
[54] General Data Protection Regulation 2016, art. 39
[55] General Data Protection Regulation 2016, rec. 97
[56] A *natural person* refers to an individual human being, distinguishing them from a "legal person," which can be either an individual or an organization, such as a company (Termly's Legal Experts, n.d.; Koch, n.d.)
[57] General Data Protection Regulation 2016, rec. 85
[58] General Data Protection Regulation 2016, art. 33(1)
[59] General Data Protection Regulation 2016, art. 33(3)
[60] General Data Protection Regulation 2016, art. 34
[61] General Data Protection Regulation 2016, art. 33(2)

2.1.12. Substantial administrative fines

The General Data Protection Regulation (GDPR) introduces substantial administrative fines that are unprecedented in European data privacy law, aiming to standardize sanctions – which were previously decided by each Member State's national law – and to strengthen the enforcement of the Regulation's rules[62] (Carrillo & Jackson, 2022; Giurgiu & Larsen, 2016).

Fines are structured into two categories based on the breach's severity. For severe breaches, such as failing to comply with data subjects' rights or violating international transfer restrictions, fines can reach up to 20 million EUR or 4% of the total worldwide annual turnover of the preceding financial year, whichever is greater[63]. The second category pertains to breaches of obligations set for data controllers and processors, such as those related to security measures, breach notifications, certification, and monitoring. In these cases, fines can be as high as 10 million EUR or 2% of the total worldwide annual turnover of the preceding financial year, whichever amount is higher[64].

For the incorporation of this element, ASEAN regulations do not need to stipulate the exact same fine amounts but must establish comparable penalties that reflect the severity of the violation.

2.2. Data Protection Regulations in the ASEAN region: Lao PDR, Singapore, and Thailand

The Association of Southeast Asian Nations (ASEAN)[65] is a regional organization consisting of ten Member States: Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. This organization showcases a rich diversity of economic, political, and social systems. For instance, Singapore boasts the highest GDP per capita in the group, at nearly 85,000 USD according to 2023 World Bank data (World Bank Group, 2023), while Myanmar has the lowest, at less than 1,200 USD. Politically, the bloc includes democracies, authoritarian regimes, and semi-democracy systems, reflecting the diversity of governance models across the region (Greenleaf, 2014). This diversity extends to the demographic and cultural landscape as well, with ASEAN countries home to a variety of religious and ethnic groups (Pew Research Center, 2023, 2014).

Despite the challenges stemming from their inherent differences, ASEAN has steadfastly prioritized economic integration and growth since its establishment in 1967, while simultaneously promoting political and security cooperation among its Member States, guided

[62] General Data Protection Regulation 2016, recs. 148, 150
[63] General Data Protection Regulation 2016, art. 83(5)
[64] General Data Protection Regulation 2016, art. 83(4)
[65] This dissertation does not aim to provide a comprehensive analysis of ASEAN. For an in-depth examination of ASEAN's structure and its political and economic dynamics, see, for instance: Albert and Maizland, (2019), Portela (2013), and Nesadurai (2008)

by foundational principles such as noninterference in internal affairs and the peaceful resolution of conflicts (Council on Foreign Relations, 2023; Albert & Maizland, 2019; ASEAN, 1967).

In 1992, ASEAN deepened its commitment to economic integration by establishing the ASEAN Free Trade Area (AFTA) through the Framework Agreement on Enhancing ASEAN Economic Cooperation (ASEAN, 1992). This effort was further bolstered by the adoption of ASEAN Vision 2020 in 1997 (ASEAN, 1997), which outlined a strategy for a competitive economic bloc with free flows of goods, services, and capital, alongside goals for equitable development and poverty reduction. The vision also emphasized infrastructural improvements, such as interconnecting telecommunications networks and information highways (Isono & Prilliadi, 2023; ASEAN, n.d.). By 2000, ASEAN adopted the e-ASEAN Framework Agreement (ASEAN, 2000) to enhance competitiveness in the ICT sector, supported by the ASEAN Telecommunications and IT Ministers Meeting (TELMIN). This strategy aimed to improve digital access and economic opportunities through investments in telecommunications infrastructure and human resource development. The ASEAN ICT Fund, created in 2004, accelerated these efforts (Chaipipat, 2019).

The drive for economic integration gained further momentum with the ASEAN Economic Community (AEC) Blueprint in 2008 (ASEAN, 2008), which mapped out the region's transformation into a single market and production base by 2015. The blueprint targeted economic competitiveness, equitable development, and global integration (Isono & Prilliadi, 2023). Complementing this, the ASEAN Information and Communication Technology (ICT) Masterplan 2015 (ASEAN, 2011), adopted in 2011, sought to position ASEAN as a global ICT hub by aligning technological advancements with broader economic integration goals (Isono & Prilliadi, 2023; Chaipipat, 2019).

Building on the successes of these initiatives, the AEC Blueprint 2025, introduced in 2015, aimed to further deepen regional integration by focusing on a cohesive economy, enhanced connectivity, and sectoral cooperation (ASEAN, 2015). The ASEAN ICT Masterplan 2020, adopted the following year, sought to create a digitally enabled and sustainable economy that would empower an innovative and inclusive ASEAN community (ASEAN, 2016). During the implementation period of the ASEAN ICT Masterplan 2020 many other frameworks were adopted such as the 2016 ASEAN Framework on Personal Data Protection (ASEAN TELMIN, 2016) and the 2018 ASEAN Digital Data Governance Framework (ASEAN TELMIN, 2018) (Isono & Prilliadi, 2023). These frameworks were strategically designed to build trust in data sharing both within and across borders, thereby facilitating trade and stimulating economic growth.

The 2016 Framework aimed to create a unified approach to personal data protection across ASEAN Member States, enhancing consistency and interoperability in data practices

while empowering individuals with greater control over their data and fostering trust in the digital economy. Key principles of the framework include consent, data accuracy, security safeguards, and accountability (Ing et.al, 2023; Walters et.al, 2019). Additionally, the 2018 ASEAN Digital Data Governance Framework outlined four strategic priorities: managing the data lifecycle with an emphasis on integrity and security, facilitating trustworthy cross-border data flows, promoting digitalization and emerging technologies through capacity building, and harmonizing personal data protection regulations. ASEAN Member States are obligated to submit biannual progress updates on their implementation of the framework, which are monitored during the annual ASEAN Data Protection Forum (Ing et.al, 2023)

However, these agreements are non-binding and voluntary, serving only as guidelines for ASEAN countries in developing or revising their national data protection laws (Ing et.al, 2023; Walters et.al, 2019). Consequently, there are variations in data protection measures among ASEAN Member States (Chaipipat, 2019). Laos, Thailand, Indonesia, Vietnam, and Singapore have implemented comprehensive personal data protection legislation, while countries like Cambodia, Brunei, and Myanmar rely on sectoral laws. Malaysia and the Philippines are awaiting the enactment of amendments to their comprehensive legislation.

The following subsections will offer a detailed analysis of the data protection regulations in ASEAN countries that, at the time of this study, have the most up-to-date versions of their comprehensive personal data protection laws. Due to language accessibility, the analysis will focus specifically on Lao PDR, Singapore, and Thailand, which have modernized their data privacy regimes with legislation enacted in 2017, 2020, and 2019, respectively. This study aims to investigate how these countries are navigating the implementation of their data privacy frameworks and the extent to which they align with the GDPR, recognized as the global standard in this field. Therefore, it will be assessed if the key elements of the GDPR have been incorporated in each of these country's data privacy legislation.

2.2.1. Laos' Law on Electronic Data Protection

Over the past decade, Laos has made significant progress in developing a comprehensive legal and regulatory framework for electronic commerce. This initiative is part of the country's strategy to modernize its economy and fulfill regional and international commitments.

As a member of ASEAN, the late 2000s marked a crucial period for Laos in the push towards deeper regional economic integration, particularly in preparation for the ASEAN Economic Community (AEC), which officially launched in 2008. A key goal of the AEC was to create a seamless digital economy, allowing Member States to easily conduct cross-border electronic transactions. This was to be achieved through the ASEAN Single Window initiative, which facilitates the electronic exchange of trade documents among Member States. As part

of this initiative, Laos was required to operationalize its National Single Window by 2012 (ASEAN, 2008; ASEAN, n.d.).

In light of this, Laos introduced the Law on Electronic Transactions in 2012, establishing key principles for the use of electronic communications, contracting, and signatures in the country. The law applies to all forms of electronic transactions, including those on websites, e-commerce platforms, emails, instant messaging, and mobile payments (Willis, 2023). By introducing concepts such as electronic consent and electronic signatures, the law represented an important step in regulating digital business transactions, though its impact remained somewhat limited (Santaniello, 2021).

The next significant regulatory step came with the Law on Cybercrime in 2015. Deputy Minister of Post and Telecommunications, Thansamay Kommasith, emphasized the importance of the law, noting, "*It was necessary to make this law because computer systems play an important role in society, as today's electronic media significantly influences both individuals and socio-economic development*" (apud Soukthavy & Manythone, 2015). He explained that the implementation of this law would help prevent cybercrime, protect critical infrastructures such as databases and server systems, and enhance national security, thereby promoting peace, order, and socio-economic growth while facilitating Laos' integration into regional and global economic communities (Soukthavy & Manythone, 2015).

The Law on Cybercrime is particularly noted for addressing issues related to personal data and privacy. It provides legal mechanisms to prosecute cybercrimes such as unauthorized computer access, data theft, and misuse of personal data. It also tackles the improper use of social media for defamation. However, while it covers certain aspects of cybercrime, it does not introduce specific standards for data administration or consent requirements across various situations (Santaniello, 2021).

To address these shortcomings, the Law on Electronic Data Protection (LEDP) was enacted in 2017 (Lao People's Democratic Republic, 2017), followed by the introduction of implementation guidelines in 2018[66]. This legislation aligns Laos' laws with regional standards and incorporates international practices to address the rapid growth of e-commerce, enhancing the nation's legal infrastructure. The LEDP demonstrates the government's commitment to developing regulatory mechanisms that safeguard individual privacy and national security amidst the complexities of online activities and digital transactions (Ferguson et al., 2022; Santaniello, 2021).

[66] The analysis of these guidelines could not be conducted, as the document does not exist in any language other than Lao. For further investigation, the document can be accessed at: https://laoofficialgazette.gov.la/kcfinder/upload/files/Introduction%20on%20Implementation%20of%20Data%20Protection%20Law.pdf

The LEDP primarily pertains to personal electronic data, defining it as *"electronic data of individual, legal entities or organizations"*[67], thereby overlooking non-automated forms of data, which are encompassed within the ambit of the GDPR. Nevertheless, both the GDPR and the Laos' LEDP delineate categories of data, with the latter defining three distinct groups: general, specific, and prohibited data[68]. While the GDPR provides clear definitions for its categories of personal data, the LEDP's categories remain somewhat ambiguous, with prohibited data being the only category that includes more detailed specifications. Moreover, the LEDP makes no reference to the pseudonymization of data.

The LEDP grants several rights to the data owners[69], including the right to data deletion under conditions such as upon request, when the data's purpose has been fulfilled, or when it poses a threat to national stability[70]. However, it is noteworthy that the LEDP does not extend to include the right to data portability. Although the regulation permits the transfer of data with the data owner's consent, this transfer is limited to specific circumstances, such as handovers to authorities. As a result, it does not encompass the broader right for individuals to transfer their data between different services of their choosing[71].

Regarding consent, the LEDP does not explicitly mention it but includes implicit references through terms like *approval*, *agreement*, and *permission concerning data handling*[72]. Besides, the LEDP does not prescribe a specific form for obtaining consent, nor does it explicitly mention a standalone right to withdraw consent, as seen in the EU's GDPR.

Additionally, while the LEDP's territorial scope applies to both domestic and international entities operating within Laos, it does not encompass the broad range of scenarios covered by the GDPR, which extends its jurisdiction to entities outside the EU if they impact EU residents[73].

Under the LEDP, the primary entities responsible for administrating electronic data are the Electronic Data Administration Authorities[74]. This role is more narrowly defined compared to the GDPR's data controller, focusing on data processing rather than determining the purposes and means of processing. Consequently, the LEDP's Data Administrator concept is somewhat closer to the GDPR's data processor, focusing on the active management and processing of data. However, it is not an exact match, as a data administrator under the LEDP does not manage data on behalf of another party. The LEDP's framework may lead to varied

[67] Laos' Law on Electronic Data Protection 2017, art. 3(12)
[68] Laos' Law on Electronic Data Protection 2017, arts. 8-10, 33(3)
[69] Article 3(10) of Laos' Law on Electronic Data Protection (Lao People's Democratic Republic, 2017) defines a *data owner* as "*an individual, legal entity, or organization that owns electronic data*."
[70] Laos' Law on Electronic Data Protection 2017, arts. 20, 27(2), 29(3)
[71] Laos' Law on Electronic Data Protection 2017, art. 15
[72] Laos' Law on Electronic Data Protection 2017, arts. 12, 15-17
[73] Laos' Law on Electronic Data Protection 2017, arts. 3, 6
[74] Laos' Law on Electronic Data Protection 2017, art. 3(14)

interpretations in practice, suggesting that it lacks a crucial element by not clearly differentiating between entities that process, treat, and use electronic data.

Nevertheless, many of the responsibilities assigned to the Data Administrator under the LEDP align with those imposed on processors under the GDPR, such as the requirement to cooperate with a supervisory authority[75] and maintain records of electronic data[76]. However, a key distinction lies in how data breaches are handled. While the LEDP addresses data breaches, the responsibility for notifying such breaches falls on individuals, legal entities, or organizations, who must inform the Data Administrator[77] – unlike under the GDPR, where the Data Administrator is responsible for breach notifications. Additionally, although Laos' Law on Electronic Data Protection briefly mentions the need to appoint an officer responsible for data protection[78]– akin to a Data Protection Officer – it lacks detailed provisions regarding the establishment of this role and a comprehensive outline of the officer's responsibilities beyond ensuring compliance. Furthermore, the organization overseeing this function is subject to government oversight, compromising its independence – a significant divergence from the GDPR, which emphasizes the necessity of independence for Data Protection Officers.

Besides, while the LEDP requires annual inspections and evaluations of data system risks and security against attacks[79], these assessments are not based on the potential risk to personal data, unlike the Data Protection Impact Assessments mandated by the GDPR.

The Laos Law on Electronic Data Protection also falls short in explicitly incorporating the principles of *privacy by design* and *privacy by default*. Although it references a limited number of related principles, its scope is constrained. While the LEDP emphasizes the importance of data security and protecting data owner rights[80], it does not address key measures such as data minimization, transparency, and pseudonymization, essential components of *privacy by design* and *default* as recognized by the GDPR.

In terms of enforcement, the LEDP designates an Administration Organization of Electronic Data Protection comprising various entities such as the National Assembly, Provincial People's Assembly, State Audit Organization, State Inspection Organization, Lao National Front for Development, and Mass Organizations, which compromises the level of independence of the authority. Nevertheless, the Administration has responsibilities akin to the

[75] Laos' Law on Electronic Data Protection 2017, art. 30(8)
[76] Laos' Law on Electronic Data Protection 2017, art. 15
[77] Laos' Law on Electronic Data Protection 2017, arts. 26, 27(3), 28(3)(4)
[78] Laos' Law on Electronic Data Protection 2017, art. 23(1)
[79] Laos' Law on Electronic Data Protection 2017, art. 23(8)
[80] Laos' Law on Electronic Data Protection 2017, art. 5(3)(4)

GDPR supervisory authority, such as raising public awareness[81], providing guidance[82], and proposing and implementing plans for personal data protection[83].

Additionally, the LEDP includes a range of punitive measures for non-compliance, including re-education, disciplinary actions, fines, civil penalties, and criminal sanctions. However, the financial penalties imposed under the LEDP are significantly modest compared to those under the GDPR, with fines capped at 15 million LAK, equivalent to approximately 650 EUR[84].

2.2.2. Singapore Personal Data Protection Act

Since 2012, Singapore's data privacy framework has been governed by the Personal Data Protection Act (PDPA). This legislation regulated the collection, use, and disclosure of personal data, ensuring organizations protect customers' and employees' information while empowering individuals to manage their own data. Additionally, the PDPA established the Do Not Call Register[85], allowing individuals to opt out of receiving unsolicited voice calls, text messages, and fax messages (Chik, 2014).

Acknowledging the need to update the Personal Data Protection Act in light of technological advancements, emerging business models, and the imperative to uphold consumer trust while aligning with international standards, the Ministry of Communications and Information (MCI)[86], together with the Personal Data Protection Commission (PDPC), conducted a series of three public consultations from 2017 to 2019. This was followed by a fourth consultation from May 14 to 28, 2020, which focused specifically on the draft Bill and aimed to refine the legislative framework to more effectively address these evolving challenges (Hill Dickinson Law Firm, 2022; Alfred, 2020; Ministry of Digital Development and Information, 2020a, 2020b; PDPC Singapore, 2020).

On November 2, 2020, the Singaporean Parliament enacted a revised version of the PDPA (Republic of Singapore, 2020), introducing significant amendments that were implemented in stages across 2021 and 2022. The key amendments include the introduction of a mandatory data breach notification requirement, the expansion of the scope of deemed consent, the inclusion of additional exceptions to the necessity for express consent, the introduction of a right to data portability, the establishment of new criminal offenses related to

[81] Laos' Law on Electronic Data Protection 2017, arts. 41(3), 42(1), 43(1)
[82] Laos' Law on Electronic Data Protection 2017, arts. 41(4)(7), 42(3), 43(2)
[83] Laos' Law on Electronic Data Protection 2017, arts. 41(2), 42(2)(4), 43(3)(4)
[84] Laos' Law on Electronic Data Protection 2017, arts. 48-54
[85] This study does not cover the Do Not Call Register aspect of the PDPA. For detailed information on this component, see, for instance: Chik (2014).
[86] In 2024, following the integration of The Smart Nation and Digital Government Group (SNDGG) with the Ministry of Communications and Information (MCI)'s digital development functions, the ministry was renamed the Ministry of Digital Development and Information (MDDI) (Smart Nation Singapore, n.d.a.)

data breaches, and an increase in the maximum financial penalties for violations of the PDPA (Lui et al., 2022; ; Rajah & Tann Law Firm, 2021; Hopland et al., 2020). Despite these amendments, the 2012 PDPA remains largely unchanged, with the 2020 version serving primarily as an update; thus, references to the PDPA in this dissertation will pertain to the latest 2020 version, which retains much of the original 2012 framework.

Similar to the GDPR, Singapore's PDPA emphasizes the protection of individuals' personal data and defines it in a broadly similar manner[87]. However, the GDPR offers a more detailed and nuanced description of personal data identifiers. Besides, while the GDPR explicitly delineates special categories of personal data, such as health or racial information, the PDPA does not provide specific definitions for these categories. However, Advisory Guidelines on Key Concepts[88] acknowledges the sensitivity of certain types of data, including that concerning vulnerable groups such as minors and individuals with physical or mental disabilities. Accordingly, it requires organizations to implement heightened protection measures for such sensitive data (Personal Data Protection Commission, 2022a, p.68). Additionally, the PDPA does not specifically define pseudonymized data, however, the Guide to Basic Anonymisation[89] describes pseudonymization as replacing identifying data with fictitious values and notes that data anonymization can be either reversible or irreversible, something that the GDPR does not consider (Personal Data Protection Commission, 2022b, p.35).

Regarding individual rights, both the PDPA and GDPR offer several similar protections, including the right to data portability, which was introduced in the PDPA through the amendments in 2020[90]. This right mandates that, upon request, organizations must transfer an individual's personal data to another organization in a commonly used, machine-readable format. Both regulations also recognize the right to withdraw consent for data processing[91]. Under the PDPA, consent must be informed, voluntary and limited to data collection purposes, aligning with GDPR requirements[92]. However, the PDPA also allows for deemed consent under certain conditions, provided it is informed and aligns with the data collection purpose[93]. An individual is considered to have given deemed consent if they voluntarily provide personal

[87] Singapore's Personal Data Protection Act 2020, § 2(1)
[88] The Advisory Guidelines for Key Concepts, created by the Personal Data Protection Commission in 2013 and revised in 2022, provides detailed explanations and examples of key obligations and terms under the PDPA. This document aids organizations and individuals in understanding and interpreting the provisions of the Act more effectively (PDPC Singapore, n.d.a.).
[89] The Guide on Basic Anonymisation, created by the Personal Data Protection Commission in 2022 and revised in 2024, offers practical guidance for businesses on effectively performing basic anonymization and de-identification of datasets through a straightforward 5-step process (PDPC Singapore, 2022; PDPC Singapore, n.d.b.)
[90] Singapore's Personal Data Protection Act 2020, §§26F, 26H
[91] Singapore's Personal Data Protection Act 2020, § 16
[92] Singapore's Personal Data Protection Act 2020, §§ 13, 14
[93] Singapore's Personal Data Protection Act 2020, § 15

data to an organization, and if it is reasonable to assume that such consent has been granted (CookieYes Blog, 2024; PDPC Singapore, n.d.c.). In contrast, the GDPR mandates explicit consent, requiring clear affirmative actions from the individual.

One significant difference is that the PDPA does not grant individuals the right to request the erasure or deletion of their personal data. According to the Advisory Guidelines on Key Concepts, while individuals can withdraw consent for the collection, use, or disclosure of their data, the PDPA does not obligate organizations to delete or destroy personal data upon such requests. Instead, organizations are required to delete personal data only if the purpose for which it was collected has been fulfilled and retention is no longer necessary for business or legal reasons (Personal Data Protection Commission, 2022a, pp. 59, 106).

Concerning territorial scope, while the GDPR applies to both public and private entities operating within the EU or processing the personal data of EU residents, the Singapore PDPA explicitly excludes public agencies and organizations acting on their behalf from its regulatory framework. Instead, the PDPA governs all non-public sector organizations involved in the collection, use, and disclosure of personal data within Singapore[94]. This includes organizations that are either established under Singaporean law or based outside Singapore, regardless of whether they have a physical presence within the country[95].

Despite some terminological differences, the PDPA and GDPR share similar concepts of data controllers and data processors. In the PDPA, the data controller is referred to as the *organization*, while the data processor is called the *data intermediary*[96]. Similar to the GDPR, an organization must ensure it contracts with data intermediaries that provide sufficient guarantees to comply with the Act. This is because the organization remains responsible for personal data processed on its behalf and for its purposes by the data intermediary, as if the organization itself was processing the data[97]. As such, most of the responsibilities under the PDPA also fall under the organization's duties, with the data intermediaries only having to ensure data security, comply with contractual terms, and notify data breaches.

The introduction of the data breach notification requirement, part of the 2020 amendments to the PDPA, further emphasizes the role of intermediaries. They must promptly inform the organizations they serve about any breaches[98]. In turn, organizations are obligated to notify the Personal Data Protection Commission and affected individuals of breaches that could cause significant harm or occur on a significant scale[99].

[94] Singapore's Personal Data Protection Act 2020, § 4(1)
[95] Singapore's Personal Data Protection Act 2020, § 2(1)
[96] Singapore's Personal Data Protection Act 2020, § 2(1)
[97] Singapore's Personal Data Protection Act 2020, § 4(2)(3)
[98] Singapore's Personal Data Protection Act 2020, §§ 26(C)(E)
[99] Singapore's Personal Data Protection Act 2020, §§ 26(C)(D)

Beyond breach notifications, organizations are also required to appoint a Data Protection Officer[100] and collaborate with the PDPC, which functions similarly to a supervisory authority[101].

The designation of a DPO does not absolve the organization of its obligations under the PDPA[102]. The legal responsibility for complying with the PDPA remains with the organization itself and is not transferred to the DPO. Instead, the organization must appoint a suitable individual for the DPO role, who may then delegate specific responsibilities to other staff members. Together, these individuals must work cooperatively to ensure the organization's compliance with the PDPA.

Although the Act does not explicitly detail the DPO's responsibilities, the Advisory Guidelines on Key Concepts (Personal Data Protection Commission, 2022a, p. 152) outline several key duties. These include developing and implementing data protection policies and practices, creating or overseeing the creation of a personal data inventory, conducting data protection impact assessments, monitoring and reporting on data protection risks, providing internal training, engaging with stakeholders on data protection issues, and serving as the primary internal expert on data protection. Additionally, depending on the organization's needs, the DPO might also collaborate with or have responsibilities related to data governance and cybersecurity functions. The DPO can also support organizational innovation by ensuring that data protection considerations are integrated into new initiatives and projects.

Moreover, the Personal Data Protection Commission, acting as a supervisory authority, holds powers similar to the GDPR, such as the power of investigation[103], the power to impose financial penalties[104], and advisory power[105]. In line with its powers, the Commission's main functions are to promote data protection awareness in Singapore, provide consultancy and advisory services, represent the Government internationally, conduct research and educational activities, manage technical cooperation with other organizations and foreign authorities, and administer and enforce the PDPA[106]. However, a notable difference between the PDPC and the GDPR supervisory authorities is the aspect of independence, which is not explicitly addressed in the PDPA.

