Jurisdictional Report
SOCIALIST REPUBLIC OF VIETNAM

Reporter: **Waewpen Piemwichai**
Foreign Registered Attorney, Tilleke & Gibbins

A BACKGROUND INFORMATION

1 Currently, Vietnam does not have restrictions on international data flow. In general, business entities as well as individuals in Vietnam are allowed to transfer the personal information of their customers (and other data subjects, such as their employees, vendors and partners) outside of Vietnam, provided that prior consent from the customers/data subjects has been obtained.[1] In certain sensitive transactions, such as transfer of information classified as state secret or sensitive data under banking laws/regulations, in addition to consent from the customers/data subjects, the person transferring such information must also encrypt the information before the information can be transferred.[2]

2 Due to the significant increase in cyberattacks in Vietnam, which afflict thousands of network information systems and cause a loss of thousands of billions of Vietnam dong each year, the Ministry of Public Security ("MOPS") has recently drafted a Law on Cybersecurity ("Draft Cybersecurity Law") in order to stipulate principles and conditions for assuring the security of information and information systems in cyberspace, despite the fact that there are other existing legislation which deal with cyber incidents in Vietnam (such as the Law on Network

1 For example, Civil Code (No 91/2015/QH13) Art 38(2); Law on Information Technology (No 67/2006/QH11) Art 21(1); Law on Network Information Security (No 86/2015/QH13) Art 17(1)(a); Law on E-Transactions (No 51/2005/QH11) Art 46(2); Law on Consumer Protection (No 59/2010/QH12) Art 6(2)(b) and Decree No 52/2013/ND-CP on e-commerce (hereinafter "Decree 52") Art 70(1); *etc*.

2 See Art 16 of Decree No 33/2002/ND-CP on detailing the implementation of the Ordinance on the protection of state secrets and Arts 21(2) and 35(2) of Circular No 31/2015/TT-NHNN regulating safety and confidentiality of banking information technology systems (hereinafter "Circular 31").

Information Security[3] and Decree No 72/2013/ND-CP on management, provision and use of Internet services and online information ("Decree 72"), both of which are under the authority of the Ministry of Information and Communication).

3 The Draft Cybersecurity Law, among its other provisions, introduces the principle of data localisation[4] to Vietnam, requiring, in particular, that foreign enterprises (*ie*, companies incorporated outside of Vietnam) when providing telecommunication ("telecom") and Internet services in Vietnam must locate their representative offices, and any servers on which Vietnamese users' data are administered, within the territory of Vietnam. In addition, in respect of information systems critical to national security (defined vaguely as information systems which, when broken down or sabotaged, will affect national sovereignty, interests and security and seriously impact social order and safety), the owners of such information systems must store the personal information and critical data they have collected or created within Vietnam. If there is an obligation to provide any information outside of Vietnam, the information system owner must assess security levels as regulated by the MOPS or in accordance with other applicable legislation.

4 This Draft Cybersecurity Law has been widely criticised in Vietnam by the business community (including both Vietnamese and foreign business chambers/associations in Vietnam such as the Vietnam Chamber of Commerce and Industry ("VCCI"), American Chamber of Commerce and Asia Internet Coalition, *etc*) in that it imposes onerous measures and liabilities on telecom and Internet service providers. If the Draft Cybersecurity Law is promulgated as currently written, it would potentially impede the digital economy and the growth of telecom and Internet services in Vietnam as it prevents free flow of data.

3 No 86/2015/QH13.

4 "Data localisation requirements" may be broadly understood here as the prohibition against transfers of personal data without official approval or permit, even if data subjects have consented to the transfer.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing data privacy protections in national legislation*

5 The right to privacy (including informational privacy and all forms of exchange of personal information) and confidentiality of information is a fundamental right recognised by the Constitution of Vietnam (Article 21). Currently, there is no single comprehensive legal document regulating data privacy in Vietnam, but there are a number of laws and regulations that have provisions to protect personal data privacy. These laws include the Civil Code,[5] the Penal Code,[6] the Law on Information Technology[7] ("IT Law"), the Law on Telecommunications[8] ("Telecom Law"), the Law on Network Information Security, the Law on Consumer Protection,[9] the Law on E-Transactions,[10] Decree 72 on Internet services and online information and Decree No 52/2013/ND-CP on e-commerce ("Decree 52").

