HARMONIZING VIETNAMESE PERSONAL DATA PROTECTION LAW WITH ASEAN STANDARDS: LESSONS LEARNED FROM THE SINGAPOREAN

Khoi Trong Dao
University of Law, Vietnam National University
Khoidt@vnu.edu.vn

Abstract: The harmonization of personal data protection (PDP) regulations amongst ASEAN members is considered by the ASEAN Digital Masterplan 2025 as essential to developing the ASEAN digital economy in the fourth industrial revolution. Vietnam has long expressed its commitment to protecting personal data and has considered PDP issues since 2006 but has yet to introduce a comprehensive system for PDP. In this regard, the article aims to examine the current Vietnamese laws, including the newly drafted Decree guiding PDP, under core principles of the ASEAN Framework on PDP (AFPDP), and also in comparison to the Singaporean PDP system – one of the most comprehensive and active systems in ASEAN. The study demonstrates that Vietnamese privacy laws have yet to be fully aligned with the ASEAN common PDP standards, yet be ready for direct application due to the lack of structural approaches and various ambiguities or overlaps between specific regulations dispersed in multiple laws. Therefore, although the newly drafted PDP Decree might be an appropriate short-term solution to substantially improve Vietnamese laws in dealing with PDP issues, further discussions on making an all-in-one PDP law are more than needed to adequately meet the ASEAN's harmonized standards. The making of such a new law should refer to the experience of the Singaporean PDP system that balances both personal data shielding and business-friendly approaches.

1. Introduction

The negative effect of the Covid-19 pandemic could not deter but contribute to the great expansion of the ASEAN digital market, with nearly 400 million users. ASEAN's digital revenue is currently generating around USD 150 billion and is expected to reach $363 billion by 2025 and USD 1 trillion in 2030.[1] Although ASEAN's digital economy surges remarkably, this is not accompanied by updated market regulations in various key areas relating to digital transformation, especially personal data protection. The comprehensiveness of Member's domestic laws on personal data protection (PDP) varies from state to state. While some countries such as Malaysia, Singapore, Thailand, and the Philippines have decent regulatory frameworks in this area,[2] Vietnam is a telling example of a fast-growing digital economy with an under-developing PDP system.

Improvements in all ASEAN Members' personal data protection (PDP) regulations are crucial to the general development of the ASEAN digital economy due to several rationales. *First*, these improvements is necessary to build a secure digital environment - an undeniable condition for the

[1] Kearney, *ASEAN Digital Revolution* (Report, 2020) 13. See also, Vietnam National Television, "Strategy to promote digital innovation and digital economy in Pacific Asia", Report on Huawei APAC Digital Innovation Conference 2022 (VTV Official Website) accessed on 10 November 2022, at < https://vtv.vn/cong-nghe/chien-luoc-thuc-day-doi-moi-ky-thuat-so-va-nen-kinh-te-so-khu-vuc-chau-a-tbd-2022052010413274.htm>

[2] Sri Handayani Nasution, *Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025* (Policy Paper, No. 46, Center for Indonesian Policy Studies, 2021) 14.

expansion of the digital market.[3] ASEAN is one of the most vulnerable regions to personal data leaks and cyberattacks.[4] Illegal trade and severe breaches of personal data are frequently reported by many ASEAN members.[5] This may remarkably drive down individual's trust in the digital market and in turn, damages the growing participation in the digital economy.[6] Low consumer trust in digital services might lead to great hesitation to share personal data and participate in online activities, which then hinder the development of the digital market.[7] Therefore, PDP regulation improvements play an indirect but essential role in securing the fast-developing digital future of the region.

Second, harmonizing PDP regulations among ASEAN members is irreversible for the target of enhancing cross-border data transfer and the introduction of a single digital market, if it may. The 2025 ASEAN Digital Masterplan (ADM) considers facilitating digital cross-border trade and services as one of its eight crucial desired outcomes. This inter-nation activity is expected to enhance ASEAN's trade digitalization, encouraging businesses to trade and transact digitally across ASEAN with over 71 million businesses and 700 million customers,[8] leading to substantial benefits for ASEAN as a whole and also for other participating countries investing in the region.[9] ASEAN had promised to build a 'single market' by 2015 since 2003, and in the digital era, it might be ambitious but necessary to dream of an ASEAN digital single market, following the concept of the European Union.[10] To fulfill such aims, the ADM emphasizes a need of a continuing identification of opportunities to harmonize digital regulation in ASEAN,[11] and most importantly, on a "harmonized principles-based data protection and privacy regulations and frameworks".[12]

Such a harmonized principles-based PDP regulation has been introduced in the ASEAN Framework on Personal Data Protection (AFPDP) by the Telecommunications and Information Technology Ministers Meeting since 25 November 2016. The frameworks provide the ASEAN

---

[3] ASEAN Digital Masterplan 2025 (ADM) 41 and 66.
[4] Sri Handayani Nasution, *Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025* (Policy Paper, No. 46, Center for Indonesian Policy Studies, 2021) 14.
[5] 96 percent of businesses in Singapore suffered a data leak from 09/2018 to 09/2019, see further: Vmware, *Carbon Black Singapore Threat Report 2020* (Vmware Report, 2021) 13. In Thailand, there was also an increasing number of reports on recent data breaches, see further at: Nikkei Asia, "Thailand's cybersecurity negligence causes personal data breaches", *Nikkei Asia* (Bangkok, 2021) at https://asia.nikkei.com/Business/Technology/Thailand-s-cybersecurity-negligence-causes-personal-data-breaches. In Vietnam, data of two third of Vietnamese citizens are leaked and transferred online, according to Minster of the Vietnamese Ministry of Police, see further Le Hiep, "Minister of the MPS: 1.300GB personal data of Vietnameses are traded online", *Thanh Nien Online* (Hanoi, 9 Aug 2022) accessed on 15 Nov 2022, at < https://thanhnien.vn/bo-truong-cong-an-1-300-gb-du-lieu-ca-nhan-nguoi-viet-bi-mua-ban-tren-mang-post1486332.html>
[6] World Bank, *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth* (Report, 2019) p17.
[7] Kearney, *ASEAN Digital Revolution* (Report, 2020) 29.
[8] Michael Schaper, "The Missing (Small) Businesses of Southeast Asia" (*Perspective*, *Yusof Ishak Institute*, *Singapore*, Issue: 2020, No. 7922, July 2020) accessed at <https://www.iseas.edu.sg/wp-content/uploads/2020/06/ISEAS_Perspective_2020_79.pdf>
[9] ADM 2025 p 24, 25.
[10] Sanchita Basu Das, "An ASEAN Single Digital Market? Small Beginnings, Great Endings" (*Yusof Ishak Institute, Commentaries*, 7 March 2018) accessed on 12 Nov 2022, at <https://www.iseas.edu.sg/media/commentaries/to-an-asean-single-digital-market-small-beginnings-great-endings-by-sanchita-basu-das/>
[11] ADM, 23.
[12] ADM, 22.