Additionally, while the PDPA does not explicitly address the conduct of Data Protection Impact Assessments, practical guidance is available in the Advisory Guidelines on Key Concepts (Personal Data Protection Commission, 2022a, p. 155) and the Guide to Data

[100] Singapore's Personal Data Protection Act 2020, § 11(3)
[101] Singapore's Personal Data Protection Act 2020, § 6(f)
[102] Singapore's Personal Data Protection Act 2020, § 11(6)
[103] Singapore's Personal Data Protection Act 2020, § 50, ninth schedule
[104] Singapore's Personal Data Protection Act 2020, § 48J
[105] Singapore's Personal Data Protection Act 2020, § 49
[106] Singapore's Personal Data Protection Act 2020, § 6

Protection Impact Assessments[107] (Personal Data Protection Commission, 2021, p. 7). These resources offer valuable advice on assessing situations that may pose potential adverse effects on individuals[108].

While the GDPR permits higher maximum penalties, the PDPC under the PDPA is also empowered to impose substantial fines, reflecting the seriousness with which Singapore treats data protection. Specifically, the PDPC can levy financial penalties of up to 1 million SGD (approximately 680,000 EUR) or 10% of an organization's annual turnover in Singapore, whichever is higher, depending on the severity of the violation[109].

Moreover, although the Singapore Personal Data Protection Act does not explicitly mandate *privacy by design* and *privacy by default* as the GDPR does, it encourages similar practices. For instance, the PDPA mandates organizations to take reasonable measures to secure personal data[110], which supports the broader objectives of *privacy by design*. Additionally, the principle of limitation of purpose and extent[111] embedded in the PDPA aligns with the spirit of *privacy by default*. Still, the PDPA does not specifically address key elements such as data minimization, transparency, and pseudonymization, which are integral to GDPR's framework. Consequently, the protection under the PDPA may not be as comprehensive as the explicit requirements for *privacy by design* and *by default* in the GDPR.

2.2.3. Thailand Personal Data Protection Act

Before the enactment of the Personal Data Protection Act (PDPA) in 2019, Thailand lacked a comprehensive statutory law governing data privacy and protection. However, the right to privacy was acknowledged in the Constitution of Thailand, with general data protection principles outlined in the Civil and Commercial Code (CCC) and specific sectoral laws, such as those for financial and telecommunication services (Bumpenboon, 2020). The Constitution safeguarded privacy rights, allowing the government to deprive these rights only according to the law, balancing individual and public interests. For disputes among private parties, courts typically referred to the CCC or sector-specific regulations rather than the Constitution's

[107] The Data Protection Impact Assessments, created by the PDPC in 2017 and revised in 2022, offers an introductory overview of key principles and considerations for organizations, particularly those lacking measures or tools to address specific personal data protection risks. It provides guidance on conducting a Data Protection Impact Assessment (DPIA) for systems and processes. However, the practices outlined in this guide are intended for general information and are not exhaustive (Data Guidance, 2017; PDPC Singapore, n.d.d.)

[108] According to these guides DPIAs are best addressed when the system or process is (i) new and in the process of being designed or (ii) in the process of undergoing major changes.

[109] Ibid 91

[110] Singapore's Personal Data Protection Act 2020, § 24

[111] Singapore's Personal Data Protection Act 2020, § 18

overarching principles. Under the CCC, privacy rights and data protection were enforced through tort law[112] (Bumpenboon, 2020).

Efforts to establish an omnibus privacy law began in 2014 when the Office of the Prime Minister introduced a draft Data Protection Act, detailing criteria for personal data processing, and establishing a Data Protection Committee. This surged at time when Thailand's Cabinet was focused on advancing the digital economy and therefore created committees – such as National Digital Economy Committee – to coordinate digital economy policies; restructured the Information and Communications Technology Ministry into the Digital Economy and Society Ministry; and highlighted the need for legal reforms, infrastructure development, and technology transfers to achieve this goal (Bangkok Post, 2014; Library of Congress, 2014; The Nation, 2014). Thus, the draft Data Protection Act was a key part of Thailand's strategy to strengthen its digital economy and ensure proper handling of personal data.

This draft underwent multiple revisions, receiving Cabinet approval in January 2015 and further amendments by the Council of State in May 2015. Ultimately, the Council of State approved the revised draft in December 2018 (Bumpenboon, 2020). However, it was not until 2019 that the Personal Data Protection Act (Kingdom of Thailand, 2019) was enacted, marking Thailand's first comprehensive data protection law and the focus of this study. The implementation of the Act was delayed due to the COVID-19 pandemic and ultimately came into force in 2022 (Tortermvasana, 2020). The PDPA is widely regarded as having substantial similarities to the EU's General Data Protection Regulation and appears to draw inspiration from it (Bumpenboon, 2020; Naparat, 2020; Chandler MHM, 2019; Greenleaf & Suriyawongkul, 2019; Tan & Azman, 2019).

Similar to the GDPR, Thailand's PDPA aims to protect personal data and defines it in a manner akin to the GDPR, encompassing any information that can identify an individual[113], however the GDPR goes a little bit further and gives examples of identifiers. Besides, while the GDPR specifies special categories of personal data, the PDPA does not. Nonetheless, it prohibits the collection of certain types of data without explicit consent, including racial or ethnic origin, political opinions, criminal records, and trade union membership, among others[114]. Moreover, while the GDPR provides a definition for pseudonymized data and it clarifies that such data are subject to the obligations of the GDPR, the PDPA does not provide a definition of pseudonymized data.

[112] In Thai law, torts encompass acts that harm an individual's person, property, reputation, or similar interests, warranting compensation for the injured party. This broad category includes various cases such as personal injury, assault and battery, negligence, defamation, medical malpractice, and fraud (Thailand Arbitration Center, n.d.)
[113] Thailand's Personal Data Protection Act 2019, §6
[114] Thailand's Personal Data Protection Act 2019, §26

Despite these differences, the PDPA grants data subjects rights that are largely similar to those under the GDPR, including the right to data portability[115], the right to erasure or destruction[116], and the right to withdraw consent[117]. Besides, consent in Thailand's PDPA follows similar requirements as consent in the GDPR, such as being freely given, clear, explicit and informed[118].

Similar to the GDPR, the PDPA applies to data controllers and data processors outside of Thailand if their activities involve offering goods or services to, or monitoring the behavior of, data subjects in Thailand[119]. In fact, as in the GDPR, data controllers and processors are crucial entities under the Act and exercise similar functions. As in the GDPR, the data controller has the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data, whereas the data processor operates on behalf of the data controller, therefore the data controller must guarantee that the processor deals with data in a lawful manner[120].

The PDPA mandates that data controllers and processors maintain records of processing activities, with an exemption granted to small organizations[121]. Additionally, under certain conditions, they must appoint a Data Protection Officer whose independence is protected by law. Notably, the PDPA prohibits the dismissal or termination of a DPO for performing their duties, ensuring their autonomy[122]. The duties of Thailand's DPO are quite similar to the GDPR's DPO, encompassing giving advice, investigating compliance, and cooperating with the supervisory authority[123].

The PDPA also imposes a duty on data controllers and processors to notify the Personal Data Protection Committee (PDPC) of data breaches. Controllers must notify within 72 hours, while the PDPA does not specify a timeframe for processors[124]. Furthermore, while the PDPA does not explicitly mandate data controllers to conduct impact assessments regarding personal data processing as required by the GDPR, both data controllers and processors are obligated to implement appropriate security measures to prevent unauthorized access, loss, alteration, or disclosure of personal data, thereby safeguarding the rights of data subjects. Regular reviews of these security measures are imperative, especially in light of technological advancements[125].

---

[115] Thailand's Personal Data Protection Act 2019, §31
[116] Thailand's Personal Data Protection Act 2019, §33
[117] Thailand's Personal Data Protection Act 2019, §§ 19
[118] Ibid 103
[119] Thailand's Personal Data Protection Act 2019, § 5
[120] Thailand's Personal Data Protection Act 2019, § 37(2)
[121] Thailand's Personal Data Protection Act 2019, §§39, 40(3)
[122] Thailand's Personal Data Protection Act 2019, §42
[123] Thailand's Personal Data Protection Act 2019, § 42
[124] Thailand's Personal Data Protection Act 2019, §§37(4), 40(2)
[125] Thailand's Personal Data Protection Act 2019, § 37(1)

The PDPC is the primary body responsible for administering data protection law in Thailand, analogous to the supervisory authority under the GDPR. Unlike its GDPR counterpart, however, the PDPC lacks legislative and financial guarantees of independence. The administrative framework established by the PDPA is complex, involving not only the PDPC but also the Office of the PDPC, a Commission that oversees this Office, the Secretary-General of the Office, and Expert Committees[126] (Greenleaf & Suriyawongkul, 2019).

This diffuse structure results in each of the various entities playing distinct and somewhat independent roles. Despite this complexity, the PDPC as a whole remains central to the data protection framework. Its broad responsibilities include developing a masterplan for data protection, issuing compliance guidelines and orders, establishing codes of conduct, setting principles for data exports, recommending legal reforms (including a quinquennial review of the Act), proposing regulations, and providing guidance on the interpretation of the Act[127]. Besides, the expert committees of the PDPC have several duties and powers similar to the supervisory authority under the GDPR, such as investigatory powers, which allow the Committee to conduct investigations of data controllers or processors causing harm to data subjects, which may come as a consequence of a complaint of the data subject[128], and corrective powers such as administering fines in case of non-compliance[129].

Fines issued by the Personal Data Protection Committee range from 500000 THB (approximately 13500 EUR) to 5 million THB (approximately 126000 EUR), depending on the severity of the offense[130]. For administrative violations, such as unauthorized disclosure of personal data or failure to comply with data subject rights, the minimum fine is 500000 THB. Criminal offenses, such as unlawfully collecting, using, or disclosing personal data, can result in fines from 1 million THB (approximately 27000 EUR) to 5 million THB and/or imprisonment for up to one year. These penalties are significantly lower compared to those imposed under the GDPR.

Moreover, although the Thailand PDPA incorporates principles like data minimization[131] and requires reasonable security measures for personal data[132], it does not explicitly mandate *privacy by design* and *privacy by default*, nor does it address key elements such as transparency and pseudonymization found in the GDPR. Consequently, the protections under the PDPA may be less comprehensive than those offered by the GDPR.

[126] Thailand's Personal Data Protection Act 2019, §§ 8, 43, 48, 57, 71
[127] Thailand's Personal Data Protection Act 2019, § 16
[128] Thailand's Personal Data Protection Act 2019, § 72
[129] Thailand's Personal Data Protection Act 2019, § 90
[130] Thailand's Personal Data Protection Act 2019, §§79-90
[131] Thailand's Personal Data Protection Act 2019, § 22
[132] Thailand's Personal Data Protection Act 2019, § 37

Chapter 3 – European External Governance in data protection laws in ASEAN countries

This chapter addresses the second sub-research question posed in sub-chapter 1.2: What are the mechanisms through which the EU GDPR is incorporated into the regulations of the ASEAN countries?

Building on the conceptual framework of European External Governance, this chapter analyzes four key mechanisms – competition, learning, emulation, and socialization – to assess their role in the influence of EU regulatory standards beyond its borders. Specifically, it examines how these mechanisms have contributed to or hindered the incorporation of key elements of the GDPR within the ASEAN region, focusing on Laos, Singapore, and Thailand. The chapter further identifies which mechanisms have been most influential in each case.

The competition mechanism illustrates how the European Union's economic influence and stringent regulatory framework exert indirect pressure on other countries to conform to its standards. This phenomenon, termed the *Brussels Effect*[133] by Bradford (2012), refers to the EU's distinctive ability to externalize its regulations globally, a capacity that, according to the author, is unparalleled by other international actors. Businesses and governments outside the EU, aiming to avoid adverse consequences and maintain access to the European market, are often compelled to adopt EU rules voluntarily, thereby reinforcing the EU's regulatory reach beyond its borders (Lavenex, 2014; Schimmelfennig, 2015, 2010; Rousselin, 2012). To assess this mechanism, the chapter examines trade relations between the selected ASEAN countries – Laos, Singapore, and Thailand – and the EU, focusing on trade volumes and key sectors. The aim is to determine whether economic interdependence has influenced these countries to align their data protection laws with the GDPR.

In contrast, the learning mechanism is driven by domestic dissatisfaction, where countries seek institutional reforms to address specific political or economic challenges. The EU often serves as a model for such reforms, offering a comprehensive legal framework that is perceived as adaptable and effective (Schwartz, 2019; Börzel & Risse, 2012; Rousselin, 2012;

[133] Anu Bradford (2012) introduced the concept of the *Brussels Effect* to describe the European Union's unilateral influence on global regulatory standards. This phenomenon operates in two distinct phases. First, the *de facto Brussels Effect* occurs when multinational companies voluntarily adopt the EU's stringent regulatory standards across the globe, even in jurisdictions with less rigorous regulations. This approach is often motivated by the efficiency of adhering to a single high standard, resulting in EU regulations becoming de facto global norms without the need for formal enforcement beyond the EU's borders. Second, the *de jure Brussels Effect* emerges when these same companies, after aligning with EU regulations, actively lobby their domestic governments to formally adopt these standards into national law. This lobbying effort ensures that all domestic competitors comply with the same regulatory framework, thereby fostering a fairer competitive environment.

Schimmelfennig & Sedelmeier, 2004). This chapter assesses whether Laos, Singapore, and Thailand have viewed the GDPR as a solution to their own challenges by examining the objectives behind their data protection laws and whether they regard the EU's approach as a model to address their domestic concerns.

Emulation, on the other hand, involves the adoption of EU rules based on their perceived legitimacy, influenced by how well EU norms align with a country's existing beliefs and practices (Lavenex, 2014; Börzel & Risse, 2012; Schimmelfennig, 2010; Lavenex & Schimmelfennig, 2009). To evaluate this mechanism, the chapter investigates whether the EU is seen as a normative model worth emulating, taking into account the unique cultural contexts, prevailing norms, and societal perspectives on the EU in the selected ASEAN countries – Laos, Singapore, and Thailand. This analysis incorporates viewpoints from diverse sectors, including foreign policy, civil society, and media.

Finally, socialization refers to the process by which actors adopt EU rules as a result of the EU's direct efforts to promote its values as legitimate or superior (Lavenex, 2014; Schimmelfennig, 2010; Schimmelfennig & Sedelmeier, 2004). This chapter examines whether the EU has engaged in collaborative and cooperative initiatives in the area of data protection, and it assesses how these initiatives may have actively promoted EU normative values. Furthermore, the chapter analyzes the impact of these efforts on the adoption of EU standards within the ASEAN region.

Each mechanism will be analyzed within the regulatory context of each country, with dedicated sections for each: sub-chapter 3.1 will focus on Laos, sub-chapter 3.2 on Singapore, and sub-chapter 3.3 on Thailand. In contrast, the socialization mechanism will be discussed collectively in sub-chapter 3.4. This approach is warranted because the EU's direct efforts to promote its values were conducted at a regional level with ASEAN, rather than on an individual basis with each country. As a result, the shared experiences among these nations can be effectively analyzed together.

The analysis will concentrate on the timeframe from the GDPR's enactment in 2016 to the adoption of national data protection laws in the ASEAN countries of interest: Laos in 2017, Thailand in 2019, and Singapore in 2020. This period enables a detailed examination of how each mechanism – competition, learning, emulation, and socialization – has influenced the formulation and implementation of data protection regulations in these countries.

3.1. Laos

3.1.1. Competition

The timeline considered to analyze the competition mechanism in Laos is between 2016 and 2017, because it refers to the time of the enactment of the EU's General Data Protection

Regulation and the Laos' Law on Electronic Data Protection, respectively. In this period, the economic relationship between the European Union and Laos remained limited[134]. Although the EU was Laos' fourth-largest trading partner during this period, it accounted for only 4.3%[135] of Laos' total trade in goods by 2017 (Directorate-General for Trade, 2024a). This share was marginal compared to Laos' trade with its top three partners during the same period – Thailand (46.9%)[136], China (26.5%)[137], and Vietnam (10.5%)[138] (Directorate-General for Trade, 2024a; WITS n.d.a). Moreover, in comparison with other ASEAN countries, the EU's trade volumes with Laos were considerably minor, with only Brunei recording smaller trade volumes (Directorate-General for Trade 2024b-j).

The limited economic relationship between the EU and Laos yields several key implications for the influence of the GDPR on Lao businesses. First, the minimal trade between these two regions means Lao companies face little external pressure to comply with EU data protection regulations. Second, with 86.2% of Laos' 2017 trade consisting of merchandise, and EU imports concentrated in low-data sectors like textiles, footwear, and agriculture, GDPR compliance is not a priority for most Lao industries. As a result, the weak trade ties provide little incentive for Laos to adopt similar data protection standards domestically (Directorate-General for Trade, 2024a; United Nations ESCAP, 2018; European Commission, n.d.a).

Interestingly, the limited trade relations between Laos and the EU illustrate how economic interdependence affects *European External Governance*. Due to the absence of significant trade ties, the EU has minimal leverage to promote its data protection standards, such as the GDPR, in Laos. This lack of economic engagement may partly explain the significant differences between Laos' Law on Electronic Personal Data and the GDPR.

---

[134] The objective of this study is not to explore the reasons behind the limited trade between the EU and Laos. For an analysis of this issue, see for instance: Thipphavong, V. *et al.* (2022)

[135] This percentage was calculated by dividing the total value of goods traded between the EU and Laos by Laos's total global trade in goods, then multiplying the result by 100. This allows us to quantify the EU's share of Laos's overall trade network. The data was retrieved from the Directorate-General for Trade (2024a, pp.3,8).

[136] This percentage was calculated by dividing the total value of goods traded between Thailand and Laos by Laos's total global trade in goods, then multiplying the result by 100. This allows us to quantify Thailand's share of Laos's overall trade network. The data on the total value of goods traded between Thailand and Laos was obtained from WITS (n.d.a), while the information on Laos's total global trade in goods was sourced from the Directorate-General for Trade (2024a, p. 8).

[137] This percentage was calculated by dividing the total value of goods traded between China and Laos by Laos's total global trade in goods, then multiplying the result by 100. This allows us to quantify China's share of Laos's overall trade network. The data on the total value of goods traded between China and Laos was obtained from WITS (n.d.a), while the information on Laos's total global trade in goods was sourced from the Directorate-General for Trade (2024a, p. 8).

[138] This percentage was calculated by dividing the total value of goods traded between Vietnam and Laos by Laos's total global trade in goods, then multiplying the result by 100. This allows us to quantify Vietnam's share of Laos's overall trade network. The data on the total value of goods traded between Vietnam and Laos was obtained from WITS (n.d.a), while the information on Laos's total global trade in goods was sourced from the Directorate-General for Trade (2024a, p. 8).

3.1.2. Learning

By 2016, the Lao People's Democratic Republic was focused on graduating from the United Nations' list of Least Developed Countries (LDC)[139]. This goal required meeting the threshold of two out of three criteria – per capita Gross National Income[140], the Human Assets Index[141], or the Economic Vulnerability Index[142] – or doubling the required per capita income over two consecutive reviews (Lao People's Democratic Republic, n.d.). To support this ambition, Lao PDR introduced its 8th National Socio-economic Development Plan (NSEDP) (2016-2020), which was aligned with long-term national strategies outlined in the Socio-economic Development Strategy to 2025 and Vision 2030. These plans reflected Laos' commitment to economic development as a pathway toward LDC graduation (Ministry of Planning and Investment, 2016).

A key component of the NSEDP was the promotion of the Information, Communications, and Technology (ICT) sector, which was viewed as critical to driving economic growth and facilitating faster, more secure data transfer for investment, manufacturing, and tourism. This emphasis on ICT development can be attributed, in part, to external pressures from the ASEAN region, which had seen rapid economic advancement, largely driven by digital economies. Recognizing the need to align with ASEAN's digital developments, Laos sought to enhance its ICT capabilities, motivated by agreements and frameworks within ASEAN, such as the e-ASEAN Framework (ASEAN, 2000), the ASEAN Framework on Personal Data Protection (ASEAN TELMIN, 2016), and the ASEAN Work Programme on Electronic Commerce (ASEAN, 2017) (UNCTAD, 2018; Ministry of Planning and Investment, 2016).

These regional frameworks have guided Laos in developing a national legal framework for electronic communications, resulting in laws like the Law on Electronic Data Protection (World Bank, 2022; UNCTAD, 2018). According to the United Nations Development Programme

---

[139] The category of Least Developed Countries (LDCs) was formally established by the UN General Assembly in 1971 to secure targeted international support for the most vulnerable and disadvantaged nations within the UN framework (United Nations General Assembly, 1971). LDCs are characterized by their low income, high susceptibility to economic and environmental shocks, and limited human resources (UNESCO, n.d.).

[140] Gross National Income represents the total income earned by a nation's people and businesses, encompassing both domestic and foreign sources. It serves as a key indicator for measuring and monitoring a country's wealth over time. Gross National Income includes the nation's Gross Domestic Product along with any income received from abroad, providing a comprehensive view of its overall economic health (Investopedia, 2024).

[141] The Human Assets Index (HAI) is a composite metric that measures a country's level of human capital by integrating indicators of education and health, including adult literacy rates and under-five mortality rates (UNDESA, n.d.a.).

[142] Economic vulnerability refers to the susceptibility of a country's development process to disruptions caused by unforeseen exogenous events, commonly referred to as external shocks. Factors contributing to this predisposition include the instability of agricultural production, geographic remoteness, and being landlocked, all of which can significantly impede economic growth and resilience (Cariolle, 2010; UNDESA, n.d.b.)

(UNDP), Laos is emerging digitally, with a strong legal and regulatory foundation aligned with international agreements to promote digital adoption and consumer protection (Mukherji *et al.,* 2022).

Overall, Laos' ambition to graduate from LDC status, coupled with its desire to capitalize on the digital revolution and align with ASEAN's rapid development, has driven its regulatory advancements. Laos has drawn lessons from its ASEAN neighbors and agreements, but there is little evidence of influence from the European Union, particularly regarding the GDPR, which explains the divergence between Laos' Law on Electronic Data Protection and the GDPR.

3.1.3. Emulation

Laos, as a nation within the Asian continent, embodies a distinct set of values and principles that shape its approach to privacy. Ess (2005) posits that it may be possible to generalize that several Asian countries, including Laos, frame privacy rights, particularly in the context of data protection, as instrumentally necessary for the advancement of e-commerce. Greenleaf (2014) further suggests that privacy in these contexts is often safeguarded to ensure that forms of surveillance deemed in the public interest operate fairly for those under surveillance, while simultaneously rendering illegal any surveillance not seen as serving the public good. This contrasts with Western nations, where privacy is often justified not only as an instrumental necessity for democratic governance but also as an intrinsic good within a pluralistic framework (Ess, 2005).

Moreover, Laos is widely recognized as a one-party authoritarian state[143], where the ruling Lao People's Revolutionary Party exercises comprehensive control over all political processes and severely restricts civil liberties (Nuttin, 2017). The absence of organized political opposition, independent civil society, or a free media sector further underscores the lack of a robust mechanism to advocate for or protect privacy rights (Freedom House, 2017a). Additionally, Laos has been accused of numerous human rights violations (International Federation for Human Rights and Lao Movement for Human Rights, 2024; Amnesty International, 2023; Human Rights Watch, 2017, 2015).

These factors suggest that Laos places less emphasis on the right to privacy and data protection compared to the European Union, a difference rooted in its distinct socio-political context and pre-existing beliefs. Consequently, it is reasonable to infer that the Lao government's primary motivation in enacting the Law on Electronic Data Protection was not the protection of human rights, as is the case with the General Data Protection Regulation in

[143] For a more comprehensive analysis of Laos' political system, see, for instance: Creak and Barney (2018), and Croissant and Lorenz (2018)

the EU. Instead, the LEDP appears to prioritize economic development, social stability, and state security, as explicitly stated in multiple sections of the law[144].

3.2. Singapore

3.2.1. Competition

The timeline considered to analyze the competition mechanism in Singapore is between 2016 and 2020, because it refers to the time of the enactment of the EU's General Data Protection Regulation and the Singapore's Personal Data Protection Act, respectively. During this period, the European Union and Singapore have sustained a robust and long-standing economic relationship, marked by significant trade and economic partnerships (Elms, 2024). Between 2016 and 2019, the EU consistently ranked as Singapore's third-largest partner in merchandise trade, following China and Malaysia, contributing approximately 10% to 11% of Singapore's total trade in goods during this period (Ministry of Trade and Industry Singapore, 2019; 2018; 2017; 2016). Concurrently, the EU was Singapore's second-largest partner in services trade from 2017 to 2019, trailing only the United States. In 2019, bilateral trade in services between the EU and Singapore reached 57 billion USD, accounting for about 55%[145] of their total bilateral trade (European Services Forum, 2023; Department of Statistics Singapore, n.d.).