6 These laws provide a common key principle that the collection, processing and use of personal information must be consented to by the information owner,[11] and the use of such information must be in line with the purposes as notified and consented to. Transfer of personal information to a third party must be consented to by the information owner or at the request of a competent authority, or where the law provides otherwise. An information owner is entitled to request any organisation or individual storing their personal information in a network environment to check, correct or remove/delete such information; to supply to the information owner such information at their request; and to stop supplying their information to a third party at their request. The

5 No 91/2015/QH13.
6 No 100/2015/QH13.
7 No 67/2006/QH11.
8 No 41/2009/QH12.
9 No 59/2010/QH12.
10 No 51/2005/QH11.
11 For instance, Art 38 cl 2 of the Civil Code (Law No 91/2015/QH13) on "Right to Private Life, Personal Privacy and Family Privacy" provides that "the collection, storage, use, and publication of information related to the private life or personal privacy of an individual must have the consent of that person".

person/organisation collecting, processing or using personal information of another person must also notify the data subject if it cannot comply with their request for technical or other reasons.

7 There is no data localisation requirement under the current legislation (*ie*, the Civil Code, the Penal Code, the IT Law, the Telecom Law, the Law on Network Information Security, the Law on Consumer Protection, the Law on E-Transactions, Decree 72 on Internet services and online information and Decree 52 on e-commerce). Data can be transferred cross-border to and from Vietnam if prior consent of the data subject is obtained. However, as discussed above, if the Draft Cybersecurity Law is promulgated as is, it will be the first legislation introducing data localisation requirements in Vietnam. At the time of writing this report, the Draft Cybersecurity Law is in the process of being reviewed by the National Assembly (*ie*, the Legislature of Vietnam). The National Assembly is scheduled to vote on this Draft Cybersecurity Law in the middle of 2018.

8 As with the data privacy rules, the definition of "personal information" under Vietnamese law is broadly provided in different pieces of legislation. Personal information is generally defined as information contributing to identifying a particular individual, including, among other things, name, date of birth, home address, phone number, medical information, identity card numbers, social insurance card numbers, credit or debit card numbers, information on personal payment transactions and other information that the individual wishes to keep confidential. The phrase "other information that the individual wishes to keep confidential"[12] is problematic in that it seems to give complete subjective discretion to the owners of the information to determine what is considered "personal information".

9 While privacy rights are rather restrictive under statute, their enforcement as of now is extremely weak. Based on reports and this reporter's discussion with the Ministry of Justice, it is uncommon for Vietnamese courts to handle privacy infringement claims.

12 Decree 52 Art 3(13).

ii *International engagement*

10 Vietnam ratified the International Covenant on Civil and Political Rights ("ICCPR") on 24 September 1982, which entered into force for Vietnam on 24 December 1982. However, Vietnam has not taken action with regards to the Optional Protocol to the International Covenant on Civil and Political Rights. In addition, to date, Vietnam has entered into ten bilateral and multilateral free trade agreements ("FTAs"), some of which cover the provisions on transfer of personal data between Member States, such as the Trans-Pacific Partnership ("TPP") which includes provisions for privacy and limitations on data localisation.

11 In theory, if there are conflicts between the provisions in the FTAs and the provisions in Vietnam's domestic law, the provisions in the FTA could override the latter if one of the concerned parties is a foreign individual or entity. In particular, the Law on Promulgation of Legislative Documents specifies that "in case a Vietnam legislative document, other than the Constitution, and an international treaty of which the Socialist Republic of Vietnam is a member contain different regulations on the same issue, the international agreement shall apply".[13] Vietnam's Civil Code also provides that "where an international treaty of which the Socialist Republic of Vietnam is a member regulates the rights and obligations of parties to civil relations involving a foreign element, such international treaty shall apply". The Commercial Law[14] reinforces that "the rights and obligations of enterprises with foreign-owned capital shall be determined in accordance with the law of Vietnam or international treaties of which the Socialist Republic of Vietnam is a member". As the receiver of cross-border data transfers is an organisation or individual residing outside of Vietnam, the provisions in the FTA could override the restrictions on cross-border data transfers in Vietnam's domestic law in cases of conflict.

12 Vietnam is a Member economy of the Asia-Pacific Economic Cooperation ("APEC"). However, Vietnam has not yet participated in the APEC Cross-border Privacy Enforcement Arrangement ("CPEA").