Members with a set of PDP standards and encourage the Members to incorporate these into their domestic law and policies. The AFPDP's guiding principles are briefly described below:

- "Consent, Notification and Purpose", requires organizations should not collect, use or disclose personal data unless obtaining the data subject's consent.
- "Accuracy of Personal Data", emphasizes that personal data should only be collected accurately and completely to the extent necessary for the using/ disclosing purpose(s).
- "Security Safeguards", requires that personal data be appropriately protected against any risks and loss, for instance, unauthorized access, collection, or destruction.
- "Access and Correction" requires organizations to provide individuals with the right to access their data and correct errors timely.
- "Transfers to Another Country or Territory" requires organizations to obtain data subjects' consents for an overseas transfer or to ensure that receivers will protect the data carefully.
- "Retention" expresses various obligations of organizations to cease to retain documents containing personal data when they are no longer necessary.
- "Accountability" requires that the organization is accountable for ensuring transparency in handling personal data.

It is widely accepted that the ADM and AFPDP are not legally regional binding documents and ASEAN does not interfere in domestic law-making. Nevertheless, the principle of *pacta sunt servanda* requires every Member to keep upgrading their national law to embrace these commitments, and Vietnam is not exceptional. Since 2019, Vietnamese political leaders have emphasized that Vietnam should "actively participate in regional … regulatory frameworks for digital economy development", by "improving laws and policies on data, data governance, … to ensure network safety and security in the country, towards connecting with … the ASEAN and the international".[13] In this regard, the Vietnamese Government also issued Resolution No. 17/NQ-CP on key tasks and solutions to develop e-Government with an orientation to 2025.[14] This Resolution specifically assigned the Ministry of Public Security (MPS) to take responsibility for drafting a first and comprehensive guidance on PDP in the form of a Government's Decree ("the Draft Decree"). The first draft version of this Decree was introduced in February 2021.[15] After a two-month consultation period, the Draft is being re-appraised by the Ministry of Justice before being officially submitted to the Government for adoption.[16] This Decree deserves to be regarded as a great move of Vietnamese PDP regulations, opening up the expectation that Vietnamese privacy laws will soon be converted to meet ASEAN's PDP common standards. However, by contrast, several observers have raised concerns that the Draft Decree might set rigid or ambigious requirements which might block the cross-border data flow.[17]

[13] Article II.2 of the Resolution 52-NQ/TW of the Vietnamese Communist Party's Politburo on policies for Active Participation in the Fourth Industrial Revolution, 27 Sep 2019.
[14] Resolution No. 17/NQ-CP of the Vietnamese Government regarding certain key tasks and measures of development of the electronic government for 2019 – 2020 with a vision towards 2025, 7 March 2019.
[15] The Draft Decree on Personal Data Protection by Vietnam's Ministry of Public Security, published 9 February 2021 ("The Draft Decree" / "Draft PDP Decree")
[16] Article 91, 57, 58 of the 2015 Law on promulgation of legislative documents.
[17] Graham Greenleaf, "Vietnam: Data privacy in a communist ASEAN state" (2021) 170 Privacy Laws & Business International Report, 1, 5-8. Mai Phuong, "Highlights in the content of Draft Regulations on the protection of personal data" (*NHQuang&Associates, Brief Report*, 2021) 5.

In this regard, this article aims to examine the recent Vietnamese PDP laws combined with the Draft Decree under the core principles of AFPDP and in comparison with Singaporean PDP law. The purpose is to clarify how far Vietnamese PDP regulations might get close to the ASEAN's harmonized PDP standards. In the way towards ADM's desired outcomes and the AFPDP principles, the PDP laws of ASEAN countries such as Philippines, Singapore, Thailand, or Malaysia with years of experience in practical application[18] are all good examples for Vietnam to refer in codification. The Singaporean PDP system stands out as one of the oldest (entered into force since 2013), most active, and most comprehensive PDP systems in ASEAN. A straight comparison between current Vietnamese PDP laws and Singaporean practices is therefore useful for Vietnamese legislators in our codification of PDP law and a better harmonization to the ASEAN common standards in this field. Therefore, after this introduction, the second part of this article briefly introduces the Vietnamese PDP legal framework, followed by the third part examining core Vietnamese PDP regulations before finally providing several law-making suggestions.

2.1. Vietnamese PDP legal framework in brief

2.1.1. From privacy rights to personal data protection and beyond

In Vietnam, personal data is generally protected through a privacy rights regime. Protecting the fundamental privacy values of an individual has been considered from the initial days of the Democratic Republic of Vietnam in our first Constitution in 1946.[19] Throughout the subsequent constitutions of 1959, 1980, 1992, and 2013, the right to privacy was all recognized with an ongoing expanded scope.[20] Article 21 of the 2013 Constitution regulates that everyone has the "inviolable" right to privacy, which includes personal secrets, family secrets, secrets of correspondence, telephone calls, telegrams, and other forms of private information exchange. Such a grand privacy right should be categorized into two groups: Rights to keep confidential (i) personal secrets and (ii) personal communications.[21] It is evident that to secure such confidentiality, legal tools to block personal identification or illegal collection of personal information are of paramount importance.[22] In acknowledgment of this issue since 2006 Vietnamese legislators started to consider protecting personal information in the Law on Information Technology, requiring any party collecting and processing personal information to obtain individual's consent and shall keep private information in secret.[23] However, several following laws did not coherently and thoroughly govern or clarify further on this matter. This hibernation was preserved until 2015-2016 when cyber security concerns took the spotlights and reminded the legislators of a need for updated regulation in this field, in combination with the extra-territorial effects of the EU's GPDR model.

---

[18] ZICO Knowledge Management, *Personal Data Protection in ASEAN* (*ZICO ASEAN Insider Series*, Sep 2020).
[19] Article 11 of the first 1946 Vietnamese Constitution. For further information, see: Chu Hồng Thanh, "Legal awareness of privacy", in *Privacy Rights* (National Politics Publishing House, Hanoi, 2018) 134.
[20] Vu Cong Giao, Le Tran Nhu Tuyen, "Protection of rights to personal data in international law and some countries' legislation and valuable reference for Vietnam" (2020) 09 Journal of Legislative Studies 409.
[21] Duong Kim The Nguyen, Huynh Thien Tu, Le Thuy Khanh, Mai Nguyen Dung, "Reforming the current privacy laws to meet the needs of personal data protection in digital transformation", in *University of Economics HoChiMinh City Series, Chapter* 7 (UEH Publisher, 2021).
[22] UDHR, Refworld, CCPR General Comment No 16, 1988.
[23] Article 21.1 and 72 of the 2006 Law on Information Technology.