This strong bilateral relationship is further underscored in Singapore's critical role in the EU's global trade, particularly within the ASEAN region. Singapore has consistently been the EU's leading trading partner in ASEAN, dominating both merchandise and services trade. In 2018, Singapore accounted for over 24% of the EU's merchandise trade with ASEAN, and in 2017, it represented more than 57% of the EU's services trade with the region (EU-ASEAN Business Council, 2019). Globally, Singapore was the EU's fourth-largest partner in services trade in 2016 and the 14th largest in goods trade by 2017 (European Commission, 2018a; European Parliamentary Research Service, n.d.). Although the value of EU imports of goods from Singapore declined between 2018 and 2020, following growth from 2016 to 2018, imports of services from Singapore demonstrated steady growth over the same period (European Services Forum, 2023; European Union Delegation to Singapore, 2023).

[144] Article 1 of the Lao Law on Electronic Data Protection clearly outlines the primary objectives of the legislation: "to contribute in Socio-Economic Development of the nation, ensures the stability of the nation, peace and orderliness of the society" (Lao People's Democratic Republic, 2017). These goals are reiterated throughout the legal text, particularly in Articles 5, 13, 22, 29, and 30.

[145] The percentage was calculated by dividing the total value of services traded between Singapore and the EU by the total trade value (encompassing both goods and services) between the two entities, and then multiplying the result by 100. The data for this calculation was sourced from the European Services Forum (2023).

The economic relationship between the EU and Singapore was further solidified by the EU-Singapore Free Trade Agreement (EUSFTA), which came into effect in 2019 (Subhani, 2023). This agreement improved market access for businesses from both regions, streamlining technical regulations and facilitating trade. However, it did not lower EU standards for products and services from Singapore, requiring full compliance with EU regulations, including stringent data protection laws (European Commission, n.d.b-c.).

Singapore's exports to the EU, particularly in data-intensive sectors such as business management, financial services, and transport, subject Singaporean companies to EU regulations, including the GDPR. The EUSFTA has expanded trade opportunities, but it has also emphasized the need for these firms to comply with EU legal frameworks (European Union Delegation to Singapore, 2023; 2022). Additionally, by 2019, over 10,000 EU companies operated in Singapore, regularly engaging in data transfers or providing services to European consumers, which placed them under GDPR jurisdiction and likely influenced Singapore's government to align its regulations with European standards (European Commission and Ministry of Trade and Industry Singapore, 2019).

Overall, the strong economic ties between the EU and Singapore, particularly in data-intensive services, have led to significant GDPR influence on Singaporean companies' data protection practices. This reflects a *de facto Brussels Effect*, where firms opt to comply with GDPR over weaker local regulations, driven by competitive pressures. It is likely that these companies have also pressured the government to align Singapore's Personal Data Protection Act with GDPR standards, demonstrating a *de jure Brussels Effect*. While this alignment does not entail a direct adoption of the EU regulation into Singaporean law, it would effectively allow Singaporean law to recognize EU standards as equivalent to its own, thus achieving a similar outcome.

3.2.2. Learning

Corning (2024) suggests a strong coincidence between the timing of public forums organized by the Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) from 2017 to 2019, and the enactment of the General Data Protection Regulation (GDPR) in 2016, indicating the GDPR's potential influence on the initiative to amend the 2012 Personal Data Protection Act (PDPA). While this timing highlights the GDPR's influence on the review process, it would be an oversimplification to view the PDPA revisions as solely a reaction to the GDPR. The updates were also significantly driven by the increasing frequency of data breaches and Singapore's ambition to solidify its position as a major digital economy (Corning, 2024).

This ambition is part of Singapore's broader strategy to establish itself as the foremost digital sustainability hub in Asia and beyond (Birch, 2023). Reflecting this goal, Singapore

consistently ranks among the most competitive, innovative, and digitally advanced nations globally (Smart Nation Singapore, n.d.a.). The International Institute for Management Development[146] ranked Singapore 7th among smart cities from 2020 to 2023, rising to 5th in 2024 (IMD, n.d.). Additionally, Singapore has been recognized as the most digitally competitive nation in the Asia Pacific region every year from 2019 to 2023, except in 2022, when it ranked second; globally, it has remained in the top five over the past five years (IMD, 2023).

Singapore's digitization journey commenced in 1981 with the Civil Service Computerisation Programme and the establishment of the National Computer Board, progressing through strategic initiatives such as IT 2000 and successive e-Government Masterplans. While these early efforts were primarily aimed at enhancing public service efficiency, a more comprehensive vision of digital transformation emerged with the launch of the Smart Nation initiative by Prime Minister Lee Hsien Loong in 2014 (Jie, 2018). This initiative seeks to digitize various aspects of urban life through collaboration with businesses, citizens, and NGOs, focusing on three core pillars: the Digital Economy, Digital Government, and Digital Society. Central to achieving these objectives is a strong emphasis on key enablers, particularly cybersecurity and data privacy (MyNZTE, 2022; Jie, 2018; Smart Nation Singapore n.d.b.).

Although data privacy has been regulated under the Personal Data Protection Act since 2012, the evolving challenges of the late 2010s underscored the need for an update. While significant data breaches were relatively rare in the early 2010s, by the end of the decade, high-profile incidents had become more frequent and severe. This increase reflects a broader global trend driven by rapid digital transformation and escalating cyber threats (Data Protection Excellence Network, 2019; Octalibrayani, n.d.).

In 2016, Uber's global data breach marked a significant turning point, compromising the personal information of 380,000 individuals in Singapore – including names, email addresses, and mobile phone numbers – and representing the largest reported data breach in the country to that date (Corning, 2024; Hio, 2017).

Surpassing the impact of the 2016 incident, the 2018 cyberattack on SingHealth marked a significant escalation in the threat landscape. This breach compromised the personal data of 1.5 million patients – including names, NRIC numbers, addresses, and dates of birth – along with the records of Prime Minister Lee Hsien Loong (Corning, 2024; Tham, 2021). The attack, characterized as deliberate, targeted, and well-coordinated, intensified concerns about potential state-sponsored cyber activities (Baek, 2024).

[146] The International Institute for Management Development (IMD) is an independent academic institution with Swiss origins and a global presence, established over 75 years ago by business leaders, for the advancement of business leadership and management practices (Kagan, 2023; The Conversation, n.d.).

In 2019, the cybersecurity landscape in Singapore continued to deteriorate as the Data Protection Excellence Centre reported an unprecedented surge in violations of the Personal Data Protection Act. The number of organizations found in breach surpassed the total number of enforcement cases from the previous year, highlighting a significant escalation in data protection challenges (Data Protection Excellence Network, 2019).

These data breaches revealed significant vulnerabilities, highlighting an urgent need to reassess and enhance government data security policies to effectively manage both current and future threats (Baek, 2024; Public Data Security Review Committee, 2019). This reassessment was crucial, as inadequate security could undermine Singapore's broader strategy to position itself as a global leader in the digital economy (Corning, 2024).

In response, Singapore undertook a comprehensive revision of the Personal Data Protection Act to balance individual privacy protection with the needs of its growing digital economy. While the General Data Protection Regulation served as a reference, its strong emphasis on human rights contrasted with Singapore’s focus on economic development. Consequently, Singapore adopted a selective approach, incorporating elements of the GDPR that align with its national priorities and intentionally omitting those that might impede economic growth (PDPC Singapore, 2019).

This selective adoption is exemplified by Singapore's inclusion of deemed consent within the PDPA, a provision absent in the GDPR. The PDPA’s expanded scope of deemed consent facilitates the collection, use, and disclosure of personal data for legitimate interests and business purposes. This new exception to consent requirements provides organizations with greater flexibility to leverage data for business innovation (Lui et al., 2022; Alfred, 2020).

Other key amendments to the PDPA, such as the introduction of the right to data portability, mandatory data breach notification, and enhanced enforcement powers for the Personal Data Protection Commission, closely mirror similar provisions in the GDPR. These amendments underscore shared objectives between Singapore and the EU, such as advancing consumer autonomy, boosting competition, and strengthening data protection. For example, data portability enhances consumer control over personal information, which promotes economic dynamism (Lui et al., 2022). Similarly, mandatory data breach notifications and reinforced enforcement mechanisms contribute to a more stringent and accountable approach to data protection.

In summary, while Singapore has drawn valuable insights from the GDPR, it has tailored its approach to meet its national objectives, demonstrating a strategic adaptation rather than a direct replication of the GDPR framework. This adaptation indicates that learning has played a significant role in the GDPR’s influence beyond EU borders, even though there is no complete adoption of its provisions. Singapore’s approach demonstrates how countries can tailor international regulations to fit their unique contexts and objectives.

3.2.3. Emulation

Singapore foreign policy elites perceive the European Union as a primarily one-dimensional actor, whose influence is largely confined to its economic strength, particularly in trade and economic integration. However, this economic presence does not translate into significant political or military influence, especially when contrasted with the dominant roles of the United States and China in the Southeast Asian region (Wong, 2012a). This assessment is corroborated by a 2019 ISEAS-Yusof Ishak Institute[147] regionwide online survey involving participants from policy, research, business, civil society, and media sectors across Southeast Asia. The survey revealed that 45.2% of respondents identified China as the most influential power in political and strategic matters, while 30.5% viewed the United States as the leading actor in this domain. The European Union, by contrast, was ranked a distant fifth, with a mere 0.7% of respondents recognizing it as the most influential in political and strategic affairs (Mun *et al.*, 2019).

Furthermore, the EU is often criticized for being an outdated institution, perceived as slow to adapt to the rapidly evolving global landscape (Jie, 2016). This criticism is echoed by former Singaporean diplomat Kishore Mahbubani (2008), who famously described the EU as "*a political dwarf*" in its response to the shifting geopolitical environment.

In addition to these criticisms, the EU's self-perception as a normative power – particularly in areas such as peacemaking, environmental policy, and human rights – is not universally shared, especially by Singapore and the broader ASEAN region (Jie, 2016). Studies of elite opinions by Jie (2016) and Portela (2010) reveal that Singaporean policy elites are often dismissive or critical of the EU's approach to human rights and its perceived interference in internal affairs. However, it is worth noting that other groups, such as media and civil society elites, view the EU's role more positively, recognizing its influence as beneficial (Portela, 2010).

This divergence in views contributes to a strained relationship between the EU and ASEAN, as ASEAN frequently perceives the EU's strong emphasis on human rights as inflexible and obstructive (Jie, 2016). Bilahari Kausikan, former Permanent Secretary of the Ministry of Foreign Affairs of Singapore, expressed this perspective during a seminar, arguing that "*Europe is tying itself into knots by clinging to systems of values; systems based on an extreme ideological conception of the universality of rights taken to ridiculous lengths – a reductio ad absurdum of values – and which moreover are out of sync with societies that are*

[147] Founded in 1968 and renamed in 2015 to honor Singapore's First President, the ISEAS–Yusof Ishak Institute is an autonomous research center in Singapore, focusing on socio-political, security, and economic trends in the Southeast Asia region. It promotes scholarly debate, public awareness, and solutions to regional issues through various research programs, conferences, publications, and a large library (ISEAS–Yusof Ishak Institute, n.d.).

evolving under demographic or other pressures in entirely different directions" (apud Jie, 2016, p.4).

Kausikan's critique touches on the broader and long standing debate between Asian and Western values, a discussion that gained prominence in the 1990s (Boll, 2001). Singapore and Malaysia were particularly vocal in this debate, challenging what they perceived as Western attempts to establish global intellectual and cultural hegemony by imposing Western notions of rights under the guise of universalism (Ghai 1998 apud Boll, 2001).

The discourse surrounding Asian values is rooted in four primary claims. First, human rights are not universal and cannot be universally applied; rather, they emerge in response to specific social, economic, cultural, and political contexts. Second, Asian societies prioritize the family over the individual, viewing the nation as an extended family, where it is considered natural for collective interests to take precedence over individual rights. Third, Asian societies place greater emphasis on social and economic rights than on individual political rights. Finally, the principle of national self-determination includes the government's authority over domestic human rights matters, suggesting that external interference in a state's internal affairs, including its human rights policies, is unwarranted (Hoon, 2004).

While the distinctiveness of so-called Asian values may have been somewhat overstated for ideological purposes or to justify authoritarian practices in certain countries, it is evident that, despite their internal differences, Asian nations may have experiences, understandings, and priorities that diverge from those of EU Member States (Flers, 2010).

For instance, privacy rights have deep roots in Europe and are enshrined as fundamental rights within the EU's constitutional framework (Chik & Pang, 2014). In contrast, in Singapore, privacy concerns are relatively recent and are primarily viewed through a practical lens. Although there is growing concern over privacy and increasing distrust of companies handling personal data in Singapore, these concerns are driven more by high-profile data breaches and the complexities of privacy policies than by a fundamental recognition of privacy as a basic right (Ross, 2022).

Furthermore, Singapore's legislative approach to privacy significantly differs from that of other jurisdictions; instead of treating the protection of personal data as a fundamental right, Singapore's laws focus on balancing individual rights with economic interests in a technology-driven environment (Angeline, 2024; Setiawati et al., 2019; Chik & Pang, 2014). A clear example of this difference is seen in Singapore's Personal Data Protection Commission response to a decision by Italy's data protection authority to ban ChatGPT. The ban was due to concerns over the extensive collection and use of personal data, lack of age restrictions, and the potential for ChatGPT to provide factually incorrect information. Singapore's PDPC considered this decision overly harsh and opts for a more balanced approach in Singapore

that aims to protect data and mitigate risks while still fostering market innovation (PDPC Singapore, 2023).

Overall, it is evident that Singapore does not regard the EU as a normative power, as reflected in its stance during the 1990s debate over Asian versus Western values. Furthermore, Singapore's understanding of values, including privacy, diverges significantly from that of the EU. Even though Singapore's Personal Data Protection Act includes individual rights similar to those in the EU's General Data Protection Regulation, these rights were established out of practical necessity rather than an alignment with the EU's normative values. Hence, emulation does not appear as a relevant mechanism in the influence of the GDPR in Singapore. At most, the European Union functioned primarily as a reference point or benchmark for comparison, rather than as an active influence shaping the discourse surrounding the review of the Personal Data Protection Act (PDPC Singapore, 2019; Wong, 2012b).

3.3. Thailand

3.3.1. Competition[148]

The 2016 to 2019 period was selected for analyzing Thailand's competition mechanism, as it spans the time between the enactment of the EU's General Data Protection Regulation and Thailand's Personal Data Protection Act, respectively. Throughout these years, trade relations between the European Union and Thailand experienced steady growth, with the EU continuing to be one of Thailand's major trading partners. From 2016 to 2018, the EU consistently ranked as Thailand's third-largest trading partner in terms of goods[149]. By 2019, the EU's position had

[148] As is common in many international trade statistics, the records of trade between the EU and Thailand show significant discrepancies depending on the data source. Discrepancies in trade data arise from different customs valuation methods along with factors like transshipment, re-exports, and trade fraud involving undervaluation to evade tariffs and taxes (Kee, 2024).

Databases like UN COMTRADE and WITS help reconcile trade data discrepancies for analytical purposes (Javorsek, 2016). UN COMTRADE, considered the most comprehensive trade database, sources data from official agencies and uses estimates or mirror data when needed (Muryawan & Paca, 2024; UN COMRADE, n.d.). WITS, developed in collaboration with institutions like the World Bank and UNCTAD, consolidates trade and trade protection data from multiple international agencies, including UN COMTRADE, into a single platform (Kaushik, 2024).

However, there are two key challenges with using these databases. First, as Linsi et al. (2023) highlight, relying on mirror data can be problematic, as neither import nor export data is consistently more reliable. However, in cases where using mirror data is unavoidable, the best approach is to rely on reputable sources like UN COMTRADE and WITS (WITS, 2010). Second, neglecting the growing importance of trade in services. To address this, databases like WITS are needed for service trade data. However, WITS does not provide aggregated data for the entire EU, offering data only for individual EU states or the broader Europe and Central Asia region. As a result, this study had to rely on secondary sources, such as Eurostat and Thailand’s Ministry of Commerce, despite potential biases, due to the lack of comprehensive data on Thailand-EU service trade.

[149] This information is drawn from the WITS (n.d.b-d) database for the specified years, identifying China, Japan, the US, and Malaysia as Thailand's key trade partners in goods. However, since the WIPS database excludes the EU as a potential partner, data on EU-Thailand trade relations was sourced from

slightly shifted, becoming Thailand's fourth-largest trading partner[150]. In comparison to other leading trading partners, however, the European Union's share of Thailand's total goods trade is somewhat smaller. During the same period from 2016 to 2018, China emerged as Thailand's dominant trading partner, consistently accounting for 15-16%[151] of Thailand's total trade in goods. In contrast, the EU's share of Thailand's goods trade hovered around 9%[152], which significantly lags behind China's larger slice of the trade pie.

From the EU's perspective, Thailand holds a modest position in its global trade network. Between 2016 and 2019, Thailand accounted for just about 1%[153] of the EU's overall trade in goods, making it a relatively minor player in the broader scope of European trade relations. By 2018, this positioned Thailand as the EU's 25th largest trading partner globally (Kunnamas, 2020).

However, within the ASEAN region, Thailand plays a more prominent role in EU trade relations. In 2017, Thailand was the EU's second-largest ASEAN partner in services trade, contributing 11.9% of the total trade in services between the EU and ASEAN countries (EU-ASEAN Business Council, 2019). Furthermore, when it comes to trade in goods, Thailand consecutively ranked as the EU's fourth-largest ASEAN partner from 2016 to 2019[154].

Despite the relatively strong trade relationship, these ties have not created significant pressure on Thai businesses to comply with the EU's General Data Protection Regulation. This is due to two primary factors: the limited scope of services trade and the predominance of Small and Medium-sized Enterprises (SMEs) in Thailand's economy.

Trading Economics (n.d.a-b), which utilizes the United Nations COMTRADE database for international trade. By integrating data from both sources, the EU was identified as Thailand's third-largest trading partner.

[150] The data collection and analysis process followed the same methodology described in the in-text reference 201, with the only change being the focus on the year 2019. The data was retrieved from WITS (n.d.e.).

[151] The percentage was determined by dividing the total value of goods traded between Thailand and China by the total value of Thailand's global trade in goods, and then multiplying the result by 100. Data on the trade value between Thailand and China was obtained from the WITS (n.d.b-e) database, while the total value of Thailand's global trade was sourced from Trading Economics (n.d.c-d), which in turn relied on data from the Ministry of Commerce of Thailand.

[152] The percentage was calculated by dividing the total value of goods traded between Thailand and the EU by the total value of Thailand's global trade in goods, then multiplying the result by 100. Data on Thailand-EU trade was sourced from Trading Economics (n.d.a-b), which in turn used the United Nations COMTRADE database. The total value of Thailand's global trade was also obtained from Trading Economics (n.d.c-d) with data provided by the Ministry of Commerce of Thailand.

[153] The percentage was calculated by dividing the total value of goods traded between Thailand and the EU by the total value of EU's global trade in goods, then multiplying the result by 100. Data on Thailand-EU trade was sourced from Trading Economics (n.d.a-b), which in turn used the United Nations COMTRADE database. The total value of EU's global trade was also obtained from Trading Economics (n.d.e-f), with data provided by Eurostat.

[154] To determine this, the total amount of EU exports and imports for all ASEAN countries – Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam – were calculated and ranked. The data was retrieved from Trading Economics (n.d.a-b,g-x), which in turn used the United Nations COMTRADE database.

By 2019, services exports to the EU represented only about 10% of Thailand's total exports, a notably low percentage compared to the global average (European Chamber of Commerce Thailand, 2023; European Services Forum, 2023). This is reflective of Thailand's broader economic profile, where the services sector constitutes just 55.6% of GDP and employs only half of the workforce. This contrasts sharply with advanced economies, where the services sector typically has a higher employment share (European Services Forum, 2023). This is relevant because the businesses with greatest exposure to the GDPR are often in services such as airlines, hotels, and online retailers dealing directly with EU citizens. Therefore, a low trade in services might impact the amount of data handling between Thailand and the EU and therefore the need to comply with the GDPR (Corning, 2024).

Moreover, by 2018 SMEs constituted a major driving force of Thailand’s economy, contributing approximately 45% of the country’s GDP, amounting to 7 trillion THB (215 billion USD). Interestingly, small enterprises alone contribute 31% of GDP, surpassing medium-sized enterprises at 12% (Korwatanasakul & Paweenawat, 2020). Due to their scale and limited resources, SMEs, especially small enterprises, tend to be less affected by the GDPR, and many even lack the capability to comply with its stringent requirements (Corning, 2024).

Nevertheless, the Thai government, notably through figures like Pichet Durongkaveroj, Minister of Digital Economy and Society from 2016 to 2019, has consistently demonstrated a commitment to promoting responsible data management practices among businesses. The government has encouraged companies to handle personal information responsibly – collecting, using, and disclosing it with proper consent – in order to minimize potential negative impacts on foreign trade and investment (Tortermvasana, 2019; Limsamarnphun, 2018). This concern is partly informed by previous experiences with EU-imposed bans and restrictions on Thailand's fishing industry, which were triggered by issues related to illegal, unreported, and unregulated (IUU) fishing. Acknowledging the EU's use of its market power and economic instruments, such as bans, boycotts, and restrictions, to advance its political objectives, the Thai government has advised businesses to comply with EU data protection standards to safeguard trade relations (Herman, 2015; Asia Society Policy Institute, n.d.).

Overall, while trade relations between the EU and Thailand are not particularly robust from a global perspective, Thailand remains one of the EU's most important trading partners within ASEAN, and the EU continues to be one of Thailand's key trade partners. Interestingly, this trade relationship has not exerted substantial pressure on Thai businesses to comply with the GDPR, largely due to the relatively limited role of data-driven services and the dominance of small and medium-sized enterprises (SMEs) in the Thai economy. Consequently, there is little incentive for Thai businesses to advocate for the adoption of GDPR-like regulations.

In contrast to Bradford’s (2012) concept of the *de jure Brussels Effect*, where businesses typically lobby for stricter regulations, the situation in Thailand follows a different trajectory.

Rather than being driven by industry-led initiatives, the impetus for compliance with the General Data Protection Regulation in Thailand stems from the government, specifically the Ministry of Digital Economy and Society (MDES). This governmental encouragement is motivated by prior instances of non-compliance with EU regulations, which resulted in adverse effects on foreign trade and investment. In an effort to mitigate such risks, the Thai government is adopting a top-down approach to regulatory enforcement, in contrast to the bottom-up, industry-driven model typically associated with the *Brussels Effect*.

3.3.2. Learning

Since the 1990s, Thailand has pursued digital government strategies aimed at bolstering economic development and addressing societal challenges. The country's e-government reforms began with the "IT 2000" policy in 1996, which sought to establish a digital infrastructure, including the Government Information Network to enhance communication across agencies. However, these efforts were hindered by compatibility issues due to the disparate approaches of individual agencies (Danuvas et.al., 2018).

To address these challenges, the "IT 2010" framework (2001-2010) introduced the '5Es Strategy,' which expanded the focus to include e-Government, e-Industry, e-Commerce, e-Education, and e-Society, with an emphasis on improving quality of life and driving economic growth. This period also saw significant advancements in broadband expansion and increased ICT access across the country. The subsequent "IT 2020" framework, launched in 2011 under the banner of "Smart Thailand 2020", aimed to transform Thailand into a *smart nation*, with a particular focus on expanding ICT access in rural areas (Danuvas et.al., 2018).

Recognizing the growing importance of the digital economy, the Thai government established the Ministry of Digital Economy and Society (MDES) in 2016. In 2017, the Digital Development for Economy and Society Act was enacted, providing the legal and regulatory framework to support the country's digital policies. This Act outlines the roles and responsibilities of various government agencies and establishes key structures, including the MDES and the National Digital Economy and Society Committee. It also initiated the Digital Development Plan for Economy and Digital Society (also known as the National Digital Economy Master Plan) and created the Digital Economy and Society Development Fund to finance future digital initiatives (Postigo, 2023).

The National Digital Economy Master Plan envisions a 20-year transformation divided into four phases: laying the digital foundations, achieving digital inclusion, transitioning to full digital transformation, and ultimately attaining global digital leadership (Bukht & Heels, 2018; Ariyapruchya *et al.*, 2017). Among the initiatives launched as part of this plan is Thailand 4.0, an economic model designed to foster sustainable, technology-driven growth and broader access to economic benefits. This model specifically targets key challenges such as the

middle-income trap, unbalanced growth, inequality, and declining export competitiveness (Danuvas et.al., 2018; Anuroj, n.d.).

As Thailand advanced its digital economy in the second decade of the millennium, it faced significant challenges related to security threats from data breaches (Pornwasin, 2018; Supernap Thailand, 2018). Notable incidents included the 2018 breaches at Krung Thai Bank and Kasikorn Bank, which compromised the data of over 120,000 customers (Corning, 2024; Xinhua, 2018). That same year, TrueMove H, the nation's second-largest mobile operator, experienced a breach exposing the personal data of more than 46,000 customers (Leesa-nguansuk & Tortermvasana, 2018). Additionally, in 2019, an open database linked to Orvibo Smart Home products was discovered, revealing over 2 billion records, including those of users in Thailand (Henriquez, 2019). These incidents severely eroded public trust, with less than 50% of Thais in 2019 expressing confidence in the secure management of their personal data, compared to a 70% average in other Asia-Pacific countries (Corning, 2024).