13 Law on Promulgation of Legislative Documents (No 80/2015/QH13) Art 156(5).
14 No 36/2005/QH11.

According to a report published by APEC in January 2017, Vietnam is among six jurisdictions considering joining the APEC Cross-Border Privacy Rules ("CBPR") system in the near future; however, the time when Vietnam will join the system was not reported.

13 With respect to Vietnam's position on the Consultative Committee of the Council of Europe Convention 108, a meeting on cybercrime and data protection organised by the Franco-Vietnamese House of Law was held on 18–19 November 2009 in Hanoi, in which the Council of Europe contributed to a regional colloquium on the legal issues of the development of information and communication technologies. Participants from Vietnam, Cambodia, Laos and Thailand discussed amendments to the Penal Code which defined additional cyber-offences as well as further reforms that were envisaged for 2010 and 2011 to bring Vietnamese legislation in line with the Convention on Cybercrime. The event also created awareness of the need for data protection standards such as those of the Council of Europe's Convention on the Protection of Personal Data (CETS 108 and 181). Except for such meeting, there does not appear to be any other publicly accessible information on Vietnam's intention of admission to the Consultative Committee of the Council of Europe Convention 108.

14 Vietnam has not been recognised by the European Union as offering an adequate level of protection under Article 25(6) of Directive 95/46/EC, and has never submitted an application to that effect.

15 It is probable that as a result of the extraterritorial reach of the European General Data Protection Regulation ("GDPR"), European businesses which have subsidiaries in or business transactions concerning Vietnam will audit and implement their internal rules and procedures on data processing to comply with the GDPR, although this regulation is stricter than the data protection regulations in Vietnam.

iii *Competent authorities in area of data protection and cross-border data transfers*

16 As discussed above, there is no single comprehensive legal document regulating data protection in Vietnam, but there are a number

of laws and regulations that have provisions to protect personal data privacy.

17 The government bodies having the power to enforce data protection in Vietnam vary depending on the sector in which the data protection activities are involved. For example, the Ministry of Information and Communications ("MIC") has the power to examine, inspect, settle complaints and denunciations, and handle data privacy violations in relation to the telecom, Internet and information technology ("IT") sectors.[15] The Vietnam e-Commerce and Information Technology Authority ("VECITA"), an organisation under the Ministry of Industry and Trade, has the power to handle data privacy violations in relation to the e-commerce sectors. VECITA is responsible for the state management of e-commerce activities in Vietnam, including guiding, licensing, monitoring and controlling the operation of e-commerce activities in Vietnam.[16] The State Bank of Vietnam has the power to handle data privacy in the banking sector.[17] The Ministry of Public Security has the power in relation to state secret protection, cybercrime, national security, social order and security. Finally, the investigation agencies of the People's Police are empowered with wide authority to request the supply of information from organisations and individuals for investigation purposes.

15 Law on Telecommunications (No 41/2009/QH12) Art 9(2)(dd); Law on Information Technology (No 67/2006/QH11) Art 10(1); Decree No 72/2013/ND-CP on management, provision and use of Internet services and online information Art 39(1)(d); Law on Network Information Security (No 86/2015/QH13) Art 27(2)(a).

16 Decree 52 Arts 6(1), 77 and 78(5).

17 Law on Credit Institutions (No 47/2010/QH12) Art 159. In respect of the provision on data privacy, Art 14(3) of the Law on Credit Institutions provides that credit institutions and foreign bank branches shall not be permitted to provide information to any other organisation or individual about accounts, deposits, deposited assets or transactions of clients conducted at such credit institution or foreign bank branch, except when requested by a competent state body in accordance with law or when the client consents.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

i *Default position*

18 Based on the current legislation, there is no specific requirement with regards to international data transfers. International transfer is authorised when prior consent of the data subject is obtained, or when the transfer is made in accordance with the transferor's obligation under Vietnamese law (such as by court order or at the request of the competent authorities).

ii *Additional requirement to consent in banking sector*

19 In addition to the consent requirement, in the banking sector, data on client passwords and password users and other sensitive information (*ie*, data containing classified matter, information restricted to internal circulation within the entity, or information which the entity manages and which, if leaked, could have an adverse impact on the reputation, finances or activities of such entity) must be encrypted and protected when transferred, regardless of whether they are domestically or internationally transferred.[18] This encryption requirement also applies to transfer of information classified as state secret.