However, the core approaches to developing PDP regulations in Vietnam have yet to be fully discussed or widely agreed. Vietnamese law still favors a traditional approach that prioritizes the protection of personal data to the level of "inviolability" as per the requirement of the 2013 Constitution.[24] This sole approach might be easily observed in two current basic principles of Vietnam's PDP law, namely (i) confidentiality and (ii) consent, specified in Article 38 of the Vietnamese Civil Code. Accordingly, information related to private life and personal secrets must be strictly kept confidential, and the other party's collection, storage, use, and disclosure of such information shall be consented to by the information subject. However, a strict application of this approach might fail to optimize the benefits of personal data, as in the digital era, personal data must not be "static" but "dynamic" with circulation to contribute value to the economy.[25] Simultaneously, this closed approach does not pay attention to the interests of other stakeholders, for instance, businesses and researchers seeking data for enhancing development, effectiveness, or other economical benefits to the digital market as a whole.

In this sense, Vietnam should consider referring to the dual-objective approach of the Singaporean PDP Act (PDPA),[26] which recognizes the significance of securing the individual's legitimate rights to privacy and the need of various other parties to collect and process personal data for other legitimate commercial and social purposes. This dual-objective approach also emphasizes the essentialness of a comprehensive PDP regime in safeguarding personal data from illegal misuse and keeping people's trust in other parties' data management, which might consequently enhance digital market participation. In the broader view, this Singaporean PDP regulation is expected to contribute to strengthening Singapore's position as a trusted hub for businesses worldwide.[27]

2.1.2. A fragmented system

There has yet to be a comprehensive law on PDP in Vietnam. Therefore, anyone interested has to check around 70 legal documents comprising of, *inter alia,* 04 codes, 37 statutes, and many decrees (sub-law documents), which introduce general rules and specific PDP requirements in specialized areas.[28] However, many of these regulations are too generic for application, as those typically state the general obligations for organizations and persons rather than specifying required conditions or steps for compliance. Sometimes, those might even be contradictory and cause difficulties in enforcement.[29]

---

[24] Article 21 of the 2013 Vietnamese Constitution.
[25] Duong Kim The Nguyen, Huynh Thien Tu, Le Thuy Khanh, Mai Nguyen Dung, "Reforming the current privacy laws to meet the needs of personal data protection in digital transformation", in *University of Economics HoChiMinh City Series, Chapter 7* (UEH Publisher, 2021).
[26] The 2012 Personal Data Protection Act of Singapore (Singapore PDPA).
[27] Singapore Personal Data Protection Committee (PDPC), "PDPA Overview" (*Official Website of the Singapore PDPC,* 13 November 2022) accessed at < https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>
[28] Hoa Chu, "Legal Framework for Personal Data Protection in Vietnam" in *Smart Cities in Asia Regulations, Problems, and Development* (SprinerBriefs in Geography, Chapter 8, 2021) 96.
[29] Hoa Chu, "Legal Framework for Personal Data Protection in Vietnam" in *Smart Cities in Asia Regulations, Problems, and Development* (SprinerBriefs in Geography, Chapter 8, 2021) 97.

As a result, when the Draft PDP Decree was introduced for consultation, the mentioned fragmentation was expected to be ended. However, several concerns might still exist even after such a Decree finalization. *First*, rather than a comprehensive act issued by the National Assembly, the most important legal document regulating PDP is just formed in a Decree by the Ministry of People's Police (MPS), typically used as "guidelines" for other laws' application. Forming as such might serve as a timely and sand-box legal experiment of a PDP regime and allow legislators to "wait and see" its effectiveness. However, the very changeability of this method also poses a risk to businesses' legitimate expectations and might cause disruptions to the digital market in case of changes. *Second*, as a secondary law guidance, the Draft Decree cannot overwrite or prevail over other PDP laws previously issued by the National Assembly[30] and might not serve as an umbrella legal document for all PDP regulations. *Third*, as the Decree was prepared by the MPS, one might concern that its provisions tend to be more conservative or protective rather than balancing the individual's "inviolable" rights to privacy and other stakeholders' economic interests.

2.2. Core regulations

2.2.1. Definition of personal data

The first and foremost matter to discuss is the crucial definition of "personal data". Vietnamese laws have yet to introduced a widely-adopted definition and generally protects "data" relating or belonging to persons that may help to particularly identify such persons. However, there are almost ten similar terms relating to "personal data" such as "private information", "personal information", "personal information on the Internet", or "digital information" being used in various laws and guiding legal documents, while the nature of these definitions and the relationship between them are unclear. Amongst the above terms, "personal information" is primary being used,[31] but its definition also varies between documents and might contradict each other. For instance, Decree No. 72 guiding the application of the 2006 Information Techonology Law defines personal information as "information associated with the identification of individuals, including names, ages, addresses, people's identity card numbers, phone numbers, email addresses and other information defined by law", irrespective of whether it has been publicized or not. However, Decree No. 52/2013/NĐ-CP specifies "personal information" as "information contributing to identifying a specific individual, including their name, age, home address, phone number, medical information, account number, information on personal payment transactions, and other information that the individual would like to keep confidential", but "does not include work contact information and other information … published in the mass media".[32] The first abstract definition of "personal information" introduced in a statute (the Network Information Security Law) is "information associated with the identification of a specific person"[33] but is too generic for direct application and in need of further clarification in, for instance, a specific guiding Decree.

This might be changed by the Draft PDP Decree, as this Decree directly targets personal data for the first time and defines it as "data about an individual or related to the identification or possible identification of a particular individual".[34] It should be understood that this definition has two

[30] Article 156 of the 2015 Law on Promulgation of Legislative Documents.
[31] Nguyen Quynh Trang, "Law on protection of personal data in the context of AI development and other emerging digital technologies" (2022) 50 Journal of Law and Legal Practice 137, 143.
[32] Article 3 of the Decree 52/2013/NĐ-CP on E-Commerce, 16 May 2013.
[33] Article 15.3 of the 2015 Network Information Security Law.
[34] Article 2.1 of the Draft Decree ("Draft PDP Decree")

factors. *First*, personal data is defined based on its functionality that whether it may contribute to identifying a specific person. *Second*, there are two ways to function: direct (the data tells itself) or indirect (related to the "possible identification" of an individual). However, for the first factor, the notion of "data *about* an individual" and its difference from data "*related to the identification of* an individual" is unclear. Both might be synonymous with each other, as data "about" someone undoubtedly allows a processor to identify the alleged person, and data "*related to the identification of* an individual" can play the same role. Regarding the second factor, this definition fails to clarify how to determine the "possibility" of any data to contribute to identifying a particular person. Therefore, even though a definition is provided in such a Draft PDP Decree, further guiding documents such as lower-level Circular(s) and Letter(s) are much needed to support a proper application.

