asia counsel

in association with Kinstellar Southeast Asia

Data Protection Guide

First Edition

January 2026

Introduction

On 1 January 2026, Vietnam became subject to a new and substantially improved regulatory framework in relation to personal data protection (the "**VN-PDP Framework**"). This new VN-PDP Framework represents a significant step forward in Vietnam's continuing development into a sophisticated and internationally integrated jurisdiction, establishing personal data protection standards which are comparable to those prevailing in major and fully developed jurisdictions worldwide.

This Asia Counsel Vietnam Personal Data Protection Guide (the "**VN-PDP Guide**") sets out a clear and practical overview of the VN-PDP Framework and highlights the key obligations to which regulated persons and entities are subject when they:

- collect ("**Data Collection**") personal data from residents of Vietnam ("**VN Personal Data**");
- process VN Personal Data ("**Data Processing**"); and/or
- transfer VN Personal Data to other persons or entities, whether within Vietnam ("**Domestic Data Transfer**") or on an outbound cross-border basis to persons or entities located outside of Vietnam ("**Cross-Border Data Transfer**").

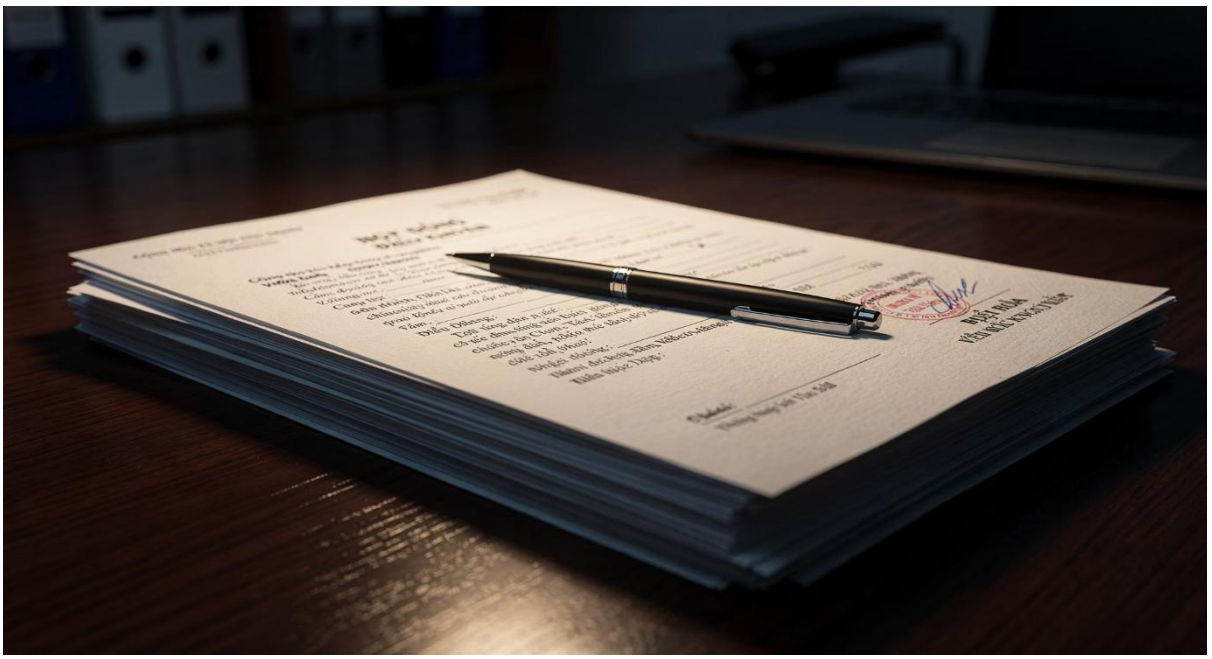
In this VN-PDP Guide, Data Collection, Data Processing, Domestic Data Transfer, and Cross-Border Data Transfer are referred to collectively as "**PDPL Regulated Activities**".

