Vietnam: Data privacy in a communist ASEAN state

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

(2021) 170 *Privacy Laws & Business International Report*, 1, 5-8

Vietnam is a 'socialist market economy' under the firm control of the Community Party.[1] It is a significant and active member of the Association of South-East Asian Nations (ASEAN), one of two such ASEAN members[2] that are one-party communist states. Vietnam has been a World Trade Organisation (WTO) member since 2007, is an APEC member economy, a party to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), and a signatory to the Regional Comprehensive Economic Partnership (RCEP).[3] Its economy is ranked 37th by GDP, flanked by Hong Kong and Denmark,[4] so it is of considerable economic weight in Asia.

Vietnam has since 2006 gradually developed a range of data privacy protections in its e-commerce and consumer laws, to the level of the OECD Guidelines (or APEC Framework) by 2014.[5] Since then the 2016 *Law on Cyber-Information Security* (CISL), a highest-level law enacted by the National Assembly, expanded existing protections into the single most detailed set of data privacy principles in a Vietnamese law, but with its scope limited to commercial processing and only in 'cyberspace', so it was not comprehensive.[6]

Vietnam is now proposing to enact a comprehensive data privacy law for the first time.[7] The Ministry of Public Security (MPS) released in February 20021 a draft *Decree on Personal Data Protection* ('Decree') for public consultation until 9 April. MPS aims to finalise the draft and submit it to the Government in time for it to come into effect on 1 December 2021 (art. 29). As a Decree made by the Government, it will not be made by the National Assembly, and therefore does not have the highest legislative status as a law, contrasting with the proposed comprehensive law in China.[8] The Decree states that it is made pursuant to the Law on Cyber Security of 2018 (see later).

An innovation is that the law creates a Personal Data Protection Committee (PDPC), located within the Ministry of Public Security (MPS).

---

[1] For background, see G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pgs 361-5.

[2] The other is the Lao People's Democratic Republic (Lao PDR, or Laos), which has a GDP only 5% of that of Vietnam, enacted the *Law on Electronic Data Protection* in 2017. It is a very ambiguous law, and its application to personal data is uncertain.

[3] G. Greenleaf ' Will Asia-Pacific Trade Agreements Collide with EU Adequacy and Asian Laws?' (2020) 167 *Privacy Laws & Business International Report* 18-21.

[4] As at March 2021 in Wikipedia: 'List of countries by GDP (nominal)'; The IMF ranking is used instead of the World Bank ranking or the UN ranking beause it includes Hong Kong and Taiwan, but otherwise there is little difference among the three.

[5] Greenleaf *Asian Data Privacy Laws*, pgs 368-74.

[6] C. Schaefer and G. Greenleaf 'Vietnam's Cyber-Security Law Strengthens Privacy… A Bit' (2016) 141 P*rivacy Laws & Business International Report*, 26-27<https://ssrn.com/abstract=2824405>. It defines 'cyberspace' so as to suggests that the scope also includes VPNs and possibly certain intranets.

[7] Draft *Decree on Personal Data Protection* (in Vietnamese) <http://bocongan.gov.vn/van-ban/van-ban-moi/lay-y-kien-gop-y-doi-voi-du-thao-nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-519.html>. This article relies upon a machine-based translation of this law, as no alternative is available. Ambiguities may be a result of machine-based translation.

[8] See G. Greenleaf 'China issues a comprehensive draft data privacy law' (2020) 168 P*rivacy Laws & Business International Report*, 1, 6-10.

Scope

The scope of the law is comprehensive, stating that it 'applies to agencies, organizations and individuals related to personal data' (art. 1), with some exceptions. Its application to the public sector differs from Singapore and Malaysia's 'private sector only' scope, but is consistent with China's proposed new law.[9] The scope of the law extends to anyone 'doing business in Vietnam' (art. 4.2), not only those located in Vietnam. It is unclear in some provisions if the text applies only to the data of Vietnamese citizens.

Other definitions are equally expansive. 'Personal data processor', the key party to determining the scope of the law, 'means an agency, organization or individual at home and abroad that performs personal data processing activities' (art. 2.8). Data controllers, and those who do processing for them, are both referred to as 'processors' (art. 2.8), and others who receive personal data are 'third parties' (art. 2.9). As a result, 'processors' (in GDPR terms) are subject to specific obligations.