In comparison, Singaporean 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 organization is likely to have access but excluding any business contact information." While there might be several similarities between these definitions, the Singaporean's is more explicit and comprehensive, as the factors above (contribution to the identification and how the data possibly helps) are clearly separated. Furthermore, it gives a way to determine how a piece of data might help to identify a particular person (and then be classified as "personal data"): if a combination of such alleged data and other available information gives the collector a chance to identify the data subject. The Singaporean definition also expresses several boundaries of its scope of covered "personal data", which is worth consideration: (i) the inclusion of "untrue" "personal data" and (ii) an exclusion of business contact information.

When it comes to sensitive personal data, the current Vietnamese laws do not define such a concept but distinguish some sensitive/ highly-protected data from other personal data in various special areas that enjoy more intense protection, such as financial data (accounts, credit history, etc.) and healthcare data (e.g. medical and disease records).[35] The Draft PDP Decree is expected to solve this issue by introducing two general categories of personal data: basic and sensitive. The Decree defines these categories by listing the names of data types belonging to each category. For instance, "sensitive data" comprises, *inter alia*, political and religious views, mental, social relationships, locations, physical health conditions, genetic, biometric data, sexual orientation, criminal records, and financial data.[36] However, including "social relationships" and "past and current physical locations" in such a list of sensitive data might be too broad and also indeterminate. These types of data might not always be sensitive and it is troublesome to legislate when such data becomes sensitve. For comparison, the GDPR combined definition of sensitive data does not include those types,[37] while Singaporean PDPA has a different approach that leaves the sensitive data to be determined and more carefully protected by a specific law in each sector.[38]

2.2.2. Rights and obligations of data subjects and processors

[35] See further: Decree No. 117/2018/ND-CP of the Vietnamese Government on protection of confidentiality and provision of client information of Credit Institutions and Foreign Banks' Branches, September 11, 2018. Article 8 of the 2009 Law on Medical Examination and Treatment.
[36] Article 2.2 and 2.3 of the Draft PDP Decree.
[37] Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the General Data Protection Regulation (GPDR).
[38] Simon Chesterman, *Data Protection Law in Singapore* (2nd edn, Academy Publishing, 2018) 40.

Under Vietnamese privacy laws, data subjects have several rights over their personal data. However, due to the lack of a comprehensive law or an all-in-one guiding legal document, the precise scope, conditions and applications of those given rights disperse amongst multiple legal documents and might easily overlap each other. Therefore, the article has to outline the relevant regulations before examining them under the seven core principles of the ASEAN Framework of PDP (AFPDP) to see whether the Vietnamese PDP combined rules might align with the ASEAN harmonized standards.

First, the AFPDP's principle of "*Consent, Notification and Purpose*" generally requires organizations to not touch personal data unless obtaining the data subject's consent. The data subject should also be notified of how and for what purpose their personal data is collected. Vietnamese privacy laws generally uphold this trio principle. For the core requirement of consent, the Vietnamese Civil Code emphasizes that collection, preservation, use and publication of information about the private life of an individual must have its permission.[39] Several laws in various areas, such as Cyber Security Law, Law on Consumer Protection, Law on Information Technology, Law on Digital Transactions and the E-commerce Decree all re-confirmed this approach by requiring that the processors could only collect personal data after having consent of data subjects.[40] The Draft PDP Decree further specifies this by requiring stricter consent in Article 8, as to obtain the data subjects' valid consent processors shall inform them of types and purposes of processing, conditions to transfer the data to any third party, and their other legitimate rights. Consent for sensitive data shall be in written or equivalent form. Silence is not consent, and in any case the processor shall take the burden of proof.[41] Automatic processing of personal data is only allowed in contract performance and the data subject shall be "made easy to understand" about such an activity and be duly notified in advance.[42] The significance is that the consent could be withdrawn anytime by the data subjects and cease to exist 20 years after their death.[43]

The current Vietnamese privacy law also requires that data collection and process purposes must be specified in the consent approval and duly notified to the data subject. The processors could use the personal information collected for and only for the declared purposes.[44] The Draft Decree will continue to follow this approach by introducing its "principle of purpose", as personal data could only be processed per the registered purpose or declaration of processing personal information.[45] In combination with the "lawful principle" introduced by the Draft Decree, which specifies that personal data could only be collected "in cases where it is necessary by law",[46] the above requirement of consent emphasizes a strict approach that personal data collection without consent is strictly prohibited.

[39] Article 38 Vietnamese Civil Code 2015.
[40] Article 21, 22 of the 2006 Law on Information Technology, Article 6 of the 2010 Law on Consumer Protection, Article 17 of the 2015 Network Information Security Law, Article 46 of the Law on Digital Transactions and Article 4.4. of the 52/2013/NĐ-CP Decree on E-commerce.
[41] Article 8.2 and 8.4 of the Draft PDP Decree.
[42] Article 13 of the Draft PDP Decree.
[43] Article 8.7 of the Draft PDP Decree.
[44] Article 17.1 of the 2015 Network Information Security Law. Article 21.2 of the 2006 Law on Information Technology. Article 6.2(b) of the Law on Consumer Protection.
[45] Article 11.2 of the Draft PDP Decree.
[46] Article 3.1 of the Draft PDP Decree.

However, the Draft Decree also allows processors to circumvent the consent requirements in several circumstances of emergency situations, public interest, investigation of law violation, for statistical research after encryption, and "(other circumstances) in accordance with the law".[47] As these circumstances have a nature of "exception" to the general requirement of consent, they shall be specified in detail. For instance, the notion of "public interest" in this situation deserves to be clarified or referred to a defintion in other laws. Especially, the last exception above (other circumstances according to law) is too broad, as any later law might easily introduce a new exception and overcome such a consent requirement. Furthermore, the Draft Decree also allows processors to be exempted from the obligation to notify data subjects of data processing if such "not affecting data subject's rights and interests and notifying the data subject is not possible".[48] This exemption might also be too broad, giving the processors wide discretion to decide whether their data processing might affect the data subjects' rights and interests, instead of allowing the subjects or an independent party to determine themselves.[49]