20 There is no restriction on the location of the transferee of data.

iii *No difference in legal qualification between roles*

21 Vietnamese law does not distinguish the roles relating to data processing into data controller, processor or intermediaries. According to Vietnamese law, every person involved with the collection, process, use, storage, transfer, disclosure and publication of personal information needs to obtain prior consent from the data subject.[19]

---

18 Circular 31 Art 35(2).

19 Civil Code (No 91/2015/QH13) Art 38(2); Law on Information Technology (No 67/2006/QH11) Art 21(1); Law on Network Information Security (No 86/2015/QH13) Art 17(1)(a); Law on E-Transactions (No 51/2005/QH11)

(*continued on the next page*)

iv *Exemption from obligation to obtain consent for certain types of data*

22 Consent, however, may be exempted for the following:

(a) collection of personal information already published on e-commerce websites;
(b) collection of personal information for signing, modifying or performing purchase and sale contracts for goods and services;
(c) collection of personal information for calculating prices or charges for use of information, products and services online; and
(d) collection of personal information for performing other obligations in accordance with the law.

D LEGAL BASIS

23 The individual's consent is always necessary to transfer their data, irrespective of the implementation of data transfer mechanisms by the data exporter and/or the data importer. However, except for consent which is required to be obtained by e-commerce websites (for which the law clearly requires express consent from information owners in the form as prescribed by law), generally, other data privacy laws/regulations do not require a specific form in which the consent must be given. Consequently, it is unclear as to whether the consent must be express (*ie*, opt-in) or whether a notice and lack of objection would suffice.

24 If the data will be transferred electronically, the IT Law, which is the law governing the use of IT in a network environment (including providing, transmitting, collecting, processing and exchanging information via an information infrastructure, such as telecom networks, the Internet, computer networks and databases),[20] requires that the person collecting, processing or using personal information of another person must notify such person of the form, scope, place and purpose of the collection,

Art 46(2); Law on Consumer Protection (No 59/2010/QH12) Art 6(2)(b); Decree 52 Art 70(1); *etc*.

20 Law on Information Technology (No 67/2006/QH11) Arts 1, 4(3) and 4(4).

processing or use of their personal information. There is no statutory form or template for this notification.

25 In addition, the Law on Network Information Security further provides that if the information is collected, edited, used, stored, supplied, shared or dispersed in the network for "commercial purposes", the organisation or individual handling the personal information must develop and publicise their own policies applicable to handling and protection of personal information.[21]

26 These notifications and privacy policies are not required to be notified to or approved by the regulator, government or public entity.

E DATA LOCALISATION[22]

27 Based on the current legislation, Vietnam does not have data localisation requirements where the transfer of personal data is prohibited without official approval or permit, even if the data subjects have consented to the transfer.

28 However, data localisation requirements are introduced by the Draft Cybersecurity Law. If the Draft Cybersecurity Law is promulgated in its current version, foreign enterprises (companies incorporated outside of Vietnam), when providing telecom and Internet services in Vietnam, will be required to locate their servers on which Vietnamese users' data are administered within the territory of Vietnam. It is unclear under the Draft Cybersecurity Law whether such foreign enterprises need to physically store and keep all the data in Vietnam or whether they can just keep a copy of the data in Vietnam for possible government inspection (while the data can also be transferred across the border to be processed and stored outside of Vietnam).

21 Law on Network Information Security (No 86/2015/QH13 Arts 3(17) and 16(3).

22 "Data localisation requirements" may be broadly understood here as the prohibition against transfers of personal data without official approval or permit, even if the data subjects have consented to the transfer.

29 In addition, the Draft Cybersecurity Law further introduces that in respect of information systems critical to national security (defined vaguely as information systems which, when broken down or sabotaged, will affect national sovereignty, interests and security and seriously impact social order and safety), the owner of such information systems must store the personal information and critical data they have collected or created within Vietnam. If there is an obligation to provide any information outside of Vietnam, the information system owner must assess the security levels as regulated by the MOPS or in accordance with other applicable legislation. However, the Draft Cybersecurity Law does not provide the definition of "critical data", details on the assessment procedure, or the criteria to establish whether the security level is sufficient for transferring the data outside of Vietnam.