The frequency and scale of these breaches highlighted the critical need for robust data privacy protections and hastened the drive to enact comprehensive data privacy legislation (Pornwasin, 2018; Supernap Thailand, 2018; The Nation, 2018). However, given that Thailand did not implement its Personal Data Protection Act until 2019, with enforcement beginning only in 2022, the country focused in the interim on promoting compliance with other internationally relevant laws, particularly the EU's GDPR (The Nation, 2018).

This effort received strong backing from Puttipong Punnakan, who served as Minister of Digital Economy and Society from 2019 to 2021. Punnakan played a key role in advancing the Thailand Data Protection Guidelines, with the first edition focused on educating Thai businesses about international data protection standards, particularly the GDPR. The second edition was aimed at preparing businesses for compliance with the forthcoming PDPA (Punnakan, 2019). Additionally, there was a broad incentive for companies to obtain GDPR certification, which not only ensured responsible data management but also enhanced organizational reputation and built trust with customers (Hussain, 2023).

Thailand's alignment with the GDPR serves two key purposes. First, it ensures continued access to the EU market and enhances digital competitiveness, particularly in significant markets such as the EU (Hussain, 2023; The Nation, 2018; Asia Society Policy Institute, n.d.). The motivation for Thailand's compliance with the GDPR through the Personal Data Protection Act is closely linked to prior EU sanctions on its fishing and civil aviation sectors (Asia Society Policy Institute, n.d.). These sanctions underscored the importance of adhering to international standards, including data protection, to maintain favorable trade relations. According to PDPC Chairman Thienchai, failing to adopt a data protection law comparable to the GDPR could lead to significant trade barriers, reinforcing the necessity of aligning with these international

standards to avoid similar penalties and secure continued access to key markets like the EU (The Nation, 2022).

Secondly, the PDPA aims to bolster Thailand's position in the global digital economy by attracting foreign investment and establishing the country as a key hub for data centers (Asia Society Policy Institute, n.d.; Jiravuttipong & Trasadikoon, n.d.). Adhering to GDPR standards enhances Thailand's credibility in this endeavor, promoting trust and transparency, affirming its commitment to fundamental digital rights, and strengthening its international reputation (Hussain, 2023; The Nation, 2018; Asia Society Policy Institute, n.d.).

However, closer examination reveals that while the PDPA draws on best practices from the GDPR, it has been tailored to the Thai context, granting the government certain preferential exemptions and the flexibility to expand its powers as needed (Asia Society Policy Institute, n.d.). This suggests that Thailand leveraged the EU's approach to data protection during a period when it lacked its own framework but made deliberate adaptations to fit local conditions and governmental priorities. Consequently, while Thailand has clearly learned from the GDPR, it has not adopted the EU regulation in its entirety.

3.3.3. Emulation

In Thailand, the Western concept of privacy – grounded in individualism, liberalism, the public-private divide, and the rule of law – does not closely align with traditional Thai cultural and historical norms. Notably, the Thai language lacks a native term for privacy (Corning, 2024). This divergence is largely shaped by the strong influence of Buddhist teachings and a historical precedent of state surveillance, which together have fostered a distinct understanding of privacy (Corning, 2024; Ramasoota & Panichpapiboon, 2014).

Buddhism's view, which regards attachment to the self and possessions as a source of suffering has shaped a cultural context in which individual rights, including the right to privacy, are not regarded as inherent to human existence, nor is their protection strongly prioritized (Corning, 2024; Kitiyadisai, 2005). Additionally, the practice of collecting personal information has deep historical roots in Thailand, from ancient customs such as wrist tattooing in the 13th century to modern-day measures like smart ID cards in the 21st century (Corning, 2024; Ramasoota & Panichpapiboon, 2014).

Thailand's historical context and conservative social norms have resulted in limited public awareness and understanding of privacy issues. Civil society leaders and activists suggest that this has led to widespread ignorance and inertia on privacy matters (Ramasoota & Panichpapiboon, 2014). For instance, while the 1949 Thai Constitution nominally protected the right to privacy, research in the early 2000s found that many Thais viewed privacy more as a tool for ensuring security or legal protection, rather than as a fundamental human right (Corning, 2024). The protracted development of privacy legislation, which took nearly two

decades to pass, further reflects the lack of awareness and prioritization of privacy issues (Chawla, 2019).

In recent years, the increased prevalence of electronic transactions in Thailand has heightened awareness of the risks associated with information technology misuse, particularly by corrupt officials or hackers. The introduction of smart ID cards, implemented before the enactment of comprehensive data protection legislation, faced significant criticism from civil society activists, academics, and human rights advocates as a major threat to privacy (Kitiyadisai, 2005).

As a result, the younger generation has increasingly prioritized and recognized the importance of privacy rights. This growing awareness has led to the emergence of new professional and civil society organizations dedicated to advocating for stronger data privacy protections. For example, the Thai Webmaster Association introduced a professional code of ethics that included data privacy in 2002, while the Thai Netizen Network (established in 2008) and the Asia Centre (founded in 2015) have been actively working to promote data privacy as a human right (Corning, 2024; Chawla, 2019).

However, the influence of these civil society groups was significantly curtailed during the period of military rule[155] from 2014 to 2019. The regime imposed stringent restrictions on organizations defending human rights, frequently citing laws on political gatherings and public disturbances as justification for heavy surveillance or outright bans on their activities (Freedom House, 2019, 2018, 2017b, 2016; Refworld, 2015). This repression was particularly acute for civil society organizations in Thailand that receive funding from Western countries, as they are often accused of advancing Western interests (Sombatpoonsiri, 2018). Consequently, this repressive environment complicates the task of directly correlating these groups' advocacy efforts with the eventual passage of the Personal Data Protection Act (Corning, 2024).

Although public awareness of data privacy as a fundamental human right has grown, this shift in perception has not necessarily led to a corresponding change in the government’s stance on privacy. The Thai government’s approach is shaped by its historical context, including surveillance practices, Buddhist traditions, and a deep-rooted suspicion of foreign influence. Consequently, instead of aligning with European standards of privacy and data protection, the government enacted the PDPA in 2019 largely in response to rapid technological growth and the misuse of citizens’ data (Chawla, 2019).

[155] On May 22, 2014, the military junta known as the National Council for Peace and Order (NCPO), led by General Prayuth Chan-ocha, overthrew Thailand's elected government, citing a need to restore order after political unrest. However, the regime used law arbitrarily to suppress civil rights and enable violence. Although the NCPO dissolved after the 2019 elections, the military retained influence, with General Prayuth becoming the elected prime minister, transitioning Thailand from outright military rule to a military-dominated democracy (Haberkorn, 2021; Rojanaphruk, 2019).

3.4. Socialization

In 2017, the European Commission, in a Communication to the European Parliament and the Council, recognized a strategic opportunity for the EU to promote its data protection values globally. The Commission emphasized that aligning international legal frameworks with the EU's robust data protection standards could enhance global data flows and bolster consumer confidence in companies that prioritize the secure handling of personal data. By doing so, the EU positioned its high data protection standards as a competitive advantage in the global digital economy (European Commission, 2017).

Building on this foundation, in 2018, the EU further acknowledged the growing significance of its relationship with Asia, particularly in trade and economic contexts. To capitalize on this potential, the European Commission proposed an EU Strategy on Connecting Europe and Asia to strengthen regional cooperation and foster long-term economic integration. This strategy aimed to improve digital connectivity by ensuring a secure ICT environment, emphasizing cybersecurity, online rights protection, and personal data safeguarding. It also called for a unified regulatory approach to boost digital infrastructure investments and address the digital divide in remote areas (European Commission, 2018b). Thus, the 2018 strategy extended the EU's global data protection agenda into a practical framework for regional connectivity and economic growth.

However, this strategy only moved forward in 2020, when the EU and ASEAN Foreign Ministers issued a joint statement underscoring the critical role of connectivity – particularly digital connectivity – as a driver of inclusive growth and sustainable development. They emphasized that protecting human rights online and personal data is essential for effective digital connectivity, advocating for collaboration in data privacy, cybersecurity, and cross-border data flows to create a secure and inclusive digital ecosystem (ASEAN-EU, 2020). Shortly after, the EU launched the Digital4Development Hub with the goal of scaling up investments in the digital transformation of partner countries. The hub also sought to promote a values-based framework for the global digital economy and strengthen the EU's involvement in international digital partnerships (European Commission, 2020b).

Building on the EU's efforts to enhance digital cooperation with ASEAN, the Enhanced Regional EU-ASEAN Dialogue Instrument facilitated a series of 11 workshops in 2021. These workshops covered a wide range of topics, including technical skills like data visualization and broader issues such as the digital economy's interconnectedness and EU e-commerce regulations. The main goal was to equip ASEAN representatives with the knowledge to develop and utilize the ASEAN Digital Index (ADIX), which measures digital integration and informs economic policies (EEAS, 2021). This index is vital for advancing ASEAN's regional

digital economy and aligns with the digital transformation objectives outlined in the ASEAN Digital Masterplan 2025[156] (EEAS, 2021).

In 2022, the EU and ASEAN celebrated 45 years of diplomatic relations and strengthened their strategic partnership with a new plan for 2023-2027 focused on the digital economy. The EU pledged to support the ASEAN Digital Masterplan 2025 through policy exchanges, technical assistance, and collaboration on areas such as cybersecurity, digital governance, and sustainable digital services. The partnership also aims to improve business connectivity, facilitate cross-border trade, and advance ICT priorities like the ASEAN Digital Index (ADIX) (Council of the European Union, 2022; EEAS, 2022). During the summit commemorating this milestone, the EU-Singapore Digital Partnership was launched, set to take effect in 2023. This partnership aims to enhance digital trade, connectivity, and transformation by advancing technology, infrastructure, and public services, while ensuring legal certainty, online security, and reducing trade barriers (European Commission, 2023; Ministry of Trade and Industry Singapore, n.d.).

Additionally, in 2023, ASEAN adopted a standard contractual clause in cooperation with the EU, resulting in the Joint Guide to ASEAN Model Contractual Clauses (MCC) and EU Standard Contractual Clauses (SCC). This Joint Guide, building on the commonalities between the ASEAN MCCs and EU SCCs, provides businesses operating across both regions with a practical tool to facilitate compliance with data protection regulations (ASEAN Secretariat and European Commission, n.d.).

In summary, in recent years, the EU has significantly enhanced its regional strategy in ASEAN[157] by emphasizing digital connectivity and advocating for its values, particularly in personal data protection. However, its influence on data protection laws in Laos, Singapore, and Thailand has been limited. This limitation stems from the EU's regional approach to collaboration – partnering individually only with Singapore – and the fact that its engagement in digital connectivity started after these countries had already established their own regulations. As a result, while the EU has advanced its digital agenda and sought alignment with ASEAN's digital framework, its impact on shaping personal data protection laws through direct influence and socialization has been minimal.

[156] The ASEAN Digital Master Plan 2025, launched in 2021, envisions ASEAN becoming a leading digital community and economic bloc. To achieve this, governments, regulators, and market players must collaborate on investments in emerging technologies, removing regulatory barriers, and improving high-speed connectivity. The plan aims to boost ASEAN's post-COVID-19 recovery, expand broadband coverage, ensure reliable digital services, foster market competition, enhance e-government, and promote cross-border trade, ultimately building a more inclusive digital society (Ing et al., 2023; ASEAN, 2021b).

[157] For a comprehensive analysis of the EU strategy and its cooperation within the ASEAN region, see: Gil (2021), Gilson (2020), and Biedermann (2019)

Conclusion

This study analyzed the influence of the EU's General Data Protection Regulation (GDPR) on the data protection laws of selected countries from the Association of Southeast Asian Nations (ASEAN), specifically Laos, Singapore, and Thailand.

The research commenced by situating the GDPR within its historical context, particularly emphasizing its key innovations relative to the prior legislative framework in the European Union, specifically the Data Protection Directive of 1995. Drawing on the analyses of Carrillo and Jackson (2022) and Bennett (2018), the study identified critical elements that distinguish the GDPR from its predecessor, noting that many of these features represent evolutions of existing concepts in data protection rather than entirely new ideas. This identification of key elements established a framework for evaluating the GDPR's influence on the data protection laws of selected ASEAN countries. The findings demonstrate significant variations in how these elements have been integrated into the domestic legislation of Laos, Singapore, and Thailand.

Of the three, the Lao Law on Electronic Data Protection (LEDP) is the least aligned with the GDPR, differing notably in key areas. For instance, the LEDP provides a less precise definition of personal data and fails to distinguish between data controllers and processors. Additionally, its applicability is limited to domestic contexts, and it provides only vague references to consent, along with minimal data subject rights; notably, the right to erasure is one of the few parallels to the GDPR.

The responsibilities assigned to Data Protection Officers and supervisory authorities under the LEDP are also constrained, lacking the requisite independence outlined in the GDPR. Furthermore, the mechanisms for data breach notifications and penalties in Laos contrast sharply with those established by the GDPR. In Laos, the onus of notifying data breaches falls exclusively on the data owner. Additionally, although penalties under the LEDP are typically less stringent – often limited to minimal amounts compared to GDPR fines – they can nonetheless be severe, potentially encompassing criminal sanctions and a range of enforcement measures for non-compliance. Moreover, the LEDP does not impose requirements for *privacy by design* or *by default*, nor does it mandate Data Protection Impact Assessments, highlighting significant gaps in its regulatory framework compared to the GDPR.

In contrast, Singapore's regulatory framework demonstrates a greater alignment with the General Data Protection Regulation, though it exhibits notable differences and limitations. The Personal Data Protection Act (PDPA) incorporates several key features of the GDPR, such as data portability rights and obligations related to data breach notifications. However, the PDPA is less comprehensive overall, lacking many of the detailed provisions present in the GDPR.

Significant differences include the PDPA's limited territorial scope and its less precise definitions of personal data. Under the PDPA, data processors bear fewer responsibilities, and the guidelines governing Data Protection Officers offer more flexibility. Furthermore, the PDPA imposes lower administrative fines compared to those outlined in the GDPR and does not guarantee the independence of supervisory authorities. The enforcement of principles such as *privacy by design* and *by default* is also less stringent. Additionally, the PDPA does not mandate Data Protection Impact Assessments or ensure the right to erasure, and it permits deemed consent under certain conditions.

Thailand, on the other hand, demonstrates a strong alignment with the GDPR. The Personal Data Protection Act (PDPA) incorporates many essential elements of the GDPR, including the rights to data portability and erasure, similar consent management practices, and the appointment of Data Protection Officers with comparable responsibilities. Both frameworks also share analogous territorial scopes that extend beyond national borders, define the responsibilities of data processors in a comparable manner, and mandate data breach notifications.

However, the Thai PDPA lacks certain specific provisions found in the GDPR, such as detailed definitions of personal data and explicit requirements for *privacy by design* and *by default*. Furthermore, the independence of its supervisory authority is not clearly mandated, and there is no requirement for Data Protection Impact Assessments. Additionally, the fines for non-compliance under the Thai PDPA are significantly lower than those established by the GDPR.

The variations in how these elements have been incorporated into the domestic legislation of Laos, Singapore, and Thailand highlight the differing degrees of EU influence across these jurisdictions. These differences in alignment can be attributed to the EU's capacity to project its regulatory framework beyond its borders through mechanisms of External Governance. Although the literature on European External Governance (EEG) often emphasizes the importance of geographical proximity in shaping the reach of EU regulations – with regulatory influence diminishing over greater distances – the cases of Singapore and Thailand demonstrate that other mechanisms play a more decisive role. Despite their geographic remoteness from the EU, both countries have integrated GDPR principles to some extent, suggesting that factors beyond proximity are at play.

Indeed, scholars such as Lavenex (2011, 2014) and Schimmelfennig (2010, 2015) argue that geography alone is insufficient to explain regulatory alignment. This study identifies four primary determinants – competition, learning, emulation, and socialization – that are more relevant in shaping the adoption of GDPR principles within ASEAN, underscoring the EU's broader capacity to influence regulations beyond its immediate vicinity.

The competition mechanism illustrates how the EU's economic influence and regulatory framework pressure other countries to adopt its standards, compelling non-EU entities to comply in order to avoid negative consequences and maintain access to the European market (Lavenex, 2014; Schimmelfennig, 2015, 2010; Bradford, 2012; Rousselin, 2012). In contrast, the learning mechanism is motivated by domestic dissatisfaction, prompting countries to pursue institutional reforms to address particular political or economic challenges. The EU frequently serves as a reference model for these reforms, providing a comprehensive legal framework that is regarded as both adaptable and effective (Schwartz, 2019; Börzel & Risse, 2012; Rousselin, 2012; Schimmelfennig & Sedelmeier, 2004).

Emulation, on the other hand, involves the adoption of EU rules based on their perceived legitimacy, influenced by how well EU norms align with a country's existing beliefs and practices (Lavenex, 2014; Börzel & Risse, 2012; Schimmelfennig, 2010; Lavenex & Schimmelfennig, 2009). Whilst socialization refers to the process by which actors adopt EU rules as a result of the EU's direct efforts to promote its values as legitimate or superior (Lavenex, 2014; Schimmelfennig, 2010; Schimmelfennig & Sedelmeier, 2004).

Furthermore, these concepts differentiate between functionalist logics – encompassing competition and learning – and normative logics – which include emulation and socialization. This distinction allows the study to integrate both rationalist approaches, where actors are viewed as strategic utility-maximizers concerned with their own power and welfare, and constructivist approaches, where actors' decisions are shaped by their internalized identities and perceptions of the identities of others (Schimmelfennig & Sedelmeier, 2004).

The analysis indicates that certain mechanisms of European External Governance exert a greater influence on the incorporation of data protection standards in the selected ASEAN countries than others. Specifically, functional mechanisms – particularly competition and learning – are more impactful than normative mechanisms, such as emulation and socialization. This finding aligns with Lavenex's (2011) research on European External Governance beyond its immediate neighborhood.

Competition emerges as a significant factor in the adoption of EU data protection standards. In Singapore, robust trade relations with the EU, especially in data-driven sectors, have likely compelled local companies to comply with GDPR requirements. Consequently, these companies, aiming to avoid additional compliance costs, have exerted pressure on the Singaporean government to align national regulations with the GDPR. This dynamic exemplifies the *Brussels Effect* as articulated by Bradford (2012). In contrast, Thailand's trade relationship with the EU is less pronounced. Given the prominence of small and medium-sized enterprises in the Thai economy, coupled with limited trade in services with the EU, Thai businesses have not faced significant exposure to GDPR regulations. As a result, there has been little incentive for these businesses to advocate for government alignment with EU

regulations. Instead, the Thai government, motivated by concerns about potential negative impacts on foreign trade, has actively promoted compliance with the GDPR. In this instance, the attractiveness of the EU market still influences the government to endorse responsible data practices. The case of Laos further underscores the relevance of competition in a contrasting manner. Given Laos' limited trade relations with the EU, there is minimal pressure on Lao companies – and by extension, the Lao government – to adopt GDPR-compliant measures. This underscores the broader point that the level of economic integration with the EU directly influences whether or not a country adopts EU standards.

Learning is another crucial mechanism identified in the analysis; however, its relevance varies based on the specific context of each country, particularly in relation to their ties with the EU, their individual motivations, and their prior experiences with data protection laws.

In Laos, for instance, learning significantly influenced the development of its data protection law, but the country drew more from regional influences than directly from EU standards. This orientation stemmed from Laos's closer ties with neighboring countries and a desire to remain aligned with regional developments. Similarly, in Singapore, the learning mechanism is evident as the country has looked to the EU as a model from which to gain insights into addressing data breach issues and enhancing its digital economy. However, having established a data protection law in 2012, Singapore adopted a strategic and tailored approach to integrating new elements, ensuring that its economic development objectives were not compromised by data protection measures that could hinder growth. In Thailand, although the country shares concerns similar to those of Singapore – such as addressing data breaches and promoting a robust digital economy – it initially lacked a data protection law. During the interim period before enacting its own legislation, Thailand heavily relied on the GDPR framework, resulting in an intensive learning phase where the country recognized the GDPR as an international standard. Consequently, the principles of the GDPR played a significant role in shaping Thailand’s legal framework.

Conversely, normative mechanisms – emulation and socialization – appear to exert minimal influence on the incorporation of GDPR principles into the data protection laws of ASEAN countries. This is largely because these nations do not perceive the EU as a normative power and view the EU’s self-image as a normative actor as somewhat arrogant and counterproductive. Additionally, Singapore, Thailand, and Laos each possess unique historical and social contexts that shape their values and conceptions of rights, which differ significantly from Western norms. As a result, these countries do not regard the GDPR as a superior model for human rights protection; any adoption of its elements is motivated by factors other than a commitment to human rights. Furthermore, socialization has had no influence on ASEAN countries' data protection laws because, prior to the establishment of these laws, there was

minimal collaboration between the EU and ASEAN countries on digital development and data protection issues.

Overall, this study concludes that the alignment of ASEAN countries' data protection laws with the GDPR is closely linked to their level of engagement with the EU, underscoring the significant influence of European External Governance on the adoption of GDPR-like standards. Functional mechanisms, particularly competition and learning, have been more influential in driving this alignment than normative mechanisms like emulation and socialization.

This study contributes to the scholarship on EU influence, particularly in the diffusion of European regulatory standards in international data protection governance. What sets this research apart from much of the existing literature is its innovative conceptual approach, using the framework of European External Governance rather than more conventional frameworks, such as Foreign Policy analysis or ontological debates, to examine the EU's influence. Additionally, the study introduced a novel dimension to the operationalization of European External Governance by examining the EU's influence in a geographically distant region, ASEAN, which would traditionally be considered less susceptible to EU regulatory impact. Overall, the findings demonstrate that the EU can exert significant influence in shaping data protection standards even in regions far from its immediate vicinity. However, this influence is not solely contingent on the EU's capacity to project its regulations, but also on the interests, aspirations, and perceptions of the third countries involved.

To advance the findings of this study, future research could examine the remaining ASEAN countries to assess the extent of GDPR influence and determine whether the European External Governance framework applied here is relevant across the broader region. Given the variation in GDPR impact observed among the countries studied, it is likely that similar disparities exist elsewhere in ASEAN, especially since the region lacks a mandatory, uniform data protection framework, allowing each country to adopt its own approach. Furthermore, the diverse social, political, and economic contexts of ASEAN Member States contribute to differing perspectives on personal data protection and GDPR integration.

In light of the fragmented regulatory landscape, it would also be worthwhile to investigate the extent of influence exerted by other major global actors, such as the United States and China, on the data protection policies of ASEAN Member States. A comparative analysis between the influence of the EU and these powers could yield valuable insights into which external actor plays a more prominent role in shaping data protection laws within the region.

Additionally, expanding the scope of inquiry to other regions of the world further illuminate the global reach of the EU's influence on data protection standards and its role in shaping international data governance.