The key laws comprising the VN-PDP Framework

Prior to 1 January 2026, personal data protection in Vietnam was primarily regulated under Decree No. 13/2023/ND-CP ("**Decree 13**"), which came into force on 1 July 2023. Decree 13 was not the only legislative instrument in Vietnam containing provisions dealing with personal data protection and related matters. On the contrary, there were (and remain) numerous legislative instruments in Vietnam which deal to varying extents and from varying perspectives with VN Personal Data and related matters.

Decree 13, however, marked Vietnam's first major step towards comprehensive regulation in relation to personal data protection. Decree 13 established foundational principles and introduced key concepts such as:

- "basic" and "sensitive" personal data;
- mandatory consent for the collection and use of VN Personal Data;
- data subject rights;
- a 72-hour data breach notification window (commencing as from the time when the relevant breach occurred); and
- requirements for controllers ("**Data Controllers**") and processors ("**Data Processors**") of VN Personal Data to prepare and file with the Ministry of Public Security (the "**MPS**"), as applicable:
    - impact assessment dossiers for Data Processing ("**DPIA Dossiers**"); and/or
    - impact assessment dossiers for Cross-Border Data Transfers ("**DTIA Dossiers**").



In this VN-PDP Guide, we refer to:

- Data Controllers;
- Data Processors; and
- persons or entities who are both Data Controllers and Data Processors,

in each case, who collect and/or engage in any PDPL Regulated Activities in connection with any VN Personal Data, as "**PDPL Regulated Entities**".

With effect as from 1 January 2026, Personal Data Protection Law No. 91/2025/QH15 (the "**PDPL**") has superseded Decree 13 as the key legislative instrument which primarily regulates PDPL Regulated Activities in Vietnam. The PDPL (unlike Decree 13) is a fully fledged national law and gives rise to a regulatory framework which is of an international standard of robustness and sophistication and is broadly comparable to the European Union's General Data Protection Regulation framework (the "**GDPR**").

Key features of the PDPL include the following:

- Extraterritorial effect (noting that its provisions are applicable to any person or entity who engages in any PDPL Regulated Activities in relation to VN Personal Data, whether or not they reside or are incorporated in Vietnam).
- Mandatory appointment of a Data Protection Officer ("**DPO**"), which requirement is applicable to all PDP Regulated Entities.
- Specific rules and regulations applicable to "data-intensive sectors" – a concept which is not explicitly defined in the PDPL, but may reasonably be interpreted as including any sectors which rely heavily on the collection and processing of personal data, such as:
    - big data and analytics;
    - marketing and advertising;
    - artificial intelligence and machine learning;
    - cloud computing and platform services;
    - healthcare;
    - banking and finance; and
    - other data-intensive business sectors.
- A strict 72-hour data breach notification window (commencing as from the time when the relevant breach is detected by the relevant PDPL Regulated Entity – as opposed to the legacy Decree 13, under which the 72-hour notification window commenced at the time of the breach occurring).
- Tough sanctions for non-compliant PDPL Regulated Entities, particularly in relation to unlawful Cross-Border Data Transfers (which can give rise to penalties in amounts equivalent to up to the higher of 5% of the offender's previous year's revenue or VND3 billion (approximately USD120,000) – which may reasonably be interpreted as applying on a "per offence" basis).

In addition, on 31 December 2025, the Government of Vietnam issued Decree No. 356/2025/ND-CP, providing guidelines on the implementation of the PDPL ("**Decree 356**"). Decree 356 took effect concurrently with the PDPL on 1 January 2026 and formally supersedes and replaces Decree 13.

In this VN-PDP Guide, we refer to the PDPL and Decree 356 collectively as the "**Prevailing VN-PDP Law**".

Decree 356 sets out numerous specific and detailed obligations applicable to PDPL Regulated Entities, including in relation to the following matters:

1

DPO qualifications

Details as to the requisite qualifications and eligibility criteria for DPOs.

2

Compliance inspections

Procedures applicable to compliance inspections of PDPL Regulated Entities.

3

Dossier templates

Specific templates to be used and procedures to be followed in relation to the preparation and submission of DPIA Dossiers and DTIA Dossiers.

4

Reporting obligations

Specific compliance and reporting obligations and procedures to which PDPL Regulated Entities are subject.