30 According to the Draft Cybersecurity Law, there is no exception to these data localisation requirements.

31 The Draft Cybersecurity Law is currently drafted to be applicable to Vietnamese agencies, organisations and citizens, and foreign organisations and citizens, directly involved in or connected to activities related to cyberspace (which is defined as the global network of information technology infrastructure, including the Internet, telecom networks, computer systems, and information processing and control systems, which is a special environment where humans perform social activities without being limited by space and time) and the protection of cybersecurity of Vietnam.

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

32 Vietnamese law does not specifically distinguish between the transfer of data within or outside of Vietnam. The rules for the transfer of personal information both within and outside Vietnam are the same. That is, organisations and individuals must refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the data owners or it is at the request of the proper state agencies.

33 The law generally does not require a specific form in which consent must be given. It is unclear whether consent must be affirmative or if implied consent is sufficient. However, Vietnam is a very formalistic jurisdiction. Thus, the recommended best practice is clear, affirmative opt-in consent, and a signature on paper is preferable. However, for electronic transactions, where it is impractical to obtain a signature on paper, consent may be obtained by a click-to-accept mechanism.

34 The person collecting, processing or using personal information of another person may only use and store the collected information for a certain time period as stipulated by law or as agreed upon by the data subject, and may not supply, transfer or disclose the information to any third party unless otherwise stipulated by law or agreed to by such person.

35 Vietnamese law does not specifically require transfer instruments that are compatible or promote interoperability between countries. In general, the law does not impose an obligation on the data exporter to ensure that the recipient is bound by legally enforceable obligations regarding the protection of the transferred data, except in certain specific industries like banking. Under the banking laws/regulations, there must be a written agreement before information is exchanged with any outside parties (regardless of whether the transfer is within or outside of Vietnam), specifying the legal responsibilities and obligations of the parties involved, including terms and conditions on dealing with breaches by the third party and its liability to pay compensation for loss and damage caused by breaches.[23]

36 The law generally provides that an individual shall be entitled to claim compensation for loss caused by a breach during the supply of personal information. However, it is unclear whether the data exporter must remain liable in the case of a breach by a data importer overseas.

23 Circular 31 Art 30(2).

ii *"Adequacy findings" and white lists*

37 Vietnamese law does not specifically require that data must only be transferred to jurisdictions that have laws establishing adequate or comparable data protection standards. A data exporter is free to assess the level of protection awarded in the country of destination. In general, there is no "black list" for jurisdictions (inside or outside Asia) which do not establish adequate or comparable data protection standards.

iii *Consent as exception to existence of privacy safeguards overseas*

38 Vietnamese law does not have requirements on privacy safeguards in the country of destination. However, the data importer/processor overseas must comply with the data protection rules under Vietnamese law when processing personal information of Vietnamese data subjects overseas. The data importer/processor overseas cannot obtain consent from the Vietnamese data subject to waive its obligations under the Vietnamese data protection rules.

iv *Other one-off exceptions*

39 Vietnamese law does not have requirements for privacy safeguards in the country of destination.

40 A data exporter cannot transfer personal information of data subjects in Vietnam to another person unless otherwise provided for by Vietnamese law or consented to by the data subject. The law does not provide explicit exceptions for cases where such information is necessary for the performance of a contract requested by the data subject or legal proceeding outside of Vietnam. It is worth noting that a foreign court's order requiring the data exporter to reveal personal information of data subjects in Vietnam requires recognition by a Vietnamese court through

a formal procedure pursuant to the Civil Proceedings Code before taking effect.[24]

v *Contracts*

41 As discussed above, except for certain specific industries like banking, it is not compulsory for a data exporter to conclude a contract with the data importer, irrespective of the status of the recipient (data intermediary, controller, *etc*). Other guarantees (CBPR certification, Binding Corporate Rules, *etc*) are also not compulsory.

42 Under the banking laws/regulations, there must be a written agreement before information is exchanged with any third parties (regardless of whether the transfer is within or outside of Vietnam) The agreement for transfer of information between the data exporter and the data importer must specify the legal responsibilities and obligations of the parties involved, including terms and conditions on dealing with breaches by the data importer and its liability to pay compensation for loss and damage caused by breaches.[25] It is not compulsory to include a third-party beneficiary clause for the benefit of the data subjects. There are no standard contractual clauses for this type of agreement.

vi *CBPR*

43 As discussed above, Vietnam has not yet participated in the APEC CPEA. According to a report published by APEC in January 2017, Vietnam is among six jurisdictions considering joining the APEC CBPR system in the near future; however, the time when Vietnam will join the system was not reported.