Sources

ASEAN (1967) *The ASEAN Declaration (Bangkok Declaration)*, *ASEAN*. Available at: https://agreement.asean.org/media/download/20140117154159.pdf

ASEAN (1992) *Framework Agreement on Enhancing ASEAN Economic Cooperation*, *ASEAN*. Available at: https://agreement.asean.org/media/download/20140119154919.pdf

ASEAN (1997) *ASEAN Vision 2020*, *ASEAN*. Available at: https://asean.org/asean-vision-2020/

ASEAN (2000) *E-ASEAN Framework Agreement*, *ASEAN*. Available at: https://agreement.asean.org/media/download/20140119121135.pdf

ASEAN (2008) *ASEAN Economic Community Blueprint*, *ASEAN*. Available at: https://www.asean.org/wp-content/uploads/images/archive/5187-10.pdf

ASEAN (2011) *Masterplan on ASEAN Connectivity 2025*, *ASEAN*. Available at: https://asean.org/wp-content/uploads/2021/08/8_compressed.pdf

ASEAN (2015) *ASEAN Economic Community Blueprint 2025*, *ASEAN*. Available at: https://asean.org/book/asean-economic-community-blueprint-2025/

ASEAN (2016) *ASEAN ICT Masterplan 2020*, *ASEAN*. Available at: https://asean.org/book/final-review-of-asean-ict-masterplan-2020/

ASEAN (2017) *ASEAN Work Programme on Electronic Commerce*, *ASEAN*. Available at: https://asean.org/wp-content/uploads/2021/09/ASEAN-Work-Programme-on-Electronic-Commerce_published.pdf

ASEAN-EU (2020) *ASEAN-EU Joint Ministerial Statement on Connectivity*, *ASEAN*. Available at: https://asean.org/wp-content/uploads/ASEAN-EU-Joint-Ministerial-Statement-on-Connectivity-Final1.pdf

ASEAN (2021a) *ASEAN Digital Integration Index Report 2021*, *ASEAN*. Available at: https://asean.org/book/asean-digital-integration-index-report-2021/

ASEAN (2021b) *ASEAN Digital Masterplan 2025*, *ASEAN*. Available at: https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

ASEAN Secretariat (2023) *ASEAN Statistical Yearbook 2023*, *ASEAN Stats*. Available at: https://asean.org/wp-content/uploads/2023/12/ASEAN-Statistical-Yearbook-2023.pdf

ASEAN Secretariat and European Commission (n.d.) *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*, *ASEAN*. Available at: https://asean.org/book/joint-guide-to-asean-model-contractual-clauses-and-eu-standard-contractual-clauses/

ASEAN TELMIN (2016) *Framework on Personal Data Protection*, *ASEAN Main Portal*. Available at: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

ASEAN TELMIN (2018) *Framework on Digital Data Governance* , *ASEAN Main Portal*. Available at: https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf

Asia-Pacific Economic Cooperation (2005) *APEC Privacy Framework*, *Asia-Pacific Economic Cooperation*. Available at: https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1

Bangkok Post (2014) *Prayut pledges support for digital economy*, *Bangkok Post*. Available at: https://www.bangkokpost.com/thailand/general/447185/thailand-still-has-some-way-to-go-before-it-can-benefit-from-a-digital-economy-says-pm-prayut

Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms and Protocol*, *The European Convention on Human Rights*. Available at: http://www.echr.coe.int/documents/d/echr/Archives_1950_Convention_ENG

Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, *Council of Europe*. Available at: https://rm.coe.int/1680078b37

Department of Statistics Singapore (n.d.) *Singapore's International Trade in Services Dashboard*, *Department of Statistics Singapore*. Available at: https://www.singstat.gov.sg/find-data/search-by-theme/trade-and-investment/trade-in-services/visualising-data/singapore-international-trade-in-services-dashboard

Directorate-General for Trade (2024a) *European Union, Trade in goods with Laos*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_laos_en.pdf

Directorate-General for Trade (2024b) *European Union, Trade in goods with Singapore*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_singapore_en.pdf

Directorate-General for Trade (2024c) *European Union, Trade in goods with Vietnam*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_vietnam_en.pdf

Directorate-General for Trade (2024d) *European Union, Trade in goods with Malaysia*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_malaysia_en.pdf

Directorate-General for Trade (2024e) *European Union, Trade in goods with Thailand*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_thailand_en.pdf

Directorate-General for Trade (2024f) *European Union, Trade in goods with Indonesia*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_indonesia_en.pdf

Directorate-General for Trade (2024g) *European Union, Trade in goods with Phillippines*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_philippines_en.pdf

Directorate-General for Trade (2024h) *European Union, Trade in goods with Cambodia*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_cambodia_en.pdf

Directorate-General for Trade (2024i) *European Union, Trade in goods with Myanmar*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_myanmar_en.pdf

Directorate-General for Trade (2024j) *European Union, Trade in goods with Brunei*, *European Commission*. Available at: https://webgate.ec.europa.eu/isdb_results/factsheets/country/details_brunei_en.pdf

EEAS (2022) *Plan of Action to Implement the ASEAN-EU Strategic Partnership (2023-2027)*, *EEAS*. Available at: https://www.eeas.europa.eu/eeas/plan-action-implement-asean-eu-strategic-partnership-2023-2027-0_en

European Commission (2012) *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, *European Commission* . Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

European Commission (2017) *Exchanging and Protecting Personal Data in a Globalised World*, *EUR-Lex*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007

European Commission (2018b) *Connecting Europe and Asia - Building blocks for an EU Strategy*, *EUR-Lex*. Available at:https://www.eeas.europa.eu/sites/default/files/joint_communication_-_connecting_europe_and_asia_-_building_blocks_for_an_eu_strategy_2018-09-19.pdf

European Commission (2020a) *Communication from the Commission to the European Parliament and the Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data*

Protection Regulation, *EUR-Lex*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264

European Commission (2020b) T*eam Europe: Digital4Development Hub launched to help shape a fair digital future across the globe*, *European Commission*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2321

European Commission (2023) *EU-Singapore Digital Partnership*, *Shaping Europe's digital future*. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership

European Commission and Ministry of Trade and Industry Singapore (2019) *European Union-Singapore Trade and Investment Agreements*, *EEAS*. Available at: https://www.eeas.europa.eu/sites/default/files/eu_singapore_trade_and_investment_report_2019.pdf

Freedom House (2016) *Thailand: Freedom in the World 2016 country report*, *Freedom House*. Available at: https://freedomhouse.org/country/thailand/freedom-net/2016

Freedom House (2017a) *Freedom in the World 2017: Laos*, *Freedom House*. Available at: https://freedomhouse.org/country/laos/freedom-world/2017

Freedom House (2017b) *Thailand: Freedom in the World 2017 country report*, *Freedom House*. Available at: https://freedomhouse.org/country/thailand/freedom-world/2017

Freedom House (2018) *Thailand: Freedom in the World 2018 country report*, *Freedom House*. Available at: https://freedomhouse.org/country/thailand/freedom-world/2018

Freedom House (2019) *Thailand: Freedom in the World 2019 country report*, *Freedom House*. Available at: https://freedomhouse.org/country/thailand/freedom-world/2019

Gibbs, S. (2015) *Facebook's privacy policy breaches European law, report finds*, *The Guardian*. Available at: https://www.theguardian.com/technology/2015/feb/23/facebooks-privacy-policy-breaches-european-law-report-finds

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014) Court of Justice of the European Union, Case C-131/12. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Henriquez, M. (2019) *The Top 12 Data Breaches of 2019*, *Security Magazine*. Available at: https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

Herman, S. (2015) *EU to Thailand: Clean Up Fishing Trade in 6 Months*, *Voice of America*. Available at: https://www.voanews.com/a/eu-to-thailand-clean-up-fishing-trade-in-six-months/2728564.html

Hio, L. (2017) *Uber's 2016 data breach affected 380,000 in Singapore, biggest reported breach here*, *The Straits Times*. Available at: https://www.straitstimes.com/singapore/ubers-

2016-data-breach-affected-380000-in-singapore-biggest-reported-breach-here#:~:text=The%20data%20breach%20incident%2C%20which%20occurred%20in%20October%202016%2C%20saw,%2C%20on%20Nov%2021%2C%202017

Kingdom of Thailand (2019) *Personal Data Protection Act*, *Government Gazette*. Available at: https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf

Lao People's Democratic Republic (2017) *Law on Electronic Data Protection (translation)*, *Lao Service Portal*. Available at: http://lsp.moic.gov.la/?r=site%2Fdisplaylegal&id=289

Leesa-nguansuk , S. and Tortermvasana , K. (2018) *Data of TrueMove H users leaked online* , *Bangkok Post*. Available at: https://www.bangkokpost.com/life/tech/1446182/data-of-truemove-h-users-leaked-online

Library of Congress (2014) *Thailand: Draft Laws to Promote Digital Economy*, *Library of Congress*. Available at: https://www.loc.gov/item/global-legal-monitor/2014-12-17/thailand-draft-laws-to-promote-digital-economy/

Limsamarnphun, N. (2021) *Government fast tracks personal data law*, *Nation Thailand*. Available at: https://www.nationthailand.com/in-focus/30345749

Maximillian Schrems v Data Protection Commissioner (2015) Court of Justice of the European Union, Case C-362/14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362

Ministry of Digital Development and Information (2020a) *Public Consultation on the Draft Personal Data Protection (Amendment) Bill*, *Ministry of Digital Development and Information*. Available at: https://www.mddi.gov.sg/media-centre/public-consultation/public-consultation-on-the-personal-data-protection-amendment-bill/

Ministry of Digital Development and Information (2020b) *Closing note to the public consultation on Draft Personal Data Protection (amendment) bill*, *Ministry of Digital Development and Information*. Available at: https://www.mddi.gov.sg/media-centre/public-consultation/closing-note-to-pc-on-draft-pdp-amendment-bill/

Ministry of Planning and Investment (2016) *8th Five-Year National Socio-economic Development Plan (2016–2020)*, *Lao People's Democratic Republic*. Available at: https://laopdr.un.org/sites/default/files/2019-08/2016_8th%20NSEDP_2016-2020_English.pdf

Ministry of Trade and Industry Singapore (2016) *Economic Survey of Singapore 2016*, *MTI*. Available at: https://www.mti.gov.sg/Resources/Economic-Survey-of-Singapore/2016/Economic-Survey-of-Singapore-2016

Ministry of Trade and Industry Singapore (2017) *Economic Survey of Singapore 2017*, *MTI*. Available at: https://www.mti.gov.sg/Resources/Economic-Survey-of-Singapore/2017/Economic-Survey-of-Singapore-2017

Ministry of Trade and Industry Singapore (2018) *Economic Survey of Singapore 2018*, *MTI*. Available at: https://www.mti.gov.sg/Resources/Economic-Survey-of-Singapore/2018/Economic-Survey-of-Singapore-2018

Ministry of Trade and Industry Singapore (2019) *Economic Survey of Singapore 2019*, *MTI*. Available at: https://www.mti.gov.sg/Resources/Economic-Survey-of-Singapore/2019/Economic-Survey-of-Singapore-2019

Ministry of Trade and Industry Singapore (n.d.) *European Union-Singapore Digital Partnership (EUSDP)*, *MTI*. Available at: https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/EUSDP

Mun, T. *et al.* (2019) *The State of Southeast Asia: 2019 Survey Report*, *ISEAS-Yusof Ishak Institute*. Available at: https://www.iseas.edu.sg/centres/asean-studies-centre/state-of-southeast-asia-survey/test-state-of-southeast-asia-survey-01/

Newcomb, A. (2018) *A timeline of Facebook's privacy issues — and its responses*, *NBC News*. Available at: https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

Octalibrayani, I. (2020) *The largest data breach in Singapore to date*, *IPHub Asia*. Available at: https://iphub.asia/largest-data-breach-in-singapore-to-date/

OECD (1980) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *OECD iLibrary*. Available at: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf

Official Journal of the European Communities (1995) *Data Protection Directive*, *Official Journal of the European Communities*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046

Official Journal of the European Communities (2000) *Charter of Fundamental Rights of the European Union*, *European Parliament*. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Official Journal of the European Union (2012) *Consolidated version of the Treaty on the Functioning of the European Union* , *EUR-Lex*. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

Official Journal of the European Union (2016) Regulation (EU) 2016/ 679 of the European Parliament and of the Council (General Data Protection Regulation). EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

PDPC Singapore (2023) *Opening Remarks by Commissioner, Mr Lew Chuen Hong, at International Association of Privacy Professionals (IAPP) Asia Privacy Forum*, *Personal Data Protection Commission Singapore*. Available at: https://www.pdpc.gov.sg/news-and-events/press-room/2023/07/opening-remarks-by-commissioner-mr-lew-chuen-

hong-at-international-association-of-privacy-professionals-asia-privacy-forum-2023-on-19-july-2023

Personal Data Protection Commission (2021) *Guide to Data Protection Impact Assessments*, *Personal Data Protection Commission Singapore*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf

Personal Data Protection Commission (2022a) *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, *Personal Data Protection Commission Singapore*. Available at: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf

Personal Data Protection Commission (2022b) *Guide to Basic Anonymisation*, *Personal Data Protection Commission Singapore*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Guide-to-Basic-Anonymisation-31-March-2022.pdf

Pornwasin, A. (2018) *Govt in race against time to update Data Privacy Law*, *The nation*. Available at: https://www.nationthailand.com/in-focus/30344739

Public Data Security Review Committee (2019) *Public Sector Data Security Review Committee Report*, *Smart Nation*. Available at: https://www.smartnation.gov.sg/files/publications/psdsrc-main-report-nov2019.pdf

Punnakan, P. (2019) *Speech at the seminar 'TDPG 2.0: Building Trust with Data Protection'*, *Ministry of Digital Economy and Society*. Available at: https://www.thairath.co.th/news/local/bangkok/1688510

Refworld (2015) *Freedom in the World 2015 - Thailand*, *UNHCR*. Available at: https://www.refworld.org/reference/annualreport/freehou/2015/en/103762

Republic of Singapore (2020) *Personal Data Protection (Amendment) Act 2020*, *Singapore Statutes Online*. Available at: https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210

Soukthavy and Manythone (2015) *Cyber crime law approved*, *Lao News Agency*. Available at: https://kpl.gov.la/En/Detail.aspx?id=4771

Subhani, O. (2023) *Most European businesses here will welcome EU-Singapore Digital Trade Pact: Survey*, *The Straits Times*. Available at: https://www.straitstimes.com/business/most-european-businesses-here-will-welcome-eu-singapore-digital-trade-pact-survey

Tham, I. (2021) *Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack*, *The Straits Times*. Available at:

https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

The Nation (2014) *Cabinet nod for draft laws on digital economy committee, restructuring of ICT Ministry*, *Nation Thailand*. Available at: https://www.nationthailand.com/in-focus/30249977

The Nation (2018) *Why we need data protection now*, *Nation Thailand*. Available at: https://www.nationthailand.com/perspective/30351346

The Nation (2022) *No more delays on personal data protection law enforcement: PDPC boss*, *Nation Thailand*. Available at: https://www.nationthailand.com/in-focus/40014581

Tortermvasana, K. (2019) *Digital Economy Ministry calls for Data Protection Officers*, *Bangkok Post*. Available at: https://www.bangkokpost.com/business/1693024/digital-economy-ministry-calls-for-data-protection-officers

Trading Economics (n.d.a.) *European Union exports to Thailand*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/thailand

Trading Economics (n.d.b.) *European Union imports fromThailand*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/thailand

Trading Economics (n.d.c.) *Thailand Imports*, *Trading Economics*. Available at: https://tradingeconomics.com/thailand/imports

Trading Economics (n.d.d.) *Thailand Exports*, *Trading Economics*. Available at: https://tradingeconomics.com/thailand/exports

Trading Economics (n.d.e.) *European Union Exports*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports

Trading Economics (n.d.f.) *European Union Imports*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports

Trading Economics (n.d.g.) *European Union imports to Singapore*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/singapore

Trading Economics (n.d.h.) *European Union imports to Vietnam*, *Trading Economics*. Available at:https://tradingeconomics.com/european-union/imports/vietnam

Trading Economics (n.d.i.) *European Union imports to Malaysia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/malaysia

Trading Economics (n.d.j.) *European Union imports to Indonesia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/indonesia

Trading Economics (n.d.k.) *European Union imports to Cambodia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/cambodia

Trading Economics (n.d.l.) *European Union imports to Philippines*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/philippines

Trading Economics (n.d.m.) *European Union imports to Myanmar*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/myanmar

Trading Economics (n.d.n.) *European Union imports to Brunei*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/brunei

Trading Economics (n.d.o.) *European Union imports to Laos*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/imports/laos

Trading Economics (n.d.p.) *European Union exports to Singapore*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/singapore

Trading Economics (n.d.q.) *European Union exports to Vietnam*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/vietnam

Trading Economics (n.d.r.) *European Union exports to Malaysia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/malaysia

Trading Economics (n.d.s.) *European Union exports to Indonesia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/indonesia

Trading Economics (n.d.t.) *European Union exports to Cambodia*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/cambodia

Trading Economics (n.d.u.) *European Union exports to Philippines*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/philippines

Trading Economics (n.d.v.) *European Union exports to Myanmar*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/myanmar

Trading Economics (n.d.w.) *European Union exports to Brunei*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/brunei

Trading Economics (n.d.x.) *European Union exports to Laos*, *Trading Economics*. Available at: https://tradingeconomics.com/european-union/exports/laos

United Nations ESCAP (2018) *Asia-Pacific Trade Briefs: Lao PDR*, UNESCAP. Available at: *https://www.unescap.org/sites/default/files/Lao_PDR_5.pdf*

United Nations General Assembly (1948) *Universal Declaration of Human Rights*, *Office of the United Nations High Commissioner for Human Rights*. Available at: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf

United Nations General Assembly (1971) *General Assembly - Twenty-sixth Session*, *United Nations*. Available at: https://documents.un.org/doc/resolution/gen/nr0/327/98/pdf/nr032798.pdf?token=oNAXOX6V8ZikvKtNlu&fe=true

Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság (2015) Court of Justice of the European Union, Case C-230/14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0230

WITS (n.d.a.) *Lao PDR trade balance, exports and imports by country and region 2017*, World Integrated Trade Solution. Available at: https://wits.worldbank.org/CountryProfile/en/Country/LAO/Year/2017/TradeFlow/EXPIMP

WITS (n.d.b.) *Thailand trade balance, exports and imports 2016*, *WITS*. Available at: https://wits.worldbank.org/CountryProfile/en/Country/THA/Year/2016/TradeFlow/EXPIMP

WITS (n.d.c.) *Thailand trade balance, exports and imports 2017*, *WITS*. Available at: https://wits.worldbank.org/CountryProfile/en/Country/THA/Year/2017/TradeFlow/EXPIMP

WITS (n.d.d.) *Thailand trade balance, exports and imports 2018*, *WITS*. Available at: https://wits.worldbank.org/CountryProfile/en/Country/THA/Year/2018/TradeFlow/EXPIMP

WITS (n.d.e.) *Thailand trade balance, exports and imports 2019*, *WITS*. Available at: https://wits.worldbank.org/CountryProfile/en/Country/THA/Year/2019/TradeFlow/EXPIMP

World Bank Group (2023) *GDP per capita (current US$) - East Asia & Pacific*, *World Bank Group*. Available at: https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=Z4

Xinhua (2018) *Two major Thai banks hacked, personal details from over 120,000 customers stolen*, *China Daily*. Available at: https://www.chinadaily.com.cn/a/201808/02/WS5b62ae2fa3100d951b8c83e9.html

Bibliographical references

Aaronson, A. and Leblond, P. (2018) *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, *Research Gate*. Available at: https://www.researchgate.net/publication/325218175_Another_Digital_Divide_The_Rise_of_Data_Realms_and_its_Implications_for_the_WTO

Albert, E. and Maizland, L. (2019) *What is ASEAN?*, *Mega Lecture*. Available at: https://megalecture.com/wp-content/uploads/2022/09/What-Is-ASEAN_-_-Council-on-Foreign-Relations.pdf

Alfred, D. (2020) *Navigating the Road Ahead: Insights into the Policy Rationale of the PDP (Amendment) Bill 2020*, *DPO connect*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/November-20/Navigating-the-Road-Ahead.html

Allen & Gledhill (2022) *Myanmar Cyber Security bill seeks to regulate online activity and access to information*, *Allen & Gledhill*. Available at: https://www.allenandgledhill.com/mm/publication/articles/21705/cyber-security-bill-seeks-to-regulate-online-activity-and-access-to-information

Amnesty International (2023) *Human rights in Laos*, *Amnesty International*. Available at: https://www.amnesty.org/en/location/asia-and-the-pacific/south-east-asia-and-the-pacific/laos/report-laos/

Angeline, W. (2024) *Safeguarding secrets*, *The Singapore Law Gazette*. Available at: https://lawgazette.com.sg/practice/practice-matters/safeguarding-secrets-data-privacy-pdpa/

Anuroj, B. (n.d.) *Thailand 4.0 – a new value-based economy*, *Thailand Board of Investment*. Available at: https://www.boi.go.th/upload/content/Thailand,%20Taking%20off%20to%20new%20heights%20@%20belgium_5ab4e8042850e.pdf

Ariyapruchya, K. *et al.* (2017) *Thailand Economic Monitor: Digital Transformation*, *World Bank Group*. Available at: https://documents1.worldbank.org/curated/en/437841530850260057/pdf/Thailand-Economic-Monitor-Digital-Transformation.pdf

Armstrong, C. (2022) *Key Methods Used in Qualitative Document Analysis*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3996213

Arner, D. et al. (2021) *The Transnational Data Governance Problem*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3912487

ASEAN (2023) *ASEAN, China reaffirm commitment to advance comprehensive strategic partnership*, *ASEAN*. Available at: https://asean.org/asean-china-reaffirm-commitment-to-advance-comprehensive-strategic-partnership/

ASEAN (n.d.) *Economic Community*, *ASEAN*. Available at: https://asean.org/our-communities/economic-community/

Asia Society Policy Institute (n.d.) *Thailand Data*, *Asia Society Policy Institute*. Available at: https://asiasociety.org/policy-institute/raising-standards-data-ai-southeast-asia/data/thailand

Atlas.ti (n.d.) *Deductive Thematic Analysis*, *ATLAS.ti*. Available at: https://atlasti.com/guides/thematic-analysis/deductive-thematic-analysis

Baek, D. (2024) *A Five-Year Review of Singapore's Cybersecurity Challenges - Major Incidents and Responses*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/five-year-review-singapores-cybersecurity-challenges-baek--usdjc/

Bennett, C. (2018) *The European General Data Protection Regulation: An instrument for the globalization of privacy standards?*, *Information Policy*. Available at: https://content.iospress.com/download/information-polity/ip180002?id=information-polity%2Fip180002

Bennett, C. and Raab, C. (2020) *Revisiting the governance of privacy: Contemporary policy instruments in global perspective*, *The University of Edinburgh*. Available at: https://www.pure.ed.ac.uk/ws/portalfiles/portal/74615489/Raab_RAG_GovernanceOfPrivacy.pdf

Biedermann, R. (2019) *The EU's Connectivity Strategy Towards ASEAN: Is a 'European Way' Feasible?*, *European Foreign Affairs Review*. Available at: https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.4/EERR2019043

Birch, K. (2023) *How Singapore is building a Sustainability Innovation Hub*, *Business Chief Asia*. Available at: https://businesschief.asia/sustainability/how-singapore-is-becoming-a-sustainability-innovation-hub

Birnhack, M. (2008) *The EU Data Protection directive: An Engine of a Global Regime*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268744

Boll, A. (2001) *The Asian values debate and its relevance to international humanitarian law*, *International Review of the Red Cross*. Available at: https://international-review.icrc.org/sites/default/files/S1560775500106170a.pdf

Borner, I. (2023) *Understanding Consumer Data Privacy Laws in the US*, *The Data Privacy Group*. Available at: https://thedataprivacygroup.com/blog/understanding-consumer-data-privacy-laws-in-the-us/

Borovikov, E., Nychay, N. and Miller, J. (2017) *GDPR 101: 5 key changes to Europe's Data Protection Framework*, *Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=da9bbc46-0b7d-4045-b8e0-23c9f255073a

Börzel, T. and Risse, T. (2012) *From Europeanisation to Diffusion: Introduction*, *Research Gate*. Available at: https://www.researchgate.net/publication/233108352_From_Europeanisation_to_Diffusion_Introduction

Bradford, A. (2012) The Brussels effect, Oxford University press. Available at: https://global.oup.com/academic/product/the-brussels-effect-9780190088583

Bretherton, C. & Vogler, J. (2013) *A global actor past its peak?*, *SAGE Journals*. Available at: https://journals.sagepub.com/doi/full/10.1177/0047117813497299

Bukht, R. and Heeks, R. (2018) Digital Economy Policy: The Case Example of Thailand, Development Implications of Digital Economies. Available at: https://diode.network/wp-content/uploads/2018/05/thai-digital-economy-policy-diode-paper1.pdf

Bumpenboon, T. (2020) *Thailand's Personal Data Protection Act: An Understanding from the Perspectives of the European Privacy Law*, *Thammasat Review of Economic and Social Policy*. Available at: https://so04.tci-thaijo.org/index.php/TRESP/article/view/249265

Cariolle, J. (2010) *The Economic Vulnerability Index*, *FERDI*. Available at: https://ferdi.fr/dl/df-cT7xN1CvmPnbwrmfA6gYL7hf/ferdi-i9-the-economic-vulnerability-index.pdf

Carolan, E. (2016) *The continuing problems with online consent under the EU's emerging data protection principles*, *Computer Law & Security Review*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916300322

Carrillo, A. and Jackson, M. (2022) *Follow the leader? A Comparative Law Study of the EU's General Data Protection Regulation's impact in Latin America*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4130437

Chaipipat, S. (2019) *ASEAN governance on data privacy: challenges to regional protection of data privacy and personal data in cyberspace*, *Chulalongkorn University*. Available at: https://digital.car.chula.ac.th/cgi/viewcontent.cgi?article=7945&context=chulaetd

Chandler MHM (2019) *Personal Data Protection Act: A New Era of Privacy Rights in Thailand*. Available at: https://www.chandlermhm.com/content/files/00000238/TN%2014Mar19.pdf

Chawla, S. (2019) *The concept of privacy in Thailand and the European Union: A comparative study of religious-cultural origins and legal developments*, *Faculty of Law Thammasat University*. Available at: http://ethesisarchive.library.tu.ac.th/thesis/2019/TU_2019_6101040209_12955_12929.pdf

Chik, W. (2014) *The Singapore Do Not Call Register and the Text and Fax Exemption Order* , *Singapore Management University*. Available at: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=%2Fcontext%2Fsol_resear

ch%2Farticle%2F3913%2F&path_info=SingaporeDoNotCallRegisterTextFaxExemptionOrder_2014.pdf

Chik, W. and Pang, K. (2014) *The Meaning and Scope of Personal Data under the Singapore Data Protection Act*, *Singapore Management University*. Available at: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3912&context=sol_research