'Personal data' is defined conventionally in terms of identifiability (art. 2.1), divided into 'basic' personal data, and 'sensitive' personal data.

Registration of sensitive data processing

'Sensitive' data is given a very extensive definition (art. 2.3) including most usual categories (political and religious opinions, health data, sexual orientation), genetic and biometric data (GDPR-influenced), as well as gender status and location data. Also included are categories that are potentially very broad, namely 'personal financial data', 'personal data about social relationships' and 'other personal data as specified by law to … need necessary security measures'.

The breadth of the definition is important because sensitive personal data must be registered with the PDPC (art. 20), by an application requiring extensive information about the proposed processing and its 'legal basis'. It must be accompanied by an 'impact assessment report' which will 'assess the potential harm to data subjects' and set out measures to deal with such potential harm'. The PDPC is to process applications within 20 days of receiving a 'valid' application. Commentators point out that just about all private sector processors will process 'sensitive' data within this wide definition, including its employee data. 'Not only will this impose significant costs on companies in terms of time, money, and human resources, but it is highly doubtful that the PDPC would have sufficient resources to process the expected volume of applications within the specified timeline,' they contend.[10]

There are exceptions to the registration requirements, almost entirely applicable to public sector bodies (involving crime, health care, social security, judicial functions, statistics etc) (art. 20.4).

Rights and obligations

Eight key principles of data protection are stated briefly (art. 3), requiring very strong data minimisation in collection, use and disclosure.[11] This does not amount to a definition of 'legitimate processing' (in GDPR terms) because the legitimate purposes are not specified. Nor do these principles describe the rights and obligations provided by subsequent articles.

---

[9] Greenleaf *ibid*.

[10] Giang Thi Huong Tran and Waewpen Piemwichai 'Vietnam Issues New Draft Decree on Personal Data Protection' Tilleke & Gibbins / Lexology, 25 February 2021.

[11] 'Personal data can only be obtained in necessary situations…; … can only be processed for the purpose that was registered or declared; ,,,, can only be obtained to the extent necessary to achieve the purpose set.' (art. 3).

The requirements for consent are relatively strict (art. 8), requiring substantial notice, stronger consent for sensitive data, that silence is not consent (positive affirmation required), that consent can be withdrawn, and that the onus of proof of consent is on the processor.

Processing must stop after a person dies, with few exceptions (art. 9). More strict conditions apply to processing children's data (art. 14), but the age limit is not set in this law. There is no general requirement that data must be automatically destroyed or anonymised once the purpose of collection is completed, only a right to request termination of processing (art. 5.4).

Processing personal data without the person's consent (including for secondary processing) is only allowed in various situations of public interest, emergencies, for statistics or research after de-identification, and where 'according to the provisions of law' (art. 10). One criticism of this last exception is that it is 'a loophole that is widely used in the legal system of Vietnam to give the government's executive branch, especially ministries, an almost unlimited ability to interpret laws and regulations using circulars and executive decisions'.[12] There are no 'legitimate interest' exceptions allowing such processing.

The processing of 'de-identified' data 'for scientific research or statistics' is allowed without the data subject's consent if (i) the data is encrypted or (ii) the data is replaced with a code, and 'the results cannot be re-synthesized' so as to identify individuals (art. 13.1-13.3). The PDPC must also given written verification that a set of protective measures has been complied with (art. 13.4). These provisions are not technologically neutral and risk becoming outdated.

Automatic processing of personal data during the performance of a contract requires the data subject's prior agreement (art. 13.1). All automatic processing requires notice (but not consent) 'made easy to understand' (art. 13.2 – 13.3). Other protections such as a right to contest fully-automated decisions are not provided.

Since 2018, Vietnam already has a data breach notification requirement, for companies covered by the *Law on Cyber Security* of 2018, requiring prompt notification of data breaches to the Cybersecurity department of the MPS, and for companies to notify users directly of such breaches. This Decree does not unambiguously include such a requirement, although the obligation to 'promptly notify' PDPC of 'violations related to personal data protection activities' (ar. 28.3) could have this meaning. Companies must therefore still refer to multiple laws.