24 Principally, foreign court orders or judgments are generally unenforceable in Vietnam unless there is a judicial decision recognition treaty with the relevant country or the Vietnamese court enforces the foreign court's order/judgment on a reciprocal case-by-case basis (Art 423(1) of the Civil Proceedings Code (No 92/2015/QH13)).

25 Circular 31 Art 30(2).

44 As Vietnam does not have a comprehensive data privacy protection law, it is cautioned that there are various unresolved issues that need to be addressed before it can join the CBPR. The issues include, for example, which government agency would lead the application process or be responsible for enforcement of the CBPR, and how to structure the certification process to ensure its scalability to companies of all sizes. To address these issues and others, Vietnam may need to bring in a number of international experts, who have been significantly involved in either the creation or implementation of the CBPR system, or have other relevant experience in the governance of cross-border data flows, organisational accountability and data protection management, before the adoption of regulations to allow for such certification.

vii *Certification, trustmarks and privacy seals*

45 Certification, trustmarks and privacy seals are currently not compulsory under Vietnamese law.

viii *Other data transfer instruments*

46 Currently, there are no other accountability instruments or data transfer mechanisms compulsorily required under Vietnamese law.

G INTERNATIONAL CO-OPERATION BETWEEN PUBLIC AUTHORITIES WITH SECTORAL RESPONSIBILITIES IN DATA PROTECTION

i *Co-operation with foreign authorities in areas other than enforcement*

47 The law currently includes provisions that enable the Vietnamese authorities to develop operational co-operation with the authorities in other countries in this area of law.

48 For example, Article 6 of the Law on Network Information Security provides that:

> 1. International cooperation on network information security should abide by the principles as follows:

a) respecting the independence, sovereignty and territorial integrity of countries without intervention in internal affairs of the others, for equality and mutual benefits;
b) complying with Vietnam laws and international treaties to which the Socialist Republic of Vietnam is a state member.

2. Contents of international cooperation on network information security include:
   a) international cooperation on research and application of science, techniques and engineering of network information security;
   b) international cooperation in prevention and fighting illegal acts in relation to network information security, and against the abuse of information networks for terrorist acts;
   c) other international cooperation on network information security.

49 The Draft Cybersecurity Law also includes provisions that enable the privacy enforcement authority ("PEA") to develop operational co-operation with the PEAs in other countries. In particular, the Draft Cybersecurity Law states that:

1. Vietnamese organisations and individuals shall cooperate with foreign organisations and individuals or international organisations on cybersecurity in the principles of respecting national independence and sovereignty, non-interference in the internal affairs of each other, equality and mutual interests.
2. The contents of international cooperation on cybersecurity include:
   a) research on and analyses of cybersecurity trends;
   b) mechanisms and policies for further cooperation between Vietnamese organisations or individuals and foreign organisations or individuals or international organisations operating in cybersecurity;
   c) sharing of information and experience, and support in training, equipment and technology for cybersecurity assurance;
   d) prevention of and fighting against cybercrimes and acts prejudicial to cybersecurity, and the prevention of cybersecurity threats;
   e) training and development of cybersecurity human resources;
   f) organisation of international workshops, conferences and forums on cybersecurity;
   g) signing, entry into and performance of bilateral and multilateral international treaties and participation in regional and international organisations on cybersecurity; and

h) execution of international cooperation programs and projects on cybersecurity.

50 However, the Vietnamese authorities do not appear to have any bilateral or multilateral arrangements with the authorities of other jurisdictions to co-operate in the implementation of privacy laws.

51 In general, before the Vietnamese authorities adopt regulatory guidance or when making decisions that have a major impact on individuals and companies operating in Vietnam, they usually organise public consultations on the draft legislation and are open to comments from experts, businesses and organisations for insight into industry perspective and internal practice. However, the authorities do not have any statutory obligation to ensure regional or international consistency in their decision-making process, unless Vietnam is bound by regional or international commitments for such consistency.

ii *Enforcement of cross-border transfer restrictions*

52 Breaches of provisions on international data transfers or data localisation, depending on the nature and level of violation, may be subject to disciplinary or administrative treatment or penal proceedings, and to payment for any damage under current laws. However, it is worth noting that while the Vietnamese data protection and privacy rules are rather restrictive under statute, their enforcement as of now is extremely weak. Based on reports and this reporter's discussion with the Ministry of Justice, it is uncommon for the Vietnamese courts to handle privacy infringement claims.