China Briefing (2021) *The PRC Personal Information Protection Law (final): A full translation*, *China Briefing News*. Available at: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

Christiansen, T. et al. (2000) *Fuzzy Politics Around Fuzzy Borders: The European Union's Near Abroad'*, *Academia.edu*. Available at: https://www.academia.edu/341917/Fuzzy_Politics_Around_Fuzzy_Borders_The_European_Unions_Near_Abroad

Christopher & Lee Ong Law Firm (2023) *Personal Data Protection Act 2010 under the New Government: Updates to the Proposed Amendments in 2023*, *Christopher & Lee Ong Law Firm*. Available at: https://www.christopherleeong.com/media/5335/2023-02_personal-data-protection-act-2010-clo.pdf

Cmakalová, K. & Rolenc, J. (2012) *Actorness and legitimacy of the European Union*, *SAGE Journals*. Available at: https://journals.sagepub.com/doi/pdf/10.1177/0010836712443176

Cohen, J. et al. (2023) *Cambodia - Data Protection Overview*, *One Trust - Data Guidance*. Available at: https://www.dataguidance.com/notes/cambodia-data-protection-overview

CookieYes Blog (2024) *Singapore's Personal Data Protection Act (PDPA)*, *CookieYes*. Available at: https://www.cookieyes.com/blog/singapore-pdpa/

Corning, G. (2024) *The diffusion of data privacy laws in Southeast Asia: learning and the extraterritorial reach of the EU's GDPR*, *Taylor & Francis Online*. Available at: https://www.tandfonline.com/doi/full/10.1080/13569775.2024.2310220

Council of the European Union (2022) *EU-ASEAN commemorative summit, 14 December 2022*, *Council of the European Union*. Available at: https://www.consilium.europa.eu/en/meetings/international-summit/2022/12/14/

Council on Foreign Relations (2023) *What is ASEAN?*, *Council on Foreign Relations*. Available at: https://www.cfr.org/backgrounder/what-asean

Creak, S. and Barney, K. (2018) *Conceptualising Party-State Governance and Rule in Laos*, *Taylor & Francis Online*. Available at: https://www.tandfonline.com/doi/full/10.1080/00472336.2018.1494849

Croissant , A. and Lorenz , P. (2018) *Laos: The Transformation of Periphery Socialism* , *Springer International Publishing*. Available at: https://d1wqtxts1xzle7.cloudfront.net/95104956/978-3-319-68182-5_5-

libre.pdf?1669882082=&response-content-disposition=inline%3B+filename%3DLaos_The_Transformation_of_Periphery_Soc.pdf&Expires=1726576642&Signature=GLyXNB3MSMiKDNw~mrMD3dgKBaRzwwJGoVf~7uPxAku4v3xDthtbUQD8Zq9EGg4h~NlSecT4V4~8z-IjtZdmdj9ZhqDC~W1Qx5WGwj9veI3tDMCMfCRs17u0sTY56sjo4DEJ7DwwJFmVOF2ttrWeFP9ej9CuVmC93XTr061qRB3XYw4GLnFumSDe3g8Ni0y7hZAwfvCBalUYJqFkbkPnXTmXMJ1Nrz6nBO9ZMKTYrWvo9XnqvzBqjXnFKzcU8I8zebzcST9nc7ATdOwAO03j2z-37cthfMmB2HVAyUuv4U7K-Ga9JCk54207KVua3lLUbXy3y5~mPOy3QA5-RN8Cog__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Damro, C. (2011) *Market Power Europe*, *European Union Studies Association*. Available at: https://eustudies.org/assets/files/papers/EUSA-11%20Damro%20MPE%20Paper-Submitted.pdf

Damro, C. (2012) *Market Power Europe* , *The University of Edinburgh*. Available at: https://www.research.ed.ac.uk/portal/files/10091990/DAMRO_2012_Market_power_Europe.pdf

Damro, C. (2015) *Market Power Europe: Exploring a dynamic conceptual framework*, *The University of Edinburgh*. Available at: https://www.pure.ed.ac.uk/ws/portalfiles/portal/19507987/Damro_C._2015_._Market_Power_Europe.pdf

Danuvas, S. *et al.* (2018) *E-government 4.0 in Thailand: The role of central agencies*, *IOS Press*. Available at: https://content.iospress.com/articles/information-polity/ip180006

Data Guidance (2017) *Singapore: PDPC releases guides on personal data management*, *Data Guidance*. Available at: https://www.dataguidance.com/news/singapore-pdpc-releases-guides-personal-data-management

Data Protection Excellence Network (2019) *The Data Protection Excellence (DPEX) Centre releases research on the number of organisations breaching Singapore's Personal Data Protection Act*, *Data Protection Excellence (DPEX) Network*. Available at: https://www.dpexnetwork.org/media-releases/the-data-protection-excellence-dpex-centre-releases-research-on-the-number-of-organisations-breaching-singapores-personal-data-protection-act

De Hert, P. and Czerniawski, M. (2016) *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, *Research Gate*. Available at: https://www.researchgate.net/publication/305340840_Expanding_the_European_data_protection_scope_beyond_territory_Article_3_of_the_General_Data_Protection_Regulation_in_its_wider_context

Delaere, V. & Van Schaik, L. (2012) The EU's actorness and effectiveness in International Institutions - EU Representation in the OPCW after Lisbon: Still Waiting for Brussels, JSTOR. Available at: https://www.jstor.org/stable/resrep05441.5

Deloitte (2017) General Data Protection Regulation (GDPR), Deloitte. Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-vision-approach.pdf

Dimitrova, A. and Dragneva, R. (2009) *Constraining external governance: Interdependence with Russia and the CIS as limits to the EU's rule transfer in the Ukraine*, *Research Gate*. Available at: https://www.researchgate.net/publication/38306163_Constraining_external_governance_Interdependence_with_Russia_and_the_CIS_as_limits_to_the_EU's_rule_transfer_in_the_Ukraine

DLA Piper (2024) *Law in Brunei*, *Data Protection Laws of the World*. Available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=BN#:~:text=At%20present%20there%20are%20no,to%20keep%20customer%20information%20confidential

EEAS (2021) *ASEAN and EU work together towards establishing an ASEAN Digital Index*, *EEAS*. Available at: https://www.eeas.europa.eu/eeas/asean-and-eu-work-together-towards-establishing-asean-digital-index_en

Elms, D. (2024) *Study on the potential impacts of a future EU-Singapore Digital Trade Agreement*, *EEAS*. Available at: https://www.eeas.europa.eu/delegations/singapore/study-potential-impacts-future-eu-singapore-digital-trade-agreement_en?s=178

EPSU (2019) *The General Data Protection Regulation (GDPR)*, *European Public Service Union*. Available at: https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf

Ess, C. (2005) *'Lost in translation'?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)*, *SpringerLink*. Available at: https://link.springer.com/article/10.1007/s10676-005-0454-0

EU-ASEAN Business Council (2019) *EU-ASEAN Trade & Investment 2019*, *EU-ASEAN Business Council*. Available at: https://www.eu-asean.eu/wp-content/uploads/2022/02/63371b_79696bd9bb6a4011bcb8e83545a7cae7.pdf

EU-ASEAN Business Council (2020) *Data Governance in ASEAN: From rhetoric to reality*, *EU-ASEAN Business Council*. Available at: https://www.eu-asean.eu/wp-content/uploads/2022/02/DATA-GOVERNANCE-IN-ASEAN-FROM-RHETORIC-TO-REALITY-2020.pdf

European Chamber of Commerce Thailand (2023) *Expectations and Challenges of an EU-Thailand Free Trade Agreement (FTA): Perspectives from European Business in Thailand*, *EABC*. Available at: https://www.eabc-thailand.org/wp-content/uploads/2019/01/EABC-2022-POSITION-PAPER-FINAL.pdf

European Commission (2015) *Questions and Answers - Data protection reform*, *European Commission - Press Corner*. Available at: https://ec.europa.eu/commission/presscorner/detail/et/MEMO_15_6385

European Commission (2018a) *Guide to the EU-Singapore Free Trade Agreement and Investment Protection Agreement*, *Astrid*. Available at: https://www.astrid-online.it/static/upload/eu-s/eu-singapore_fta-ipa_04_2018.pdf

European Commission (n.d.a.) *EU trade relations with Laos*, *Trade*. Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/laos_en#:~:text=Trade%20picture,largest%20trade%20partner%20in%202023

European Commission (n.d.b.) *EU-Singapore Free Trade Agreement*, *European Commission*. Available at: https://trade.ec.europa.eu/access-to-markets/en/content/eu-singapore-free-trade-agreement

European Commission (n.d.c.) *The EU-Singapore Agreements explained*, *Trade*. Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreements/agreements-explained_en

European Data Protection Board (2021) *The EDPB: Guaranteeing the same rights for all*, *One-Stop-Shop Leaflet*. Available at: https://www.edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf

European Data Protection Board (n.d.a.) *Who is data controller and who is data processor?*, *Data Protection Guide for Small Business*. Available at: https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/who-data-controller-and-who-data_en#:~:text=Examples%20of%20data%20processors%3A&text=a%20payroll%20company%20processes%20personal,and%20is%20therefore%20data%20controller

European Data Protection Board (n.d.b.) *Data Controller or Data Processor*, *Data Protection Guide for Small Business*. Available at: https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en#toc-7 European Parliamentary Research Service (n.d.) *EU-Singapore trade in goods and services*, *Epthinktank*. Available at: https://epthinktank.eu/2018/10/10/eu-singapore-trade-and-investment-agreements-close-in-on-conclusion-international-agreements-in-progress/eu-singapore-trade-in-goods-and-services/

European Data Protection Board (n.d.c.) *Legacy: Art. 29 Working Party*, *EDPB*. Available at: https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en

European External Action Service (2024) *EU-ASEAN relations*, *EEAS*. Available at: https://www.eeas.europa.eu/eeas/eu-asean-relations_en#:~:text=On%201%20December%202020%2C%20the,the%20EU%2DASEAN%20Strategic%20Partnership.

European Services Forum (2023) *The importance of Trade in Services in Trade between EU & Singapore*, *European Economic and Social Committee*. Available at: https://www.eesc.europa.eu/sites/default/files/files/pascal_kerneis_importance-of-trade-in-services-between-the-eu-and-singapore.pdf

European Union Delegation to Singapore (2022) *EU-Singapore Trade and Investment 2022*, *EEAS*. Available at: https://www.eeas.europa.eu/sites/default/files/documents/TRADE-EU-SINGAPORE-TRADE-BOOKLET_2022_WEB.pdf

European Union Delegation to Singapore (2023) *EU-Singapore Trade & Investment 2023*, *EEAS*. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-EU-SINGAPORE-TRADE-BOOKLET_2023_230920_WEB.pdf

Ferguson, D. *et al.* (2022) *White Paper: Electronic Data Protection and Personal Data*, *European Chamber of Commerce and Industry in Lao PDR*. Available at: https://eccil.org/publication/white-paper-electronic-data-protection-and-personal-data/

Flers, N. (2010) *EU-ASEAN Relations: The Importance of Values, Norms and Culture* , *EU Centre in Singapore*. Available at: https://aei.pitt.edu/14480/1/EUASEAN-AlecuFlers-8June2010.pdf

Gao, R.Y. (2023) *A battle of the big three? - Competing Conceptualizations of Personal Data Shaping Transnational Data Flows*, *OUP Academic*. Available at: https://doi.org/10.1093/chinesejil/jmad040

GDPR Hub (n.d.) *Article 52 GDPR*, *GDPRhub*. Available at: https://gdprhub.eu/Article_52_GDPR

Gil, G. (2021) *ASEAN and the EU: From Pupil to Strategic Partner?, Academia.edu*. Available at: https://www.academia.edu/46873642/ASEAN_and_the_EU_From_Pupil_to_Strategic_Partner

Gilson, J. (2020) *EU-ASEAN relations in the 2020s: pragmatic inter-regionalism?*, *Springer*. Available at: https://support.springer.com/en/support/solutions/articles/6000081876-link-in-to-content-on-springerlink

Giurgiu, A. and Larsen, T. (2016) *Roles and Powers of National Data Protection Authorities - Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?*, *European Data Protection Law Review*. Available at: https://orbilu.uni.lu/bitstream/10993/29819/1/Roles%20and%20Powers%20of%20National%20Data%20Protection%20Authorities_EDPL%203_2016.pdf

Greenleaf, G. (2007) *Asia-Pacific Developments in Information Privacy Law and its Interpretation*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=952578

Greenleaf, G. (2012) *The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299

Greenleaf, G. (2014) *Asian Data Privacy Laws: Trade & Human Rights Perspectives*. Available at: http://ndl.ethernet.edu.et/bitstream/123456789/5452/1/171.pdf.pdf

Greenleaf, G. (2017) *Countries with Data Privacy laws – by Year 1973-2016* , *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2996139

Greenleaf, G. (2018) *Global Convergence of Data Privacy Standards and Laws*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184548

Greenleaf, G. (2021) *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, *University of New South Wales Law Research Series*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

Greenleaf, G. (2023) *Global Data Privacy Laws 2023: 162 national laws and 20 bills*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146

Greenleaf, G. and Cottier, B. (2018) *Data Privacy Laws and Bills: Growth in Africa, GDPR influence*, *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212713

Greenleaf, G. and Suriyawongkul, A. (2019) *Thailand – Asia's strong new data protection law*, *Privacy Laws & Business*. Available at: https://www.privacylaws.com/media/2994/thailand.pdf

Ha, H. (2021) *The ASEAN-China Comprehensive Strategic Partnership: What's in a Name?*, *ISEA*. Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-157-the-asean-china-comprehensive-strategic-partnership-whats-in-a-name-by-hoang-thi-ha

Haberkorn, T. (2021) *Dictatorship on Trial in Thailand*, *Central European University*. Available at: https://events.ceu.edu/2021-05-05/dictatorship-trial-thailand

Hawcock, N. (2022) *FT-Omdia Digital Economies Index: Tomorrow's Top Tech Growth Markets*, *Financial Times*. Available at: https://www.ft.com/content/eb373c95-eace-4a9c-9b45-9ace63ae12d5

Heiman, M. (2020) *The GDPR and the Consequences of Big Regulation*, *Pepperdine Law Review*. Available at: https://digitalcommons.pepperdine.edu/plr/vol47/iss4/3/

Hill Dickinson Law Firm (2022) *Amendments to Singapore's Personal Data Protection Act*, *Hill Dickinson Law Firm*. Available at: https://www.hilldickinson.com/insights/articles/amendments-singapore%E2%80%99s-personal-data-protection-act

Hoon, C. (2004) *Revisiting the Asian Values Argument used by Asian Political Leaders and its Validity*, *Singapore Management University*. Available at: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=%2Fcontext%2Fsoss_research%2Farticle%2F1832%2F&path_info=Asian_values.pdf

Hopland, C. et al. (2020) *Singapore's Personal Data Protection Act shifts away from a consent-centric framework*, *Future of Privacy Forum*. Available at: https://fpf.org/blog/singapores-personal-data-protection-act-shifts-away-from-a-consent-centric-framework/

Human Rights Watch (2015) *Human rights Watch Concerns on Laos*, *Human Rights Watch*. Available at: https://www.hrw.org/news/2015/11/05/human-rights-watch-concerns-laos

Human Rights Watch (2017) *Laos: No Progress on Rights*, *Human Rights Watch*. Available at: https://www.hrw.org/news/2017/07/17/laos-no-progress-rights

Hussain, S. (2023) *GDPR Certification in Thailand*, *Medium*. Available at: https://medium.com/@syedhussain.veave/gdpr-certification-in-thailand-fa93b787217f

Hustinx, P. (2014) *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, *State Watch*. Available at: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

IMD (2023) *Digital Competitiveness Ranking: Singapore*, *IMD* . Available at: https://worldcompetitiveness.imd.org/countryprofile/SG/digital

IMD (n.d.) *Smart City Observatory: Singapore*, *IMD*. Available at: https://www.imd.org/entity-profile/singapore/

Ing, L. et al. (2023) ASEAN Digital Community 2045, ERIA Discussion Paper Series. Available at: https://www.eria.org/uploads/ASEAN-Digital-Community-2045-DP.pdf

International Federation for Human Rights & Lao Movement for Human Rights (2024) *FIDH*, *Assessment of the Lao PDR's implementation of the UN Human Rights Committee's recommendations on key priority issues*. Available at: https://www.fidh.org/IMG/pdf/fidh-lmhr_lao_pdr_js_upr35_july_2018.pdf

Investopedia (2024) *Gross National Income (GNI) Definition, With Real-World Example*, *Investopedia*. Available at: https://www.investopedia.com/terms/g/gross-national-income-gni.asp

ISEAS–Yusof Ishak Institute (n.d.) *Mission*, *ISEAS-Yusof Ishak Institute*. Available at: https://www.iseas.edu.sg/about-us/mission/

Isono, I. and Prilliadi, H. (2023) *ASEAN's Digital Integration Evolution of Framework Documents*, *Economic Research Institute for ASEAN and East Asia*. Available at: https://www.eria.org/uploads/10-Oct-ASEAN-Digital-Integration-Evolution-of-Framework-Documents.pdf

Javorsek, M. (2016) *Asymmetries in International Merchandise Trade Statistics: A case study of selected countries in Asia-Pacific*, *European Commission*. Available at: https://ec.europa.eu/eurostat/documents/7828051/8076585/Asymmetries__trade_goods.pdf

Jie, A. (2016) *European Union Politics: The Perception of the European Union Among Singapore Policy Elites*, *Academia.edu*. Available at: https://www.academia.edu/29974567/European_Union_Politics_The_Perception_of_the_European_Union_Among_Singapore_Policy_Elites

Jie, W. (2018) *Singapore's Smart Nation Initiative – A Policy and Organisational Perspective*, *Lee Kuan Yew School of Public Policy at the National University of Singapore*. Available at: https://lkyspp.nus.edu.sg/docs/default-source/case-studies/singapores-smart-nation-initiative-final_112018.pdf?sfvrsn=354e720a_2

Jiravuttipong, G. and Trasadikoon, K. (n.d.) *Examining the benefits and challenges of Thailand's latest Data Protection Law*, *Tech For Good Institute*. Available at: https://techforgoodinstitute.org/blog/expert-opinion/examining-the-benefits-and-challenges-of-thailands-latest-data-protection-law/

Kagan, J. (2023) *International Institute for Management Development (IMD): Overview*, *Investopedia*. Available at: https://www.investopedia.com/terms/i/imd.asp

Kaushik, S. (2024) *How the World Integrated Trade Solution (WITS) is helping understand Global Commerce*, *World Bank Blogs*. Available at: https://blogs.worldbank.org/en/opendata/how-world-integrated-trade-solution-wits-helping-understand-global-commerce

Kee, H. (2024) *Exploring the puzzle of trade discrepancies in international trade statistics*, *World Bank Blogs*. Available at: https://blogs.worldbank.org/en/developmenttalk/exploring-puzzle-trade-discrepancies-international-trade-statistics

Kefron (2016) *How will the term "Personal Data" be defined within the GDPR?,* Kefron. Available at: https://kefron.com/2016/11/will-term-personal-data-defined-within-gdpr/

Kitiyadisai, K. (2005) *Privacy Rights and Protection: Foreign Values in Modern Thai Context*, *SpringerLink*. Available at: https://link.springer.com/article/10.1007/s10676-005-0455-z

Koch, R. (n.d.) *What is considered personal data under the EU GDPR?*, *GDPR.EU*. Available at: https://gdpr.eu/eu-gdpr-personal-data/

Korwatanasakul, U. and Paweenawat, S. (2020) *Trade, Global Value Chains, and Small and Medium-sized Enterprises in Thailand: a Firm-level Panel Analysis*, *ADBInstitute*. Available at: https://www.adb.org/sites/default/files/publication/604661/adbi-wp1130.pdf

Kunnamas, N. (2020) *Normative Power Europe, ASEAN and Thailand - International Economics and Economic Policy*, *SpringerLink*. Available at: https://link.springer.com/article/10.1007/s10368-020-00478-y

Lao People's Democratic Republic (n.d.) *Criteria for LDC Graduation*, *Round Table Process*. Available at: https://rtm.org.la/nsedp/criteria-ldc-graduation/

Lavenex, S. (2011) *Concentric circles of flexible 'EUropean' integration: A typology of EU external governance relations*, *SpringerLink*. Available at: https://link.springer.com/article/10.1057/cep.2011.7

Lavenex, S. (2014) *The power of functionalist extension: how EU rules travel*, *Taylor & Francis Online*. Available at: https://www.tandfonline.com/doi/full/10.1080/13501763.2014.910818

Lavenex, S. and Schimmelfennig, F. (2009) EU rules beyond EU borders: theorizing external governance in European politics, *Journal of European Public Policy.* Available at: https://www.researchgate.net/publication/233085492_EU_Rules_Beyond_EU_Borders_Theorizing_External_Governance_in_European_Politics

Le Ton, V. (2023) *Vietnam - Data Protection Overview*, *One Trust - Data Guidance*. Available at: https://www.dataguidance.com/notes/vietnam-data-protection-overview

Lee, J.-O. (2024) *How ASEAN is building trust in its digital economy*, *World Economic Forum*. Available at: https://www.weforum.org/agenda/2024/01/asean-building-trust-digital-economy/#:~:text=If%20planned%20inclusively%2C%20the%20ASEAN,for%20women%2C%20youth%20and%20rural

Lin, J. (2023) *Is ASEAN's Comprehensive Strategic Partnership Becoming A Farce?*, *FULCRUM - Analysis on Southeast Asia*. Available at: https://fulcrum.sg/aseanfocus/is-aseans-comprehensive-strategic-partnership-becoming-a-farce/

Lin, Y. (2024) *More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance*, *Columbia Journal of Transnational Law*. Available at: https://www.jtl.columbia.edu/volume-62/the-role-of-

previous-resolutions-in-the-practice-of-the-security-council-pn55l-5pfcl-4a8y2-chapm-b9krg-z4jbc

Linsi, L. et al. (2023) *The Problem with Trade Measurement in International Relations*, *Oxford Academic*. Available at: https://academic.oup.com/isq/article/67/2/sqad020/7085502

Lobo, M. (2023) *GDPR Data Processing: Processor & Data Protection*, *WSI*. Available at: https://www.wsiworld.com/blog/responsibilities-of-a-controller-processor-and-data-protection-officer-according-to-gdpr

Lui, B. *et al.* (2022) *Singapore Personal Data Protection Act changes have implications for healthcare sector*, *Morgan Lewis Law Firm*. Available at: https://www.morganlewis.com/pubs/2022/08/singapore-personal-data-protection-act-changes-have-implications-for-healthcare-sector

Mahbubani, K. (2008) *Europe is a geopolitical dwarf*, *Financial Times*. Available at: https://www.ft.com/content/6fa5b8b4-2745-11dd-b7cb-000077b07658

Manners, I. (2002) Normative Power Europe: A contradiction in terms?*, Journal of Common Market Studies. Available at: https://www.princeton.edu/~amoravcs/library/mannersnormativepower.pdf

Manners, I. (2009) *The Concept of Normative Power in World Politics*, *DIIS Brief*. Available at: https://pure.diis.dk/ws/files/68745/B09_maj_Concept_Normative_Power_World_Politics.pdf

McDermott, Y. (2017) *Conceptualising the right to data protection in an era of Big Data*, *Sage Journals*. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951716686994

Mukherji, P. *et al.* (2022) *Digital Maturity Assessment – Lao PDR*, *UNDP*. Available at: https://www.undp.org/sites/g/files/zskgke326/files/2022-08/UNDP_LaoPDR_DMA_2022.pdf

Mundin, M.T. (2023) *Philippines - Data Protection Overview*, *One Trust - Data Guidance*. Available at: https://www.dataguidance.com/notes/philippines-data-protection-overview

Muryawan, M. and Paca, M. (2024) *The (essential) role of UN's Comtrade in trade data*, *World Bank Blogs*. Available at: https://blogs.worldbank.org/en/opendata/the--essential--role-of-un-s-comtrade-in-trade-data#:~:text=UN%20Comtrade%20relies%20on%20official,bodies%20to%20collect%20the%20data

MyNZTE (2022) *Singapore's Smart Nation plan: what's in it for your tech business?*, *MyNZTE*. Available at: https://my.nzte.govt.nz/article/how-to-win-business-from-singapores-smart-nation-initiative

Naparat, D. (2020) *Exploring Thailand's PDPA Implementation Approaches and Challenges*, *AIS Electronic Library* . Available at: https://aisel.aisnet.org/acis2020/76/

Nasution, S.H. (2021) *Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025*, *Center for Indonesian Policy Studies (CIPS)*. Available at: https://repository.cips-indonesia.org/publications/353777/improving-data-governance-and-personal-data-protection-through-asean-digital-mas

Nesadurai, H. (2008) *The Association of Southeast Asian Nations (ASEAN)*, *Research Gate*. Available at: https://www.researchgate.net/publication/247516583_The_Association_of_Southeast_Asian_Nations_ASEAN

Nuttin, X. (2017) *The future of EU - ASEAN relations*, *Policy Department, Directorate-General for External Policies*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/578043/EXPO_STU(2017)578043_EN.pdf

Obendiek, A.S. (2021) *What Are We Actually Talking About? Conceptualizing Data as a Governable Object in Overlapping Jurisdictions*, *OUP Academic*. Available at: https://doi.org/10.1093/isq/sqab080

Palmer, M. (2006) *Data is the New Oil*, *ANA Blog*. Available at: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

PDPC Singapore (2019) *Personal Data Protection Digest 2019*, *PDPC Singapore*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/2019-Personal-Data-Protection-Digest.pdf

PDPC Singapore (2020) *Singapore's Review of the PDPA and its Opportunity for Leadership in the Region*, *Personal Data Protection Commission Singapore*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/August-20/Singapores-Review-of-the-PDPA-and-its-Opportunity-for-Leadership-in-the-Region

PDPC Singapore (2022) *Guide to Basic Anonymisation Now Available*, *Personal Data Protection Commission*. Available at: https://www.pdpc.gov.sg/news-and-events/announcements/2022/03/guide-to-basic-anonymisation-now-available

PDPC Singapore (n.d.a.) *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, *Personal Data Protection Commission*. Available at: https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

PDPC Singapore (n.d.b.) *Basic Anonymisation*, *Personal Data Protection Commission*. Available at: https://www.pdpc.gov.sg/help-and-resources/2018/01/basic-anonymisation

PDPC Singapore (n.d.c.) *Collection, Use and Disclosure of Personal Data - Notification, Consent and Purpose*, *PDPC Singapore*. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/obligations_edm_01.pdf

PDPC Singapore (n.d.d.) *Guide to Data Protection Impact Assessments*, *Personal Data Protection Commission*. Available at: https://www.pdpc.gov.sg/help-and-resources/2017/11/guide-to-data-protection-impact-assessments

Petrov, R. (2006) *The Dynamic Nature of the Acquis Communautaire in European Union External Relations*, *European University Institute*. Available at: https://cadmus.eui.eu/handle/1814/8252.