Data exports and localisation

Vietnam currently has no explicit legislation on data export restrictions, but consent or government approval is required for overseas transfers.[13] A 2013 law required some businesses to have a server located in Vietnam, if state authorities so requested, which can be seen as a limited sectoral data localisation requirement. Vietnam enacted a controversial *Law on Cyber Security* ('CSL') in 2018 introducing data localisation requirements, but also imposing severe penalties on the publication of anything considered to be anti-State activities, which some commentators considered 'imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to customers in Vietnam'.[14] However,

---

[12] Trinh Huu Long '9 Takeaways From Vietnam's Draft Decree On Personal Data Protection' *Luat Khoa Magazine* 19 February, 2021 <https://www.thevietnamese.org/2021/02/9-takeaways-from-vietnams-draft-decree-on-personal-data-protection/>

[13] Waewpen Piemwichai *Jurisdictional Report – Vietnam* in C. Girot (Ed.) *Regulation of Cross-Border Transfers of Personal Data in Asia*, (ABLI, February 2018) , paras. 18-45 <http://abli.asia/PUBLICATIONS/Data-Privacy-Project>.

[14] W. Piemwichai and Tu Ngoc Trinh 'Vietnam's New Cybersecurity Law Will Have Major Impact on Online Service Providers', Tilleke & Gibbins, June 18 2018 <https://www.tilleke.com/index.php?q=resources/vietnam%E2%80%99s-new-cybersecurity-law-will-have-major-impact-online-service-providers>

the data localisation requirements of the CSL did not prevent data stored in Vietnam from being transferred overseas.[15] Nor did they explicitly require offshore providers' servers to be located in Vietnam,[16] and they are only applied *ex post facto* if breaches occur. These localisation provisions in the CSL (art. 26(3)) have been the subject of successive draft implementation decrees which are still incomplete.

This proposed Decree has detailed baseline data export requirements for the first time, although other sectoral laws may cover specific situations such as banking or health. Personal data 'of Vietnamese citizens' may only be transferred overseas when four conditions are satisfied (art. 21.1): (i) data subject consent to transfer; (ii) 'original data is stored in Vietnam' (one form of data localisation); (iii) documentary proof that the recipient destination has laws 'at a level equal to or higher' than Vietnam; and (iv) written approval from the PDPC. The required application documentation is specified (art. 21.7), and must include details of the sources of the data to be transferred, the purposes and legal basis of the transfer, and a 'report on impact assessment' including measures to reduce harms. The PDPC is supposed to complete processing within 20 working days (art. 21.8). The processor must store data transferred, consents etc, for three years (art. 21.4). The 'documentary proof' required for (ii) has three requirements (art. 21.2). The PDPC will evaluate each data transfer regime annually (art. 21.5).

Not surprisingly, business interests are very critical:

> 'It is apparent that these requirements in Article 21 could create a barrier to trade and the flow of data, and increase cost, time, and human resources requirements for companies across many industries. For example, there are a significant number of multinational companies operating in Vietnam that need to regularly process personal data, and they usually process such data in a selected country outside of Vietnam or use cloud services with physical servers located outside of Vietnam. This practice is very common for many industries, including e-commerce, banking, travel, education, health care, etc. If all companies sending personal data overseas have to store data in Vietnam, it would create huge costs and additional work and overhead for them. Moreover, the process for applying for approval from the PDPC would unavoidably delay transactions and data transfers, which usually need to be processed instantly.'[17]

Where it is not possible to meet the above requirements of art. 21.1, particularly the requirement that the destination has laws of at least equal standard to Vietnam, can instead satisfy alternative data export requirements (art. 21.3): (a) data subject consent; (b) written approval from PDPC; (c) commitment by the processor to protect the data; and (d) commitment by the processor to apply 'personal data protection measures'. The requirement that 'original data is stored in Vietnam' seems to be waived if these conditions are satisfied.

Given that article 21.1 only applies to personal data of Vietnamese citizens (unless this is a drafting error), it appears that transfers of data on foreigners must be dealt with under article 21.3.

---

[15] Piemwichai and Trinh, *ibid*: ''The adopted version of the law seems to relax these restrictions by requiring the online service providers to store the Vietnamese users' information within Vietnam for a certain period of time. However, during the statutory retention time, the law does not appear to expressly prohibit the online service providers from duplicating the data and transferring/storing such duplicated data outside of Vietnam.'