53 There are small administrative penalties that might apply (the local equivalent of about US$450 to US$900) for an act of collecting, processing, using and transferring personal data without proper consent.

54 A breach of cross-border data transfer may also be subject to criminal sanction if:

(a) the transfer infringes secret information, mail, telephone, or telegraph privacy, or other means of private information exchange, for which the offender has already been disciplined or assessed with administrative penalty; or

(b) the transfer is associated with trading, exchanging, giving, changing, or publishing lawfully private information of an organisation or individual on a computer or telecom network without the consent of the information owner, provided that the offender earns an illegal profit of from VND50,000,000 to under VND200,000,000 (approximately US$900 to US$8,800) or causes property damage of from VND100,000,000 to under VND500,000,000 (approximately US$4,400 to under US$22,000) or damages the reputation of an organisation or individual.

55 The potential criminal sanctions range from a fine of VND20,000,000 to VND200,000,000 (approximately US$880 to US$8,800), a penalty of up to three years community sentence, being prohibited from holding certain positions for up to five years and imprisonment for up to three years. However, imprisonment penalties may be assessed only if: the offence is committed by an organised group; the offence involves abuse of the offender's position or power; the offence has been committed more than once; the obtained information is disclosed and affects another person's dignity or reputation; or the offence results in the suicide of the victim.

56 Relatedly, with regard to the risk of civil claims, it is uncommon for the Vietnamese courts to handle privacy infringement claims. The Vietnamese courts are limited to actual and direct losses, which often are out-of-pocket costs. Losses which are more difficult to prove are not usually awarded. A claimant who has suffered from a violation of data protection and privacy laws would need to prove their losses, which is difficult to do in practice. Given various factors, including the difficulties with litigation in Vietnam, a common scenario in many contexts is that would-be claimants might just ask for an apology or some form of negotiated monetary settlement.

57 The inspectorate division of an authority may initiate an investigation into a violation of the law or, more frequently, conduct an investigation when it is notified either by other government bodies, private sectors or news reports with high public visibility. However, to the best of this reporter's knowledge, no Vietnamese authority has ever taken action against a (national or foreign) controller based on the

conditions in which local data had been transferred to another jurisdiction.

iii *International enforcement by Vietnamese authorities*

58 Vietnam is a member of Interpol (International Criminal Police Organization), an international organisation facilitating international police co-operation. Interpol's National Central Bureau ("NCB") for Vietnam, which also serves as the MOPS's Department of Foreign Relations, is the primary law enforcement platform for Vietnamese police investigations requiring co-operation with other countries.

59 The NCB's principal responsibilities include:

(a) working with domestic, regional and international partners in developing events and programmes to boost Vietnam's ability to identify and prevent transnational crime;
(b) providing intelligence support to domestic law enforcement units when investigations require global outreach;
(c) co-ordinating the arrest and extradition of fugitives located in Vietnam, and of Vietnamese fugitives located in Interpol member countries; and
(d) working with all member countries for matters relating to mutual legal assistance on criminal matters and extradition.

60 Vietnamese domestic law currently does not include provisions for any of the following: transfer of complaints to the authorities in other jurisdictions; disclosure to the authorities in other jurisdictions of information obtained in investigations; assisting other authorities in cross-border investigations; or a prohibition on providing information to other enforcement authorities.

61 The Vietnamese authorities have not yet participated in any of the existing enforcement co-operation networks or arrangements on data protection and privacy (*eg*, GPEN, GPEN Alert and UCENet).

62 Vietnam does not have any bilateral arrangements with the PEAs of other countries to co-operate in the enforcement of privacy laws. However, Vietnam has co-operated with a number of PEAs in other

countries, including those from the US, the UK and China, in order to exchange intelligence and information and jointly investigate cases relating to cybercrime. Vietnam has also co-operated with its international counterparts in training and sending its officers to meetings, conferences and training courses.