Second, the AFPDP's principle of *"Accountability"* focuses on ensuring that the organizations shall transparently explore how personal data is handled. This principle is essential, as without accountability, the data subjects have no idea of how their personal data are processed, who takes responsibility for and should be contacted when breaches occur. The lack of accountability may lead to a decline in people's trust in processors, and in turn, discourage data sharing. In line with this principle, the ASEAN Member's PDP laws should identify all relevant parties in personal data collection, usage, or transfer before regulating their relevant rights and other obligations, such as clarifying their data policies and publishing their contacts for support. For instance, Singapore PDP Act (PDPA) requires the organizations to, *inter alia*, provide transparent information about data policies, ensure their staff follow these policies, appoint a particular Data Protection Officer (DPO) for such compliance, and always be ready to demonstrate that personal data is appropriately managed and protected.[50]

The demonstration of Vietnamese law regarding this principle is not clear cut. The first issue to notice is that the current Vietnamese law does not distinguish between data collectors or controllers and processors. Under the well-known EU's GDPR model, in general data controllers are those determining the purposes and means of processing personal data, while processors mean who processes personal data on behalf of the controller.[51] In Singapore's PDPA, the "data intermediary" is an equivalent to such GPDR concept of "data processor", who processes data for Data Controller and also is subject to the PDPA's Protection and Retention Limitation obligations.[52] In Vietnamese law, any subject handling personal data under the scope of data privacy laws shall obey, disregard who might it be. The Draft PDP Degree continues to work with this approach as all "foreign or domestic agency, organization and individual who process personal data" are considered as personal data processors. There is another party processing personal data but not processors or data subjects, mentioned in the Draft Decree as the "third party". However,

[47] Article 10 of the Draft PDP Decree.
[48] Article 11.3(c) of the Draft PDP Decree.
[49] Mai Phuong, "Highlights in the content of Draft Regulations on the protection of personal data" (*NHQuang&Associates, Brief Report*, 2021) 4.
[50] Part 3 of the 2012 Singapore PDPA.
[51] Article 4.7 GPDR
[52] Article 25 of the Singapore PDPA.

this "third party" receives data from the processors and basically does not process the data on behalf of the data processors.[53]

In addition, Vietnamese law has not recognized the concept of a data protection officer (DPO) or required organizations to designate such a position in any case. Under the well-known GDPR model, the controllers and processors shall appoint a DPO in several cases, for instance, the processing is carried out by a public authority, or requires regular and systematic monitoring of data subjects on a large scale, or when collecting special categories of data (mostly sensitive) on a large scale.[54] In Singapore, any organization subject to the PDPA shall have at least one employee overseeing data protection responsibilities and ensuring compliance with the PDPA.[55] This designation is critical as DPOs will not only enhance data protection compliance in practice but also demonstrate the high commitment of all organizations to obey PDPA regulations. In return, compulsorily requiring all organizations to designate one DPO as such might raise business costs, especially for small and medium firms. However, a compromise should be applied rather than totally skipping such a requirement, for instance, by setting a specific test for the scale of organizations being obligated to have a DPO.

Third, AFPDP's "*Accuracy of Personal Data*" principle emphasizes that personal data should only be collected accurately and completely to the extent necessary for the use or disclosing purpose(s). The Singaporean PDPA upholds this principle by introducing that organizations must make a reasonable effort to ensure that personal data is accurate and complete if such data might be disclosed or used to make a decision affecting the data subject.[56] However, the current Vietnamese privacy laws might fail to meet this principle, as those typically pay attention to allowance and purposes of data collection but not the necessary quantity and quality of data collected. The Draft PDP Decree might solve this issue by introducing a principle of "minimization", requiring that personal data shall be gathered to the extent necessary to achieve the defined purpose only.[57] However, as this Decree does not specify the degree of necessity or any method to calculate such, it is unclear how the principle might be applied in reality.

Fourth, the AFPDP's "*Security Safeguards*" requires that personal data be appropriately protected against loss and unauthorized access, collection, use, disclosure, copying, modification, destruction or similar risks. Vietnamese privacy regulations could generally fulfill this requirement, as it regards confidentiality as one of the most important principles. The principle is generally governed by both the 2013 Constitution and the Civil Code, as the private life, personal secrets, and family secrets of a person are considered "inviolable" and shall be "ensured and kept confidential".[58] The laws regulating the processing of personal data in many specialized areas such as information technology, financial, health and consumer protection also seek to secure personal data in exchange, transmission, or storage, sometimes by introducing specific procedures.[59] Processors are responsible for ensuring network information security for the information (of

[53] Article 2 Draft PDP Decree.
[54] Article 37 GDPR.
[55] Article 11.3 PDPA.
[56] Article 23 Singapore PDPA.
[57] Article 3.4 of the Draft PDP Decree.
[58] Article 38 Vietnamese Civil Code 2015.
[59] Article 72(1) of the 2006 Law on Information Technology. Article 14 of the 2010 Law on Credit Institutions. Article 6 of the 2010 Law on Consumer Protection.

individuals) they process and taking technical measures to prevent cyber attacks.[60] In other areas outside those specialized laws' scope, it is unclear whether all processors are required to conduct accordingly, and how exactly they should comply with the Civil Code's general requirement. The Draft Decree is expected to strengthen this protection by introducing two similar principles, namely "the security principle" and "the confidential principle", combinedly require that personal data shall be protected and kept confidential by data protection measures,[61] and the processors shall prevent any unauthorized access, copying, alteration, deletion in processing personal data.[62]

In case of data breaches, Vietnamese cyber laws do obligate the processors to notify data subjects and the relevant authorities, such as the Cyber Security Department of the MPS.[63] However, such an important obligation is not furthered in the Draft Decree, although this Decree still obligates the relevant parties to notify PDPC of "any law violation" related to personal data protection activities.[64] It is also unsure whether all types of breaches, regardless of their seriousness, shall be notified and when exactly. In comparison, the Singapore PDPA goes further by incorporating the whole part 6A for a specific definition of data breach and the required steps to deal with such an incident. For instance, organizations have to notify the PDPC no more than 3 calendar days after discovering that a data breach is "notifiable" and the notification obligation shall be fulfilled.[65] The degree of notifiability will be particularly calculated based on the breach's scale (typically more than 500 individuals) and its "significant" consequences to the relevant individual.[66]

Fifth, the "*Access and Correction*" principle in AFPDP requires the organizations to provide individuals with the right to access their data and the right to correct errors timely. Vietnamese privacy laws recognize this principle, as the Network Information Security law allows data subjects to request processors to update, edit, delete their personal data or stop to share such with any third party.[67] The Draft Decree re-emphasizes this by introducing that personal data must be "updated" and "complete" to "ensure data processing purposes".[68] Data subjects can request the processors to access, edit, and delete their personal data, and may complain to the PDPC if their requests were denied and could claim for compensation.[69] However, it is unclear when and to what extent the processors shall react to those requests. In comparison, requests of data subjects in Singaporean PDPA should be responded "as soon as reasonably possible", and each type of request (access, correction, preservation, or deletion) is specifically regulated.[70] Given that these rights are both critical to the data subjects for securing their legitimate interests and troublesome to organizations to proceed, they should be specified in detail to prevent abusive application.