Pew Research Center (2014) *Global Religious Diversity*, Pew Research Center. Available at: https://www.pewresearch.org/religion/2014/04/04/global-religious-diversity/

Pew Research Center (2023) *Buddhism, Islam and Religious Pluralism in South and Southeast Asia*, *Pew Research Center*. Available at: https://www.pewresearch.org/religion/2023/09/12/religious-landscape-and-change/

Phillips, M. (2018) *International data-sharing norms: From the OECD to the General Data Protection Regulation (GDPR)*, *SpringerLink*. Available at: https://link.springer.com/article/10.1007/s00439-018-1919-7

Ping, J.C.Y. (2023) *Malaysia - Data Protection Overview*, *One Trust - Data Guidance*. Available at: https://www.dataguidance.com/notes/malaysia-data-protection-overview

Portela, C. (2010) *The perception of the EU in Southeast Asia*, *Academia.edu*. Available at: https://www.academia.edu/5417309/The_Perception_of_the_EU_in_Southeast_Asia?rhid=29697960475&swp=rr-rw-wc-29974567

Portela, C. (2013) *ASEAN: Integration, Internal Dynamics and External Relations* , *Singapore Management University*. Available at: https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=2946&context=soss_research

Positive Technologies (2023) *Cybersecurity Threatscape of Asia: 2022–2023*, *Positive Technologies*. Available at: https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

Postigo, A. (2023) *Governing the Digital Economy in Thailand: Domestic Regulations and International Agreements*, *ISEAS*--Yusof Ishak Institute. Available at: https://www.iseas.edu.sg/wp-content/uploads/2023/06/ISEAS_Perspective_2023_58.pdf

Proudfoot, K. (2023) Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research, Sage Journals. Available at: https://journals.sagepub.com/doi/pdf/10.1177/15586898221126816

Purtova, N. (2018) *The law of everything. Broad concept of personal data and future of EU data protection law*, *Taylor & Francis Online*. Available at: https://www.tandfonline.com/doi/epdf/10.1080/17579961.2018.1452176?needAccess=true

Radaelli, C. (2004) *Europeanisation: Solution or problem?*, *Research Gate*. Available at: https://www.researchgate.net/publication/5015009_Europeanisation_Solution_or_Problem

Rajah & Tann Law Firm (2021) *Amendments to the Personal Data Protection Act to Take Effect in Phases Starting from 1 February 2021*, *Rajah & Tann Asia*. Available at: https://eoasis.rajahtann.com/eoasis/lu/pdf/2021-02_Amendments-PDPA-Take-Effect-in-Phases.pdf

Ramasoota, P. and Panichpapiboon, S. (2014) *Online Privacy in Thailand: Public and Strategic Awareness*, *Journal of Law, Information and Science*. Available at: https://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/JlLawInfoSci/2014/5.html#fn22

Robinson, N. *et al.* (2009) *Review of the European Data Protection Directive*, *RAND Europe*. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

Rojanaphruk, P. (2019) *Thailand's democratic dictatorship*, *Deutsche Welle*. Available at: https://www.dw.com/en/opinion-thailands-democratic-dictatorship/a-49082008

Ross, C. (2022) *Privacy in Asia-Pacific: Shifting perspectives and changing expectations*, *Economist Impact*. Available at: https://impact.economist.com/perspectives/technology-innovation/privacy-asia-pacific-shifting-perspectives-and-changing-expectations

Rousselin, M. (2012) *But Why Would They Do That? European External Governance and the Domestic Preferences of Rule Importers.*, *Research Gate*. Available at: https://www.researchgate.net/publication/281674248_But_why_would_they_do_that_European_external_governance_and_the_domestic_preferences_of_rule_importers

Rustad, M. and Koenig, T. (2019) *Towards a Global Data Privacy Standard* , *Florida Law Review*. Available at: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1446&context=flr

Santaniello, D. (2021) *Laos Personal Data - Data Privacy*, *Tilleke & Gibbins*. Available at: https://www.youtube.com/watch?v=V6WuS5NNegw&list=UURQKPcy9kYGdYqFVkqzSqVA&t=4s&ab_channel=Tilleke%26Gibbins

Schimmelfennig, F. (2010) *Europeanization beyond the member states: How does the EU export its governance model (effectively)?*, *Research Gate*. Available at: https://www.researchgate.net/profile/Frank-

Schimmelfennig/publication/305031798_Europeanisation_Beyond_the_Member_States/links/5ff824ada6fdccdcb83b74d0/Europeanisation-Beyond-the-Member-States.pdf

Schimmelfennig, F. (2015) *Europeanization Beyond Europe*, *Living Reviews in European Governance*. Available at: https://www.research-collection.ethz.ch/handle/20.500.11850/107421

Schimmelfennig, F. and Sedelmeier, U. (2004) *Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe*, *Journal of European Public Policy*. Available at: https://cadmus.eui.eu/bitstream/handle/1814/71646/Schimmelfennig2004Sedelmeier_GovernanceAcceptVersion.pdf;jsessionid=E23F382F00F653AE479614E9B713016A?sequence=1

Schwartz, P. (2019) *Global Data Privacy: The EU Way*, *NYU Law Review*. Available at: https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf

Secure Privacy (2024) *What Is a Data Protection Officer and Do You Need One?*, *Data Protection*. Available at: https://secureprivacy.ai/blog/data-protection-officer-guide#:~:text=Under%20the%20GDPR%2C%20organizations%20are,individuals%20on%20a%20large%20scale

SeeUnity (2017) The main differences between the DPD and the GDPR and how to address those moving forward, British Legal Technology Forum. Available at: https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf

Setiawati, D. et al. (2019) *Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore*, *Academia.edu*. Available at: https://www.academia.edu/92480922/Optimizing_Personal_Data_Protection_in_Indonesia_Lesson_Learned_from_China_South_Korea_and_Singapore

Sharma, S. (2019) *Data privacy and GDPR handbook*, *Google Books*. Available at: https://books.google.pt/books?hl=pt-PT&lr=&id=Db64DwAAQBAJ&oi=fnd&pg=PA1&dq=data+GDPR&ots=bTBr57rxxv&sig=7_hiw5rpp8VyTKwxc0QmxvOSymw&redir_esc=y#v=onepage&q=data%20GDPR&f=true

Smart Nation Singapore (n.d.a.) *Achievements*, *Smart Nation Singapore*. Available at: https://www.smartnation.gov.sg/about-smart-nation/our-journey/achievements/

Smart Nation Singapore (n.d.b.) *Milestones*, *Smart Nation Singapore*. Available at: https://www.smartnation.gov.sg/about-smart-nation/our-journey/milestones/

Sombatpoonsiri, J. (2018) *Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines*, *GIGA*. Available at: https://www.giga-hamburg.de/en/publications/giga-focus/manipulating-civic-space-cyber-trolling-in-thailand-and-the-philippines

Sponselee, A. and Mhungu, R. (n.d.) *GDPR Top Ten - One Stop Shop*, *Deloitte*. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html

Supernap Thailand (2018) *SUPERNAP Thailand and Affiliate Partners Aim For Data Security in digital transformation economy*, *Supernap Thailand*. Available at: https://www.supernap.co.th/supernap-thailand-and-affiliate-partners-aim-for-data-security-in-digital-transformation-economy/

Synopsys (2018) The Data Protection Directive versus the GDPR: Understanding key changes. Available at: https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes.html

Tan, S. and Azman, N. (2019) *The EU GDPR's impact on ASEAN Data Protection Law*, *Financier Worldwide*. Available at: https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law

Termly's Legal Experts (n.d.) *Natural person*, *Termly*. Available at: https://termly.io/legal-dictionary/natural-person/#:~:text=A%20natural%20person%20(also%20sometimes,an%20individual%20or%20a%20company.

Thailand Arbitration Center (n.d.) *Civil case in Thailand: An overview of definition, types, and proceedings*, *Thailand Arbitration Center (THAC)*. Available at: https://thac.or.th/get-to-know-civil-case/#:~:text=Also%20known%20as%20%E2%80%9Cwrongful%20acts,compensation%20for%20the%20injured%20party.

The Conversation (n.d.) *International Institute for Management Development (IMD)*, *The Conversation*. Available at: https://theconversation.com/institutions/international-institute-for-management-development-imd-3333

The White House (2023) *Fact sheet: U.S.-ASEAN Comprehensive Strategic Partnership, One Year On*, *The White House*. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/05/fact-sheet-u-s-asean-comprehensive-strategic-partnership-one-year-on/

Thipphavong, V. *et al.* (2022) *The Export Potential of Laos agri-food to the EU market*, *Michigan State University*. Available at: https://www.canr.msu.edu/resources/the-export-potential-of-laos-agri-food-to-the-eu-market

Tobing, D. (2022) *Preparing Southeast Asia's youth to enter the Digital Economy*, *Asian Development Bank*. Available at: https://blogs.adb.org/blog/preparing-southeast-asia-s-youth-enter-digital-economy

Tonra, B. (2015) *Europeanization*, *University College Dublin Research Repository*. Available at: https://researchrepository.ucd.ie/handle/10197/7303

Tortermvasana, K. (2020) *Most parts of PDPA to be deferred by a year*, *Bangkok Post* Available at: https://www.bangkokpost.com/business/1920972/most-parts-of-pdpa-to-be-deferred-by-a-year

UN COMTRADE (no date) *UN Comtrade Analytics (About)*, *United Nations*. Available at: https://comtrade.un.org/labs/data-explorer/#:~:text=The%20data%20are%20estimated%20either,(so%20called%20mirror%20data)

UNCTAD (2018) *Rapid eTrade Readiness Assessment* , *UNCTAD*. Available at: https://unctad.org/system/files/official-document/dtlstict2018d3_en.pdf

UNDESA (n.d.a.) *LDC Identification Criteria & Indicators*, *United Nations*. Available at: https://www.un.org/development/desa/dpad/least-developed-country-category/ldc-criteria.html

UNDESA (n.d.b) *EVI Indicators*, *United Nations*. Available at: https://www.un.org/development/desa/dpad/least-developed-country-category/evi-indicators-ldc.html

UNESCO (n.d.) *Least Developed Countries (LDCs)*, *UNESCO*. Available at: https://www.unesco.org/en/ldcs#:~:text=Least%20Developed%20Countries%20(LDCs)%20are,of%20which%20are%20in%20Africa.

Vogel, D. (1997) *Trading up and governing across: transnational governance and environmental protection*, *Research Gate*. Available at: https://www.researchgate.net/publication/228913447_Trading_Up_and_Governing_Across_Transnational_Governance_and_Environmental_Protection

Walters, R. et al. (2019) *Data Protection Law - A Comparative Analysis of Asia-Pacific and European Approaches*, *Springer*. Available at: https://unidel.edu.ng/focelibrary/books/Data%20Protection%20Law%20A%20Comparative%20Analysis%20Of%20Asia-Pacific%20And%20European%20Approaches%20by%20Robert%20Walters,%20Leon%20Trakman,%20Bruno%20Zeller%20(z-lib.org).pdf

Warren, S. and Brandeis, L. (1890) *The Right to Privacy*, *Warren and Brandeis, 'The Right to Privacy'*. Available at: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Willis, M. (2023) *IBI supports a modern, flexible framework for electronic transactions in Laos*, *IBI*. Available at: https://www.ibi-usa.com/single-post/ibi-supports-a-modern-flexible-framework-for-electronic-transactions-in-

WITS (2010) *Imports, Exports and Mirror Data with UN COMTRADE*, *WITS*. Available at: https://wits.worldbank.org/wits/wits/witshelp/content/data_retrieval/T/Intro/B2.Imports_Exports_and_Mirror.htm

Wolford, B. (n.d.) *What is GDPR, the EU's new Data Protection Law?*, *GDPR.EU*. Available at: https://gdpr.eu/what-is-gdpr/

Wong, R. (2012a) *Still in Deficit: Perceptions of the EU's Capabilities among Foreign Policy Elites in Singapore, Indonesia and Vietnam*, *Academia.edu*. Available at: https://www.academia.edu/1770673/R_Wong_2012_Still_in_Deficit_Perceptions_of_the_EU_s_Capabilities_among_Foreign_Policy_Elites_in_Singapore_Indonesia_and_Vietnam_EU_External_Affairs_Review_vol_2_pp_34_45

Wong, R. (2012b) *Model power or reference point? The EU and the ASEAN Charter*, *Taylor & Francis Online*. Available at: https://www.tandfonline.com/doi/pdf/10.1080/09557571.2012.678302?casa_token=8iaCQ4LbBc0AAAAA:LnggFeUeGwy5nA7115el255QXu7RIRiDub9WKXxSkMuH_xeEU0ANs9sF0DoXA7JAQGyX6n5_IbNX9g

World Bank (2022) *Positioning the Lao PDR for a Digital Future*, *World Bank*. Available at: https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

World Economic Forum (2011) *Personal Data: The Emergence of a New Asset Class*. Available at: https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

World Economic Forum (2023) *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows*, *World Economic Forum*. Available at: https://www3.weforum.org/docs/WEF_From_Fragmentation_to_Coordination_2023.pdf.

WP29 (2009) *The Future of Privacy*, *European Commission*. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

WP29 (2017) *Guidelines on Data Protection Officers ('DPOs')*, *European Commission*. Available at: https://ec.europa.eu/newsroom/article29/items/612048

Yuriutomo, I. (2023) *Indonesia - Data Protection Overview*, *One Trust - Data Guidance*. Available at: https://www.dataguidance.com/notes/indonesia-data-protection-overview

Annexes

Annex A – Personal Data

Table 2 - Personal Data in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 4(1)) The GDPR defines **personal data** as: "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"	(Art. 3(12)) Laos' LEDP defines **personal data** as: "electronic data of individual, legal entities or organizations"	(Sec. 2(1)) Singapore's PDPA defines **personal data** as: "data, whether true or not, about an individual who can be identified — (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access"	(Sec. 6) Thailand's PDPA defines **personal data** as "any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular"
(Art. 9) The GDPR identifies certain categories of personal data that require special protection (**sensitive data**)	(Arts. 8-10, 33(3)) Laos' LEDP differentiates between: • **general data -** "data of individual, legal	Singapore's PDPA **does not distinguish or define special categories** of personal data	Thailand's PDPA **does not define special categories of data.** Still, it prohibits the collection of specific

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."	entities or organizations which able to access, use and disclose, and must indicate sources of data correctly" • **specific data -** "data that not allow individual, legal entities or organizations to access, use or disclose without permission from the owner or relevant organizations." • "**prohibited data** - "Data administration authority are prohibited to act as follow: (3) Collecting, using, disclosing electronic data that relating to race, ethnic, political attitude, religion belief, sexual behavior, criminal record, health or other data that effect on the stability of the nation, peace and orderliness of the society"		data without explicit consent (with exceptions) (Sec. 26) "Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject"

(Art. 4(5)) The GDPR defines **pseudonymisation** as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"	The Laos LEDP makes **no reference to pseudonymization of data**	Singapore's PDPA makes **no reference to pseudonymization of data**	Thailand's PDPA makes **no reference to pseudonymization of data**

Annex B – Right to Data Portability

Table 3 - Right to Data Portability in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 20) "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a	The Laos' LEDP does not provide data subjects the right to data portability	(Part of the Amendment) (Sec. 26H) "1. An individual may give a porting organisation a request (called a data porting request)	(Sec. 31) "The data subject shall have the right to receive the Personal Data concerning him or her from the Data Controller. The Data Controller shall

structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her **right to data portability** pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible”		that the porting organisation transmits to a receiving organisation the applicable data about the individual specified in the data porting request. 2. Subject to subsections (3), (5) and (6), the porting organisation must, upon receiving the data porting request, transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any prescribed requirements.” (Sec. 26F) “2. This Part [the right to data portability] applies only to applicable data that — (a) is in electronic form on the date the porting organisation receives a data porting request relating to the applicable data”	arrange such Personal Data to be in the format which is readable or commonly used by ways of automatic tools or equipment, and can be used or disclosed by automated means. The data subject is also entitled to: (1) request the Data Controller to send or transfer the Personal Data in such formats to other Data Controllers if it can be done by the automatic means; (2) request to directly obtain the Personal Data in such formats that the Data Controller sends or transfers to other Data Controllers, unless it is impossible to do so because of the technical circumstances.”

Annex C – Right to Erasure (*right to be forgotten*)

Table 4 - Right to Erasure (right to be forgotten) in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 17) 1. The data subject shall have **the right to** obtain from the controller the **erasure** of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are **no longer necessary** in relation to the purposes for which they were collected or otherwise processed; (b) the data subject **withdraws consent** on which the processing is based according to point (a) of Article 6(1),	(Art. 20) "Data administration authority **must delete electronic data** that they collected **as proposed by the data owner** or when using purpose is terminated, the collection is expired or as specify in the Article 29 section 3 of this law. Deleting of electronic data must inform the data owner, except the law is specified in others." (Art. 27(2)) "Data owners have the following rights: (2) Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, **delete** his or her data"	The PDPA does not afford data subjects the right to have their data erased	(Sec. 33) "The data subject shall have the right to request the Data Controller to erase or destroy the Personal Data, or anonymize the Personal Data to become the anonymous data which can not identify the data subject, where the following ground applies: (1) the Personal Data is **no longer necessary** in relation to the purposes for which it was collected, used or disclosed; (2) the data subject **withdraws consent** on which the collection, use, or disclosure is based on, and where

or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject **objects to the processing** pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been **unlawfully processed**; (e) the personal data have to be erased for **compliance with a legal obligation** in Union or Member State law to which the controller is subject; (f) the personal			the Data Controller has no legal ground for such collection, use, or disclosure; (3) the data subject **objects to the collection, use, or disclosure** of the Personal Data referred in Section 32(1), and the Data Controller can not reject to such request as referred in Section 32(1) (a) or (b), or where the data subject exercise his or her right to object as referred in Section 32(2); or (4) the Personal Data have been **unlawfully collected, used, or disclosed** under this Chapter.”

data have been **collected in relation to the offer of information society services** referred to in Article 8(1). “			

Annex D – Consent

Table 5 – Consent in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU’s General Data Protection Regulation (GDPR)	Laos’ Law on Electronic Data Protection (LEDP)	Singapore’s Personal Data Protection Act (Singapore’s PDPA)	Thailand’s Personal Data Protection Act (Thailand’s PDPA)
(Art. 4(11)) The GDPR defines **consent of the data subject** as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”	The Laos LEDP does not make explicit reference to consent, however, there are several implicit references: (Art. 12) “The collection of data **must be approved by data owner**(...)” (Art. 15) “Data administration authority is able to handover electronic data to other authorities and **shall be agreed from the data owner**.” (Art. 16)	(Sec. 13) “An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless — (a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure (as the case	(Sec. 19) “The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do so by the provisions of this Act or any other laws. A request for consent shall be **explicitly** made in a written statement, or via electronic means, unless it cannot be done by its nature. In requesting consent from the data subject, the Personal Data

	"Data administration authority can use or disclose personal data that they collected, maintained or administrated when have been **approved by data owner**(...)" (Art. 17) "Sending or transferring of electronic data shall comply as following: (1) Have **permission from the data owner**(...)" The Laos LEDP **does not mention any consent requirements**.	may be) without the individual's consent is required or authorised under this Act or any other written law" (Sec. 14) "1 An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless — (a) **the individual has been provided with the information required** under section 20; and (b) the individual provided his or her consent for that purpose in accordance with this Act. 2. An organisation must not — (a) as a condition of providing a product or service,	Controller shall also **inform the purpose of the collection, use, or disclosure** of the Personal Data. (...) In requesting consent from the data subject, the Data Controller shall utmost take into account that the data subject's consent is **freely given**."

		require an individual to consent to the collection, use or disclosure of personal data about the individual **beyond what is reasonable** to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by **providing false or misleading information** with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices." (Sec. 15) 1.An individual is **deemed to consent** to the collection, use	

		or disclosure of personal data about the individual by an organisation for a purpose if — (a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. 2. If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.”	

(Art. 7(3)) "The data subject shall have the right to **withdraw** his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. "	The Laos LEDP **does not make reference to the right to withdraw consent**	(Sec. 16) "On giving reasonable notice to the organisation, an individual may at any time **withdraw any consent given**, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose."	(Sec. 16) "The data subject **may withdraw his or her consent at any time**. The withdrawal of consent shall be as easy as to giving consent, unless there is a restriction of the withdrawal of consent by law, or the contract which gives benefits to the data subject. However, the withdrawal of consent shall not affect the collection, use, or disclosure of personal data that the data subject has already given consent legally under this Chapter."

Annex E – Territorial Scope

Table 6 - Territorial Scope in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 3) "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of	(Art. 6) "[Laos' LEDP] is applicable to domestic and international individuals, legal entities or organizations that located or activated within the territory of the Lao PDR"	(Sec. 4(1)) "1. Parts 3, 4, 5, 6, 6A and 6B do not impose any obligation on — (a) any individual acting in a personal or domestic capacity;	(Sec. 5) "This Act applies to the collection, use or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand, regardless of whether such collection, use or

whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue		(b) any employee acting in the course of his or her employment with an organisation; (c) any public agency; or (d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision." (Sec. 2(1)) ""organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not — (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore;"	disclosure takes place in the Kingdom of Thailand or not. In the event that a Data Controller or a Data Processor is outside the Kingdom of Thailand, this Act shall apply to the collection, use or disclosure of Personal Data of data subjects who are in the Kingdom of Thailand, where the activities of such Data Controller or Data Processor are the following activities: (1) the offering of goods or services to the data subjects who are in the Kingdom of Thailand, irrespective of whether the payment is made by the data subject; or (2) the monitoring of the data subject's behavior, where the behavior takes place in the Kingdom of Thailand."

of public international law."			