[16] Piemwichai and Trinh, *ibid*: 'However, by requiring offshore service providers to "store" Vietnamese users' information in Vietnam, the offshore service providers, as a practical matter, will likely need to locate servers in Vietnam, either by directly owning/operating the servers or leasing servers owned/operated by other service providers in Vietnam, to store such information'.

[17] Giang Thi Huong Tran and Waewpen Piemwichai *op cit*

Processors are required to stop transfers when: (a) transfer volumes exceed a set limit; (b) a data subject has difficulty protecting his interests; or (c) a processor or receiver cannot protect data (art. 21.6).

Data protection authority

The law creates a Personal Data Protection Committee (PDPC), located within the Ministry of Public Security (MPS), and comprised of 'no more than 06 comrades', working part-time, appointed by the government. Its Chairman is the Director of the MPS Department of Cyber Security and High Tech Crime Prevention and Control (art. 23). This may be a regarded as a 'separate' or 'specialised' DPA, up to a point, but it is certainly not an 'independent' one. PDPC has authority to hear complaints against government bodies, and it cannot possibly be regarded as 'independent' of them. However, PDPC is a separate and specialised data protection body, which can investigate and make findings against private sector companies and its role is a departure from the 'Ministry model' of data protection, still adopted in China and Taiwan. In these countries, there is no specialised

data privacy body, and responsibilities for enforcement sits with a diffuse array of sectoral ministries and telecommunications authorities.

The PDPC has a wide range of functions and duties (art. 24), with some of the more significant being:

- Individuals may complain to the PDPC where their personal data is compromised, or processed improperly, or where any of their rights are violated (art. 5.5), but not for all failures of data processors to comply with the law. But PDPC must ask the MPS to 'settle' complaints, require processors to change their practices, suspend or stop processing etc (art. 24.17). PDPC can therefore investigate, but only MPS has teeth.
- PDPC may request a unit of the Ministry of Public Security to inspect the data protection activities of a processor, and PDPC will be in the inspection team (art. 19).
- It will 'evaluate and rate' processors' 'personal data protection reliability' and publish the result on the National Personal Data Protection Portal (art. 24.7) which it operates. It sets the evaluation criteria (art. 25.2).
- It will evaluate the 'regulations' of each processor relating to data protection (art. 24.14).
- It operates the registration system for sensitive data processing, and cross-border transfers (arts. 24.16, 25), with the potential problems mentioned above.

Enforcement

A Department of the Ministry of Public Security (not the PDPC) has authority to impose administrative fines, and impose other penalties such as suspending particular types of processing (art. 22.6). Many violations are specified, with fines up to 100 million VND (US$4,333) (art. 22.1-22.2). In addition to specified fines, multiple violations 'with great consequences' may result in fines up to 5% of the total turnover of the business 'in Vietnam' (art. 4.3), for violations specified (art. 22.3). Data localisation may also be required under the CSL, if the MPS decides that a breach justifies this.

Individuals may 'claim compensation' for breaches of their personal data, in accordance with the law' (art. 5.6), but this would be before a court, not the PDPC.

Conclusions: Moderately strong (on paper) and potentially onerous

Overall, Vietnam's draft decree, if enacted, would constitute a strengthening of its data privacy laws. Its comprehensive scope, and inclusion of a 'specialist', though not independent, DPA, are significant moves toward global standards.

The Decree includes many of the requirements of the EU Data Protection Directive 1995, including some limits on automated processing, data minimisation, sensitive data protections, export limits based on the law of the recipient country, and individual access to the courts. In addition, the influences of the GDPR are seen in the inclusion of genetic and biometric data in sensitive data, and fines based on business turnover. Going beyond the GDPR is the inclusion of geographical location data in sensitive data.

However, the PDPC's largely discretionary powers over the approval of processing sensitive data, and over personal data exports, make the proposed Decree potentially onerous for foreign companies, with doubts that the PDPC will be able to process the volume of applications in the 20 days specified.

Information: Clarisse Girot (Asian Business Law Institute, Singapore) has provided very valuable comments, but all responsibility for content remains with the author.