Sixth, the "*Retention*" principle of AFPDP expresses the organization's obligation to cease to retain documents containing personal data when they are no longer necessary. Article 18.3 of the Vietnamese Network Information Security also requires processors to destroy stored personal

[60] Article 16 of the 2015 Law on Network Information Security, Article 19.2 and 41 of the 2018 Cyber Security Law
[61] Article 3.6 and 3.8 of the Draft PDP Decree.
[62] Article 17.2 of the Draft PDP Decree.
[63] Articles 21.3, 21.4, and 24.3 of the 2018 Cyber Security Law.
[64] Article 28.3 of the Draft PDP Decree.
[65] Article 26D of the Singapore PDPA.
[66] Article 26B of the Singapore PDPA.
[67] Article 18 of the 2015 Network Information Security.
[68] Article 3.5 of the Draft PDP Decree.
[69] Article 5.4 of the Draft PDP Decree.
[70] Part 5 of the Singapore PDPA.

information after the purpose of use has been completed or the storage period expires and notifies the subject of personal information. This approach might be partially observed in the Draft Decree, as the processors shall delete personal data when such storage is no longer necessary for the processors' activities,[71] and must stop processing when the data subject dies with few exceptions.[72] However, as the degree of necessity has yet to be cleared and a declaration of unnecessary by processors is very occasional, it is rare to observe an obligation as such to be fulfilled. In this regard, the "reasonable" concept in Article 25 of the Singapore PDPA might serve as a helpful solution. Accordingly, deletion shall be conducted as soon as it is "reasonable" to assume that the notified purpose is unnecessary or no longer being served. Such a reasonableness standard is "evolutionary" and will be determined based on what an ordinary person would consider appropriate in the similar circumstances.[73]

Seventh, the AFPDP's "*Transfers to Another Country or Territory*" principle requires organizations to obtain the consent of data subjects for an overseas transfer or to ensure the receiver will protect the data carefully per other mentioned principles. The Singapore PDPA strictly upholds this requirement by obligating the organizations to not transfer to overseas parties unless evidence showing that such parties can meet PDP standard equivalent to Singaporean PDPA requirements.[74] Conditions for proving as such are: the overseas recipient is bound by legally enforceable obligations (laws, contracts, binding corporate rules, etc.), or specified certifications[75] to ensure a standard of protection comparable to the Singaporean PDPA's.[76] In comparison, cross-border transfer of personal data has not been fully regulated by Vietnamese privacy laws, as there is only requirements on data localization but not on transferring data to abroad receivers.[77]

The Draft Decree may fill in this gap by strongly regulating that cross-border transfer of personal data of Vietnamese citizens shall only be allowed after fulfillment of all these specific conditions: (i) being duly notified to and consented by the data subject,[78] (ii) original data is localized in Vietnam, (iii) the destination shall have data protection standards equivalent to Vietnamese's, and last but most troublesome, (iv) obtaining the written approval of the PDPC. While Article 21.3 of this Decree opens a small back door that the (iii) condition might be skipped if the processors show their commitment to protect personal data by applying data protection measures, the other conditions are still much stricter than that of the Singaporean. While the Singaporean PDPA allows data collectors and processors to determine the PDP equivalent standards themselves and focuses on ex-post checking, the Vietnamese's Draft PDP Decree introduced a rigid ex-ante checking as each cross-border transfer of Vietnamese's personal data shall meet all paperwork conditions above. Furthermore, the Vietnamese PDP Committee (PDPC) will also have a minimal number of part-time members for issuing approvals, which usually does not exceed 06 comrades. These

[71] Article 16 of the Draft PDP Decree.
[72] Article 9 of the Draft PDP Decree.
[73] Article 9 of the PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act, 23 September 2013, revised 1 October 2021.
[74] Article 26 of the Singapore PDPA.
[75] This refers to certifications such as: Asia Pacific Economic Cooperation Cross Border Privacy Rules System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors System.
[76] Article 19 of the PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act, 23 September 2013, revised 1 October 2021.
[77] Article 26.3 of the 2018 Law on Cyber Security and Article 26 of the Decree 53/2022/ND-CP.
[78] Article 11 of the Draft PDP Decree.

features both lead to concerns about their ability to timely process cross-border data transfer applications, especially when businesses in Vietnam are promoting digital transformation and conducting many international exchanges.[79]

2.2.3. Enforcement

There has yet to be any single regulator in data protection law enforcement in Vietnam. The central authorized governmental bodies in regulating and enforcing PDP law in private matters are both Ministry of Public Security (MPS) and the Ministry of Information and Communications, as the former considers cyber security and the latter oversees data privacy.[80] However, the specific duties of those bodies and their interaction with other state bodies in regulating and enforcing PDP laws are unclear. This might be a reflection of the 'Ministry model' of data protection in China and Taiwan, as these countries refuse to introduce specialized data privacy bodies, and enforcement responsibilities are spreaded to the relevant authorities in each relevant sector.[81]

Alongside such an administrative procedure, Vietnamese data subjects can claim compensation for personal data breaches following the civil procedure for tort,[82] or may report to relevant authorities following a criminal procedure. However, it is less likely that plaintiffs might successfully be compensated in their tort claims, as it is challenging to prove that a single data leak straightly led to any "direct" and "actual" damages.[83] In addition, victims are required to take the onus of proof that the alleged tortfeasor violated a particular clause in the laws (unlawful act)[84]. Given that the PDP regulations have not been fully formed and did not clearly impose specific obligations on data collectors and processors, it is troublesome to point out which particular act of them violates any given clause in the law. Vietnamese criminal law also imposes punishments on persons committing a crime relating to personal data if such may inflict serious consequences.[85] For instance, exchanging or publishing private information without the data subject's consent shall be subject to a fine of up to VND 200 mil (approx. USD 8600) or a prison term of 6 months to 3 years.[86] One may observe that this fine is not severe enough to correspond to the data intrusion's seriousness. It is also rare to observe any practical applications of this clause, which might be due

[79] Mai Phuong, "Highlights in the content of Draft Regulations on the protection of personal data" (*NHQuang&Associates, Brief Report*, 2021) 5.
[80] Article 36 and 38 of the 2018 Cyber Security Law, Article 52.2 of the 2015 Law on Network Information Security.
[81] Graham Greenleaf, "Vietnam: Data privacy in a communist ASEAN state" (2021) 170 Privacy Laws & Business International Report, 1, 6.
[82] Article 13 and 584 of the 2015 Civil Code.
[83] Article 585 of the 2015 Civil Code.
[84] Article 584 of the 2015 Civil Code and Resolution No. 03/2006/NQ-HĐTP issued by Justice Council of the Supreme People's Court, 08 July 2006.
[85] For instance, gaining illicit profits of between VND 50 mil and under VND 200 mil, or causing damage from VND 100 mil to under VND 500 mil, or causing negative public condemnation, ruining the reputation of agencies, organizations or individuals.
[86] Article 288 of the 2015 Criminal Code and Article 8.3 of the Joint Circular No.10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC on the Application of the Criminal Code provisions.

to several legal issues making the case unable to be criminally handled,[87] such as the difficulties in the calculation of the illegal profits and the victim's actual damage.