Annex F – Data Processor

Table 7 - Data Processor in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 4(8)) The GDPR defines **processor** as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"	(Art. 3 (14)) Laos' LEDP does not clearly define or recognize the role of a data processor. Instead, the regulation designates the **Electronic Data Administration Authority (EDAA)** which means "individual, legal entities or organizations that responsible for administrating the electronic data which mainly are Ministries, Data Center through internet, telecommunication service providers, banks;"	 Singapore's PDPA does not use the term 'data processor'; instead, it employs the more general term '**data intermediary**' (Sec. 2(1)) ""data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;"	(Sec. 6) Thai's PDPA defines **data processor** as "a person or a juristic person who operates in relation to the collection, use or disclosure of the personal data pursuant to the orders given by or on behalf of a data controller."
(Art. 28(1)(3)) "1. Where processing is to be carried out on behalf of a controller, the controller shall use **only processors providing sufficient**	 The Laos LEDP does not differentiate between entities such as controllers and processors.	(Sec. 4(2)(3)) "2. Parts 3, 4, 5, 6 (except sections 24 and 25), 6A (except sections 26C(3)(a) and 26E) and 6B do not impose any obligation on a data	(Sec. 37(2)) "The Data Controller shall have the following duties: (...) 2. in the circumstance where the Personal Data is

guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." "3. Processing by a processor shall be governed by a **contract** or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"		intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. 3. An organisation has the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself."	to be provided to other Persons or legal persons, apart from the Data Controller, the Data Controller shall take action to prevent such person from using or disclosing such Personal Data unlawfully or without authorization;"
(Art. 30(2)) "Each processor and, where applicable, the processor's representative shall **maintain a record** of all categories of **processing**	(Art. 15) "Data administration authority can maintain electronic data when necessary from the collection purpose and other purposes. (...)	Singapore's PDPA does not explicitly mandate data intermediaries to maintain records of their processing activities.	(Sec. 40(3)) "The Personal Data Processor shall have the following duties: (...) 3. prepare and maintain records of personal data processing activities

activities carried out on behalf of a controller”	Data administration authority **must create a list of electronic data maintenance** which can be easily check and the maintenance measures and methods must be safe. (...)”		in accordance with the rules and methods set forth by the Committee. (...) The provisions in (3) may not apply to the Data Processor who is a small organization pursuant to the rules as prescribed by the Committee, unless the collection, use, or disclosure of such Personal Data is likely to result in a risk to the rights and freedoms of data subjects, or not a business where the collection, use, or disclosure of the Personal Data is occasional, or involving in the collection, use, or disclosure of the Personal Data pursuant to Section 26”
(Art. 31) “The controller and the processor and, where applicable, their representatives, shall **cooperate**, on request, **with the supervisory authority** in the performance of its tasks.”	The Laos LEDP **mentions the cooperation between the EDAA and a supervisory authority** (which in the case of the Laos Law is most similar to the Administration Organization of Electronic Data Protection) (Art. 30(8))	Singapore’s PDPA mentions the cooperation between the Commission and other organizations, but not specifically with data intermediaries	Thailand’s PDPA makes no explicit reference to cooperation between data processors and supervisory authority

	"Data administration authority has the following obligations: (8) **Coordinate** with Posts and Telecommunication Sectors regarding to secure form attacking data"		
(Arts. 33(2)) "The processor shall **notify** the controller without undue delay after becoming aware of a personal **data breach**"	(Art. 26) "Responding to data attacks shall comply as following: (1) Data administration authority uses interception and fixed methods when have been informed by individual, legal entities or organizations that relating to sending of data that cause or may cause unpeaceful of the society;" (Art. 27(3)) "Data owners have the following rights: (3) Inform data administratio	(Sec. 26(C)) "(3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation — (a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data	(Sec. 40(2)) "The Personal Data Processor shall have the following duties: (...) 2. provide appropriate security measures for preventing unauthorized or illegal loss, access to, use, alteration, correction or disclosure, of Personal Data, and notify the Data Controller of the Personal Data breach that occurred;"

	n authority and other relevant sectors to secure his or her electronic data when the data have been damaged or in risk;" (Art. 28(3)(4)) "Data owners have the following obligations: (3) Report the abnormal of electronic data to the data administratio n authority; (4) Report the illegal activation that relating to electronic data to the relevant organizations ;"	intermediary, conduct an assessment of whether the data breach is a notifiable data breach." (Sec. 26E) "Where an organisation — (a) is a data intermediary processing personal data on behalf of and for the purposes of a public agency; and (b) has reason to believe that a data breach has occurred in relation to that personal data, the organisation must, without undue delay, notify the public agency of the occurrence of the data breach."	
(Art. 37) "1. The controller and the processor shall **designate a data protection officer** in any case where:	The Laos LEDP mentions the necessity of appointing a data protection officer only once. However,	Singapore's PDPA does not explicitly mandate data intermediaries to appoint one or more individuals	(Sec. 41) "The Data Controller and the Data Processor shall designate a data protection officer in the following

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal	it does not specify who is responsible for this designation.	responsible for ensuring compliance with the Act	circumstances: (1) the Data Controller or the Data Processor is a public authority as prescribed and announced by the Committee; (2) the activities of the Data Controller or the Data Processor in the collection, use, or disclosure of the Personal Data require a regular monitoring of the Personal Data or the system, by the reason of having a large number of Personal Data as prescribed and announced by the Committee; or (3) the core activity of the Data Controller or the Data Processor is the collection, use or

convictions and offences referred to in Article 10”			disclosure of the Personal Data according to Section 26.”

Annex G – *Privacy by design* and *Privacy by default*

Table 8 - Privacy by design and Privacy by default in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU’s General Data Protection Regulation (GDPR)	Laos’ Law on Electronic Data Protection (LEDP)	Singapore’s Personal Data Protection Act (Singapore’s PDPA)	Thailand’s Personal Data Protection Act (Thailand’s PDPA)
(Art. 25) “1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are **designed to implement data-protection**	The Laos LEDP does not make an explicit reference to “privacy by design” and “privacy by default”	Singapore’s PDPA does not make an explicit reference to “privacy by design” and “privacy by default”	Thailand’s PDPA does not make an explicit reference to “privacy by design” and “privacy by default”

principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."			
(Rec.78) "(...) In order to be able to demonstrate	However, the LEDP defines provisions	However, Singapore's PDPA	However, Thailand's PDPA defines

compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of **minimising** the processing of personal data, **pseudonymising** personal data as soon as possible, **transparency** with regard to the functions and processing of personal data, **enabling the data subject to monitor the data processing**, enabling the **controller to create and improve security features**."	that support the concepts of privacy by design and by default, such as: (Art. 5) "Electronic Data Protection shall base on the following principles: (3) **Keep the data** of the state, individual, legal entities or organizations in confidential and **security**; (4) **Ensure rights** and benefits of data owner;"	defines provisions that support the concepts of privacy by design and by default, such as: (Sec. 24) "An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored." (Sec. 18) "An organisation may collect, use or disclose personal data about an individual only for purposes — (a) that a reasonable person would	provisions that support the concepts of privacy by design and by default, such as: (Sec. 22) "The collection of Personal Data shall be limited to the extent necessary in relation to the lawful purpose of the Data Controller." (Sec. 37) "The Data Controller shall have the following duties: 1. provide appropriate security measures for preventing the unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of Personal Data, and such measures must be reviewed when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety. It shall also be in accordance with the minimum standard specified and announced by the Committee;"

		consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable”	

Annex H – Supervisory Authorities

Table 9 - Supervisory Authorities in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU’s General Data Protection Regulation (GDPR)	Laos’ Law on Electronic Data Protection (LEDP)	Singapore’s Personal Data Protection Act (Singapore’s PDPA)	Thailand’s Personal Data Protection Act (Thailand’s PDPA)
(Art.4(21)) The GDPR defines **supervisory authority** as “an independent public authority which is established by a Member State pursuant to Article 51”	 The Laos LEDP equivalent to a supervisory authority is the Administration Organization of Electronic Data Protection, which it defines as: (Art. 40) “The government is an administration center of Electronic Data Protection and unity throughout the country which the Ministry of Posts and Telecommunication is a key person in responsible and coordination with line ministries, Government	(Sec. 5) “1. The Info-communications Media Development Authority is designated as the Personal Data Protection Commission. 2. The Personal Data Protection Commission is responsible for the administration of this Act.”	(Sec. 8) “There shall be a **Personal Data Protection Committee**, consisting of: (1) a Chairperson who is selected and appointed from the persons having distinguished knowledge, skills, and experience in the field of Personal Data protection, consumer protection, information

	Organizations equivalence to the ministry, Local Authorities, and other relevant sectors are implemented.		technology and communicati on, social science, law, health, finance, or any other field that must be relevant to, and useful for, the protection of Personal Data; (2) the Permanent Secretary of the Ministry of Digital Economy and Society, shall be a Vice-Chairperson; (3) directors by position as five members consisting of the Permanent Secretary of the Prime Minister Office, the Secretary-General of the Council of State, the Secretary-General of the Consumer Protection Board, the Director-

			General of the Rights and Liberties Protection Department, and the Attorney General; (4) honorary directors as nine members, selected and appointed from the persons having distinguished knowledge, skills, and experience in the field of Personal Data protection, consumer protection, information technology and communication, social science, law, health, finance, or any other field that must be relevant to, and useful for, the protection of Personal Data." (Sec. 43) "There shall be an

			Office of the Personal Data Protection Committee, whose objectives are to protect Personal Data, encourage and support the country's development regarding Personal Data protection" (Sec. 48) "There shall be a **commission supervising the Office of Personal Data Protection Committee** consisting of a Chairperson, who is selected and appointed from a person having distinguished knowledge, skills and experience in Personal Data protection, the Permanent Secretary of the Ministry of Digital Economy and Society, and the Secretary-General of Office of the National Digital Economy and Society Commission as directors, and six honorary directors which ,at least three persons, are selected and appointed from persons having

			distinguished knowledge, skills and experience in Personal Data protection; and other related areas which will be useful for the operation of the Office." (Sec. 57) "There shall be a **Secretary-General** who is appointed by the commission supervising the Office of Personal Data Protection Committee and the SecretaryGeneral has the duty to administer the affairs of the Office." (Sec. 71) "The Committee shall appoint one or more **expert committees** based upon their field of expertise, or as the Committee deems fit."
(Art.51) "1. **Each Member State shall provide** for one or more **independent** public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights	There is no reference on the independence of the Administration. However, since it is comprised of government agencies, its independence is questionable	There is no reference on the independence of the Personal Data Protection Commission	There is no reference on the independence of the Personal Data Protection Committee

and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')"			
(Art.57) "Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce (...) (b) promote public awareness (...) (c) advice (...) (d) promote awareness of controllers and processors (...) (e) (...) provide information (...) (f) handle complaints (...) (g) cooperate (...) and provide assistance (...) (h) conduct investigations (...) (i) monitor	(Arts. 41-44) The Laos LEDP sets out a hierarchical and coordinated effort at multiple administrative levels to ensure comprehensive electronic data protection across the country. Still, they have common responsibilities: • Public Awareness and Education (Arts. 41(3), 42(1), 43(1)) • Implementation of Policies and Plans (Arts. 41(2), 42(2)(4), 43(3)(4)) • Guidance and Oversight (Arts. 41(4)(7), 42(3), 43(2)) • Issue Resolution and Proposal Handling (Arts. 41(9), 42(5)	(Sec. 6) "The functions of the Commission are — (a) to promote awareness of data protection in Singapore; (b) to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection; (c) to advise the Government on all matters relating to data protection; (d) to represent the Government internationally on matters relating to data protection; (e) to conduct research and	(Sec. 16) "The Committee shall have the following duties and power: (1) to make the master plan on the operation for the promotion and protection of Personal Data´(...) (2) to promote and support government agencies and the private sector (...) (3) to determine measures or guidelines of the operation in relation to Personal Data protection in order to comply with this Act; (4) to issue notifications or rules for the execution

(...) (j) adopt standard contractual clauses (...) (k) establish and maintain a list in relation to the requirement for data protection impact assessment (...) (l) give advice on the processing operations (...) (m) encourage the drawing up of codes of conduct (...) (n) encourage the establishment of data protection certification mechanisms (...) (o) (...) carry out a periodic review of certifications (...) (p) draft and publish the criteria for accreditation of a body (...) (q) conduct the	• Coordination (Arts. 41(10), 42(6), 43(6)) • Reporting (Arts. 41(12), 42(8), 43(7)) • Fulfilling Additional Legal Duties, specified in each level of responsibility	studies and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities; (f) to manage technical cooperation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or inter-governmental organisations, on its own behalf or on behalf of the Government; (g) to	of this Act; (5) to announce and establish criteria for providing protection of Personal Data which is sent or transferred to a foreign country; (6) to announce and establish guidance for the protection of Personal Data as guidelines with which the Data Controller and the Data Processor shall comply; (7) to recommend the Cabinet on the enactment, or revision, of the laws or rules applicable to the protection of Personal Data; (8) to recommend the Cabinet on the enactment of the Royal Decree or reconsiderati on the

accreditation of a body (r) authorise contractual clauses and provisions (...) (s) approve binding corporate rules (...) (t) contribute to the activities of the Board (u) keep internal records of infringements (...) (v) fulfil any other tasks related to the protection of personal data”		administer and enforce this Act; (h) to carry out functions conferred on the Commission under any other written law; and (i) to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order in the Gazette”	suitability of this Act at least every five years; (9) to provide advice or consultancy (...) (10) to interpret and render rulings with respect to the issues arising from the enforcement of this Act; (11) to promote and support learning skills and understandin g on the protection of Personal Data among the public; (12) to promote and support research for the development of technology relating to the protection of Personal Data; (13) to perform any other acts as prescribed by this Act, or other laws, which state the duties

			and power of the Committee.”
(Art.58) “1. Each supervisory authority shall have all of the following **investigative powers**: (...) (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; 2. Each supervisory authority shall have all of the following **corrective powers:** (...) (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;	The Laos LEDP does not refer to powers of the Administration Organization of Electronic Data Protection	(Sec. 50) “1. The Commission may, upon complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation or a person is complying with this Act, including a voluntary undertaking given by the organisation or person under section 48L(1). 2. The **powers of investigation** under this section of the Commission and the inspectors are set out in the Ninth Schedule.” (Sec.48J) “1. Subject to subsection (2), the Commission may, if it is satisfied that — (a) an organisation has intentionally or negligently contravened any provision of Part 3, 4, 5, 6, 6A or 6B; or (b) a person has	(Sec. 72) “Section 72 The expert committee shall have the following duties and power: (1) Consider complaints under this Act; (2) **Investigate** any act of the Data Controller or the Data Processor, including the employees or the contractors of the Data Controller or the Data Processor in connection with the Personal Data that causes damage to the Data subject; (3) Settle disputes in connection with Personal Data; and (4) Carry out any other acts which are stipulated as the expert committee’s

3. Each supervisory authority shall have all of the following **authorisation and advisory powers**: (...) e) to accredit certification bodies pursuant to Article 43;"		intentionally or negligently contravened — (i) any provision of Part 9; or (ii) section 48B(1), require, by written notice, the organisation or person (as the case may be) to **pay a financial penalty**." (Sec. 49) "The Commission **may issue written advisory guidelines** indicating the manner in which the Commission will interpret the provisions of this Act."	duty and power under this Act or as assigned by the Committee." (Sec. 90) "The expert committee shall have the **power to render the punishment as an administrative fine** prescribed in this Part. In the event that it deems fit, the expert committee may issue an order for rectification or a warning first."

Annex I – Data Protection Impact Assessment (DPIA)

Table 10 - Data Protection Impact Assessment (DPIA) in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Art. 35(1)) "Where a type of processing in particular using new technologies, and taking into account	Laos' LEDP does not include a Data Protection Impact Assessment, but it does require that:	Singapore's PDPA does not explicitly mention a DPIA	Thailand's PDPA does not explicitly mention a DPIA

the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact of the envisaged processing operations on the protection of personal data**. A single assessment may address a set of similar processing operations that present similar high risks."	(Art. 23(6)) "The data administration authority shall maintain electronic data as follow: (6) Inspect and evaluate the risk of data system at least once a year and must fix the detected problem including update the data system to be secured;"		
(Art. 35(3)) "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a **systematic and extensive evaluatio**n of personal aspects relating to natural persons which is **based on automated processing**, including			

profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of **special categories of data** referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a **large scale**.			
(Art. 35(7)) "The assessment shall contain at least: (a) a **systematic description** of the envisaged processing operations	The Laos' LEDP makes no reference to what the assessment must contain		

	and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an **assessment of the necessity and proportionality** of the processing operations in relation to the purposes; (c) an **assessment of the risks to the rights and freedoms** of data subjects referred to in paragraph 1; and (d) the **measures envisaged to address the risks,** including safeguards, security measures and mechanisms to ensure the protection of personal			

data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."			

Annex J – Data Protection Officer (DPO)

Table 11 - Data Protection Officer (DPO) in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Arts. 37(1)) "The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a **public authority** or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or	The Laos LEDP makes only one mention of the necessity to appoint an officer to be in charge of data protection: (Art. 23(1)) "The data administration authority shall maintain electronic data as follow: (1) Contain specific units or staffs that responsible for the	(Art. 11(3)) "An organisation must designate one or more individuals to be responsible for ensuring that the organisation complies with this Act." (Art. 11(6)) " The designation of an individual by an organisation under subsection (3) does not relieve the organisation of any of its	(Sec. 41) "The Data Controller and the Data Processor shall designate a data protection officer in the following circumstances: (1) the Data Controller or the Data Processor is a **public authority** as prescribed and announced by the Committee; (2) the activities of

the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a **large scale**; or (c) the core activities of the controller or the processor consist of processing on a large scale of **special categories** of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10. “	administration of data security”	obligations under this Act.”	the Data Controller or the Data Processor in the collection, use, or disclosure of the Personal Data require a **regular monitoring** of the Personal Data or the system, by the reason of having a large number of Personal Data as prescribed and announced by the Committee; or (3) the core activity of the Data Controller or the Data Processor is the collection, use or disclosure of the Personal Data according to **Section 26**.”
(Rec. 97) “(...) Such data protection officers, whether or not they are an employee of the controller, should be in a position to	Laos’ LEDP does not mention the independence of the DPO	Singapore’s PDPA does not mention the independence of the DPO	(Sec. 42) “The Data Controller or the Data Processor **shall not dismiss or terminate the data protection officer’s**

perform their duties and tasks in an **independent manner**."			**employment** by the reason that the data protection officer performs his or her duties under this Act. In the event that there is any problem when performing the duties, the data protection officer must be able to directly report to the highest management person of the Data Controller or the Data Processor."
(Art. 39) "1. The data protection officer shall have at least the following tasks: (a) to **inform and advise the controller or the processor** and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to **monitor compliance** with this Regulation, with other Union or Member State	The Laos LEDP does not specify the tasks of the data protection officer beyond the general duty of maintaining data security.	Singapore's PDPA does not mention the responsibilities of the DPO	(Sec. 42) "The data protection officer shall have the following duties: (1) **give advices** to the Data Controller or the Data Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect to compliance with this Act; (2) **investigate the performance** of the Data Controller or the Data

data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection **impact assessment** and monitor its performance pursuant to Article 35; (d) to **cooperate with the supervisory authority**; (e) **to act as the contact point** for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and			Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect to the collection, use or disclosure of the Personal Data for compliance with this Act; (3) **coordinate and cooperate with the Office** in the circumstance where there are problems with respect to the collection, use or disclosure of the Personal Data undertaken by the Data Controller or the Data Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect

to consult, where appropriate, with regard to any other matter.			to the compliance with this Act; and (4) **keep confidential** the Personal Data known or acquired in the course of his or her performance of duty under this Act."

Annex K – Data Breach Notification

Table 12 - Data Breach Notification in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Arts. 4(12)) The GDPR defines a **personal data breach** as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"	The regulation does not mention "data breach," consistently referring only to matters of security. Laos' LEDP delineates that: (Art. 26) "Responding to data attacks shall comply as following: Data administration authority uses interception and fixed methods when have been informed by individual, legal entities or organizations that relating to sending of data that cause or	(Sec. 26A) Under Singapore's PDPA, a "data breach" concerning personal data is defined as "(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure,	Thailand's PDPA does not provide a definition of data breach

	may cause unpeaceful of the society;"	copying, modification or disposal of the personal data is likely to occur."	
(Art. 33) "1. In the case of a personal data breach, the **controller shall** without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, **notify the personal data breach to the supervisory authority** competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The **processor shall notify the controller** without undue delay after becoming aware of a personal data breach."	The Laos LEDP makes no reference of the requirements for notification	(Sec. 26(C)) "2. Subject to subsection (3), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. 3. Where a data intermediary (other than a data intermediary mentioned in section 26E) has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation — (a) the data intermediary must, without undue delay, notify that other	(Sec. 37(4) "The Data Controller shall have the following duties: (...) (4) notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Persons. If the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Persons, the Data Controller shall also notify the Personal Data breach

		organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach." (Sec. 26E) "Where an organisation — (a) is a data intermediary processing personal data on behalf of and for the purposes of a public agency; and (b) has reason to believe that a data breach has occurred in relation to that personal data, the organisation must, without undue delay, notify the public agency of the occurrence	and the remedial measures to the data subject without delay. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Committee." (Sec. 40(2)) "The Personal Data Processor shall have the following duties: (...) (2) provide appropriate security measures for preventing unauthorized or illegal loss, access to, use, alteration, correction or disclosure, of Personal Data, and notify the Data Controller of the Personal Data breach that

		of the data breach."	occurred;"
(Art.34(1)) "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall **communicate the personal data breach to the data subject** without undue delay.		(Sec. 26D) "2. Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances"	

Annex L – Administrative Fines

Table 13 - Administrative Fines in the EU's GDPR, Laos' LEDP, Singapore's PDPA and Thailand's PDPA

EU's General Data Protection Regulation (GDPR)	Laos' Law on Electronic Data Protection (LEDP)	Singapore's Personal Data Protection Act (Singapore's PDPA)	Thailand's Personal Data Protection Act (Thailand's PDPA)
(Arts. 83(4)(5)) "4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to **10 000 000 EUR**, or in the case of an undertaking, up to **2 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher: (a) the	(Art 52) "Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in Article 31, 32, and 33 which are not considered as criminal offence will be fined 15.000.000 Kip."	(Sec.48J) "3. A financial penalty imposed on an organisation under subsection (1)(a) must not exceed the maximum amount to be prescribed, which in no case may be more than the following: (a) in the case of a contravention on or after the date of commencement of section 24 of the Personal	(Sec. 79) "Any Data Controller who violates the provisions under Section 27 paragraph one or paragraph two, or fails to comply with Section 28, which relates to the Personal Data under Section 26 in a manner that is likely to cause other person to suffer any damage, impair his or her

obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4). 5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to **20 000 000 EUR,** or in the case of an undertaking, up to **4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6,		Data Protection (Amendment) Act 2020 by an organisation whose annual turnover in Singapore exceeds $10 million — 10% of the annual turnover in Singapore of the organisation; (b) in any other case — $1 million."	reputation, or expose such other person to be scorned, hated, or humiliated, shall be punished with imprisonment for a term not exceeding six months, or a **fine not exceeding five hundred thousand Baht**, or both." (Sec. 80) "Any person who comes to know the Personal Data of another person as a result of performing duties under this Act and discloses it to any other person shall be punished with imprisonment for a term not exceeding six months, or a **fine not exceeding five hundred thousand Baht**, or both" (Sec. 82) "Any Data Controller who fails to comply with Section 23, Section 30 paragraph four, Section 39 paragraph one, Section 41 paragraph one, or Section 42

7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)."			paragraph two or paragraph three, or fails to obtain consent using a form or statement set forth by the Committee under Section 19 paragraph three, or fails to notify the impact of the withdrawal of consent under Section 19 paragraph six, or fails to comply with Section 23 which applies mutatis mutandis according to Section 25 paragraph two, shall be punished with an administrative **fine not exceeding one million Baht.**" (Sec. 83) "Any Data Controller who violates or fails to comply with Section 21, Section 22, Section 24, Section 25 paragraph one, Section 27 paragraph one or two, Section 28, Section 32 paragraph two, or Section 37, or who obtains consent by deceiving or misleading the Data subject about the purposes, or

			fails to comply with Section 21 which applies mutatis mutandis according to Section 25 paragraph two, or fails to send or transfer the Personal Data in accordance with Section 29 paragraph one or paragraph three, shall be punished with an administrative **fine not exceeding three million Baht**" (Sec. 84) "Any Data Controller who violates Section 26 paragraph one or three, or Section 27 paragraph one or paragraph two, or Section 28 in relation to the Personal Data under Section 26, or fails to send or transfer the Personal Data under Section 26 to be in accordance with Section 29 paragraph one or paragraph three, shall be punished with an administrative **fine not exceeding five million Baht.**" (Sec. 85)

			"Any Data Processor who fails to comply with Section 41 paragraph one, or Section 42 paragraph two or three, shall be punished with an administrative **fine not exceeding one million Baht.**" (Sec. 86) "Any Data Processor who fails to comply with Section 40 without appropriate reasons, or fails to send or transfer the Personal Data in accordance with Section 29 paragraph one or three, or fails to comply with Section 37 (5) which applies mutatis mutandis according to Section 38 paragraph two, shall be punished with an administrative **fine not exceeding three million Baht.**" (Sec. 87) "Any Data Processor who send or transfer the Personal Data

			under Section 26 paragraph one or three, by not complying with Section 29 paragraph one or three, shall be punished with an administrative **fine not exceeding five million Baht.**" (Sec. 88) "Any representative of the Data Controller or of the Data Processor who fails to comply with Section 39 paragraph one which applies mutatis mutandis according to Section 39 paragraph two, and Section 41 paragraph one which applies mutatis mutandis according to Section 41 paragraph four, shall be punished with an administrative **fine not exceeding one million Baht.**" (Sec. 89) "Any person who fails to act in compliance with the order given by the expert committee, or fails to provide

			statement of facts under Section 75, or fails to comply with Section 76(1), or fails to facilitate government officials under Section 76 paragraph four, shall be punished with an administrative **fine not exceeding five hundred thousand Baht.**" (Sec. 90) "The expert committee shall have the power to render the punishment as an administrative fine prescribed in this Part. In the event that it deems fit, the expert committee may issue an order for rectification or a warning first."