Therefore, the Draft PDP Decree will play an important role as a game-changer in this matter, as it will initially establish a single regulator in Vietnam - the PDP Committee (PDPC) – incorporated in the MPS.[88] PDPC shall protect the rights of data subjects, prevent any misuse of personal data, and ensure compliance with legal regulations. Individuals may complain to the PDPC in case of a data breach, or a violation of their rights over personal data occurs. In return, the PDPC can conduct appraisals of processors's PDP policies, and most importantly, can request the Director of the Department of Cybersecurity and High-Tech Crime Prevention of the MPS to suspend or terminate the process of personal data of processors violating relevant regulations, or cancel the granted certificate for processing sensitive data or cross-border data transfer.[89] A fine up from 50 to 100 million VND, or even 5% of the total turnover of all business in Vietnam might also be imposed.[90]

For comparison, the "robust" PDPC in Singapore shares certain similarities with the Vietnamese PDPC model. The Singaporean PDPC is designed to, *inter alia*, facilitate the resolution of an individual's complaint relating to an organization's PDPA contravention, to ensure the organization's compliance or application of appropriate corrective measures timely per PDPA obligations.[91] For such purposes, the Sing's PDPC is empowered with many powers, including: (i) to resolve the complainant's complaint; (ii) to review organizations' replies to the individual's data-related request; and (iii) investigate organizations of their compliance with the PDPA. After discovery of a PDPA violation, the PDPC may take certain measures to ensure obeyance, such as ordering to stop collecting, processing, disclosing data, destroying collected data, or to fine up to S$1 mil (in practice, the fine of around S$10K-30K is often imposed).[92] Parties can also appeal PDPC's decisions at the Data Protection Appeal Panel and later to the District Court. This model has proved its effectiveness as from January 2022 until now, the PDPC has issued 25 decisions on PDP compliance of various organizations, mostly ending up with a financial penalty imposition of around S$10K to even S$60K.[93] This might give rise to an expectation of the Vietnamese government to adopt a very similar model of PDPC, as other enforcement remedies following civil and criminal procedures are now available but not effective in this particular field.

3. Conclusion and further suggestions

Several points should be made after the above examination of current Vietnamese PDP laws under AFPDP principles and comparing them with the Singaporean PDP system. The *status quo* of

[87] Thi Cam, "The rampant situation of buying and selling personal information in Vietnam", *The People's Prosecutor Online* (Hanoi, 2018), accessed on 13 November 2022, at <https://kiemsat.vn/tran-lan-tinh-trang-mua-ban-thong-tin-ca-nhan-50866.html>.
[88] Article 23 of the Draft PDP Decree.
[89] Article 24 of the Draft PDP Decree.
[90] Article 22 of the Draft PDP Decree.
[91] Singapore PDPC's 2016 Advisory guidelines on enforcement of the Data Protection Provisions, issued 21 April 2016, 4-5. Detailed functions of the PDPC are specified in Article 6, part 2 of the PDPA.
[92] Singapore PDPC's 2016 Advisory guidelines on enforcement of the Data Protection Provisions, issued 21 April 2016.
[93] Singapore PDPC, "All Commission's Decision" (*PDPC Official Website*, 2022) accessed on 14 November 2022, at <https://www.pdpc.gov.sg/All-Commissions-Decisions>

Vietnamese PDP laws might not sufficiently deal with the urgent need for personal data protection in Vietnam. Vietnamese PDP regulations are currently dispersed amongst various laws in many specialized areas, as there has yet to be a comprehensive all-in-one PDP guidance. The provisions provide several core principles and regulations but are typically too generic and not ready for direct application. In light of the AFPDP core principles, Vietnamese PDP regulations generally fulfill some principles (for instance, "Consent, Notification and Purpose" and "Security Safeguards"), but fail to meet other important ones (such as "Access and Correction", "Transfers to Another Country or Territory", or most importantly, "Accountability"). Therefore, codification and harmonization towards ASEAN's standards are both in need, given that the Vietnamese digital economy is surging remarkably, many Vietnamese individuals have begun to participate in digital transformation,[94] while their personal data are not effectively protected.

In this regard, introducing a Draft Decree by the MPS should be considered a lifesaver to the fragmented PDP system in Vietnam. There might be several concerns about the completeness of the Draft Decree and whether the Draft Decree might *de facto* serve as an umbrella and effective legal document for PDP in Vietnam. However, it is undeniable that applying such a Decree will act as the most suitable short-term solution, which may set up the core framework for Vietnamese PDP law and remarkably raise the standard of protection towards AFPDP's requirements. Therefore, the article suggests that more resources should be poured into the drafting and consultation process of such a Draft Decree to faster its finalization process.

However, the above short-term solution should not obscure the need for a comprehensive all-in-one statute on PDP in Vietnam. The making of such a law should, first and foremost, clarify the general approaches of Vietnam in regulating issues relating to personal data protection. In this regard, the Singaporean dual objectives should be referred to as a successful example: both the individual's rights of PDP and the businesses' interest in data development should be upheld and weighed. This dual-objective approach is vital to the law-making of PDP law in many ways. Skipping to consider the businesses' interests might lead to over-protective PDP regulations and unnecessarily block the growth of the digital data market. Secondly, this dual-objective approach should also shape the design of each PDP provision. For instance, several important concepts balancing the conflicting interests of various stakeholders (between data subjects and processors), such as the reasonable concept and the ex-post checking requirements for cross-border data transfer in Singaporean PDPA, should all be considered for incorporating into Vietnamese law. For a future orientation, the definition of "personal data" and its coverage should be clarified precisely for both PDP aims and further discussion of data propertization/ownership. This balanced but more complex approach thus requires more active engagement in law-making of many other important stakeholders. For instance, the National Assembly, other ministries enforcing private and business laws, and other relevant organizations should actively participate in the regulation of PDP law, to ensure the balance between protective and business-friendly features of the law.

(8000 words)

REFERENCES

1. Kearney, *ASEAN Digital Revolution* (Report, 2020).

[94] Truong Thi Hien, "Vietnam promotes digital economy development" (2022) The Communist Review, 8/2022.

2. Vietnam National Television, "Strategy to promote digital innovation and digital economy in Pacific Asia", Report on Huawei APAC Digital Innovation Conference 2022 (VTV Official Website) accessed on 10 November 2022, at < https://vtv.vn/cong-nghe/chien-luoc-thuc-day-doi-moi-ky-thuat-so-va-nen-kinh-te-so-khu-vuc-chau-a-tbd-2022052010413274.htm>
3. Sri Handayani Nasution, *Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025* (Policy Paper, No. 46, Center for Indonesian Policy Studies, 2021).
4. Vmware, *Carbon Black Singapore Threat Report 2020* (Vmware Report, 2021).
5. Nikkei Asia, "Thailand's cybersecurity negligence causes personal data breaches", *Nikkei Asia* (Bangkok, 2021) at https://asia.nikkei.com/Business/Technology/Thailand-s-cybersecurity-negligence-causes-personal-data-breaches. Le Hiep, "Minister of the MPS: 1.300GB personal data of Vietnameses are traded online", *Thanh Nien Online* (Hanoi, 9 Aug 2022) accessed on 15 Nov 2022, at < https://thanhnien.vn/bo-truong-cong-an-1-300-gb-du-lieu-ca-nhan-nguoi-viet-bi-mua-ban-tren-mang-post1486332.html>
6. World Bank, *The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth* (Report, 2019) p17.
7. Michael Schaper, "The Missing (Small) Businesses of Southeast Asia" (*Perspective*, *Yusof Ishak Institute*, *Singapore*, Issue: 2020, No. 7922, July 2020) accessed at <https://www.iseas.edu.sg/wp-content/uploads/2020/06/ISEAS_Perspective_2020_79.pdf>
8. Sanchita Basu Das, "An ASEAN Single Digital Market? Small Beginnings, Great Endings" (*Yusof Ishak Institute, Commentaries*, 7 March 2018) accessed on 12 Nov 2022, at <https://www.iseas.edu.sg/media/commentaries/to-an-asean-single-digital-market-small-beginnings-great-endings-by-sanchita-basu-das/>
9. Graham Greenleaf, "Vietnam: Data privacy in a communist ASEAN state" (2021) 170 Privacy Laws & Business International Report, 1.
10. Mai Phuong, "Highlights in the content of Draft Regulations on the protection of personal data" (*NHQuang&Associates, Brief Report*, 2021).
11. ZICO Knowledge Management, *Personal Data Protection in ASEAN* (*ZICO ASEAN Insider Series*, Sep 2020).
12. Chu Hồng Thanh, "Legal awareness of privacy", in *Privacy Rights* (National Politics Publishing House, Hanoi, 2018) 134.
13. Vu Cong Giao, Le Tran Nhu Tuyen, "Protection of rights to personal data in international law and some countries' legislation and valuable reference for Vietnam" (2020) 09 Journal of Legislative Studies 409.
14. Duong Kim The Nguyen, Huynh Thien Tu, Le Thuy Khanh, Mai Nguyen Dung, "Reforming the current privacy laws to meet the needs of personal data protection in digital transformation", in *University of Economics HoChiMinh City Series, Chapter* 7 (UEH Publisher, 2021).
15. UDHR, Refworld, CCPR General Comment No 16, 1988.
16. Singapore Personal Data Protection Committee (PDPC), "PDPA Overview" (*Official Website of the Singapore PDPC,* 13 November 2022) accessed at < https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

17. Hoa Chu, "Legal Framework for Personal Data Protection in Vietnam" in *Smart Cities in Asia Regulations, Problems, and Development* (SprinerBriefs in Geography, Chapter 8, 2021) 96.
18. Simon Chesterman, *Data Protection Law in Singapore* (2nd edn, Academy Publishing, 2018) 40.
19. Thi Cam, "The rampant situation of buying and selling personal information in Vietnam", *The People's Prosecutor Online* (Hanoi, 2018), accessed on 13 November 2022, at <https://kiemsat.vn/tran-lan-tinh-trang-mua-ban-thong-tin-ca-nhan-50866.html>.
20. Truong Thi Hien, "Vietnam promotes digital economy development" (2022) The Communist Review, 8/2022.
21. Nguyen Quynh Trang, "Law on protection of personal data in the context of AI development and other emerging digital technologies" (2022) 50 Journal of Law and Legal Practice 137.

Vietnamese legislations

22. Vietnamese Constitution 1946
23. Vietnamese Constitution 2013
24. Vietnamese Criminal Code 2015
25. Vietnamese Civil Code 2015
26. Law on Information Technology 2006.
27. Resolution 52-NQ/TW of the Vietnamese Communist Party's Politburo on policies for Active Participation in the Fourth Industrial Revolution, 27 Sep 2019.
28. Resolution No. 17/NQ-CP of the Vietnamese Government regarding certain key tasks and measures of development of the electronic government for 2019 – 2020 with a vision towards 2025, 7 March 2019.
29. Draft Decree on Personal Data Protection by Vietnam's Ministry of Public Security, published 9 February 2021.
30. Law on Promulgation of Legislative Documents 2015.
31. Law on Consumer Protection 2010
32. Law on Network Information Security 2015
33. Law on Digital Transactions 2005
34. Decree 52/2013/NĐ-CP on E-Commerce, 16 May 2013.
35. Law on Credit Institutions 2010
36. Law on Cyber Security 2018
37. Decree No. 117/2018/ND-CP of the Vietnamese Government on protection of confidentiality and provision of client information of Credit Institutions and Foreign Banks' Branches, September 11, 2018.
38. Law on Medical Examination and Treatment 2009
39. Joint Circular No.10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC on the Application of the Criminal Code provisions.
40. Resolution No. 03/2006/NQ-HĐTP issued by Justice Council of the Supreme People's Court, 08 July 2006.

Overseas legislations and guidelines

41. ASEAN Digital Masterplan 2025.

42. ASEAN Framework on Personal Data Protection by the Telecommunications and Information Technology Ministers Meeting, 25 November 2016.
43. Regulation (EU) 2016/679, General Data Protection Regulation of the European Union.
44. Singapore Personal Data Protection Act 2012.
45. Singapore PDPC's 2016 Advisory guidelines on enforcement of the Data Protection Provisions, issued 21 April 2016
46. PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act, 23 September 2013, revised 1 October 2021.
47. Singapore PDPC, "All Commission's Decision" (*PDPC Official Website*, 2022) accessed on 14 November 2022, at <https://www.pdpc.gov.sg/All-Commissions-Decisions>