Key principles

The PDPL sets out a broad and technology-neutral definition of the concept of "personal data", namely:

"Personal data is digital data or information in other forms that identifies or helps to identify a particular person, including basic personal data and sensitive personal data. Personal data, after deidentification, is no longer personal data."

This definition is broader and stricter as compared with the corresponding definition under the GDPR and on its face captures a significant scope of VN Personal Data which would clearly or arguably fall outside the scope of the corresponding GDPR definition.

The PDPL retains the core data processing principles which were established under Decree 13, including:

- the requirement for there to exist a lawful basis for engagement in PDPL Regulated Activities;
- limitation of purpose in relation to PDPL Regulated Activities; and
- the requirement for valid consent in relation to PDPL Regulated Activities.

In comparison to Decree 13, however, the PDPL significantly raises the applicable standards for compliance in Vietnam, by introducing new and detailed obligations. These include:

- a mandatory DPO for all PDPL Regulated Entities;
- stricter requirements for processing VN Personal Data relating to children and other vulnerable Vietnamese citizens;
- new safeguards in respect of automated decision-making; and
- comprehensive procedures for assessment of the impact of Cross-Border Data Transfers.

Importantly, the PDPL expands and increases the breadth and severity of the sanctions to which non-compliant PDPL Regulated Entities may be subject in Vietnam. Key examples include the following:

Serious violations

The maximum fine for serious breaches, particularly those involving unlawful Cross-Border Data Transfers, is set at 5% of the revenue generated by the violating PDPL Regulated Entity during the entirety of its most recently ended financial year.

General violations

Fines for any other general violations of any of the provisions of the Prevailing VN-PDP Law may be imposed in amounts up to VND3 billion (approximately USD120,000).

Illegal trading

Fines for the illegal buying or selling of VN Personal Data can be imposed in amounts equivalent to up to ten times (10x) the monetary gains realised by the violating PDPL Regulated Entity as a result of such illegal transactions; or VND3 billion (approximately USD120,000), if no monetary gains have been realised by the violating PDPL Regulated Entity from the violation.

The potential fines summarised above apply in respect of companies or other organisations who violate the provisions of the Prevailing VN-PDP Law. Individuals who commit violations may have fines imposed upon them in amounts up to the equivalent of 50% of the maximum fines applicable to organisational violators (as summarised above).

In severe cases, particularly those impacting upon national security, violations of the Prevailing VN-PDP Law may give rise to the commission of criminal offences and thus attract criminal sanctions under the Criminal Code of Vietnam.

The sanctions summarised above:

- are of a significantly higher degree of severity, as compared with the sanctions applicable under the legacy Decree 13 regime;
- provide a clear demonstration of the determination of the Vietnamese Government to elevate the importance of personal data protection in Vietnam and its regulation and enforcement; and
- bring Vietnam's personal data protection regime closer to an international standard of the kind represented by the GDPR.

Regulatory authority

The Prevailing VN-PDP Law does not introduce any changes in relation to the State authorities which have competent jurisdiction to administer and enforce the laws of Vietnam as they relate to personal data protection.

As was the case under the legacy Decree 13 regime, the MPS continues to be empowered to act as Vietnam's primary national authority for the regulation and enforcement of personal data protection.

The A05 Department

Specifically, the Department of Cybersecurity and High-Tech Crime Prevention (the "**A05 Department**") of the MPS exists specifically to hold and exercise primary authority and responsibility for regulation and enforcement of the Prevailing VN-PDP Law, including to carry out the functions set out below:

01

Issue guidelines

Issue guidelines in relation to the preparation and submission DPIA Dossiers and DTIA Dossiers.

02

Assess dossiers

Receive, assess, and approve (or reject) DPIA Dossiers and DTIA Dossier.

03

Conduct inspections

Conduct inspections or audits of PDPL Regulated Entities.

04

Handle breaches

Handle breach notifications in relation to violations of the Prevailing PDPL Law

05

Impose penalties

Impose penalties for violations of the Prevailing PDPL Law, including those constituting cross-border violations.

In addition, the A05 Department is responsible to:

- coordinate with other relevant State authorities (such as the Ministry of Science and Technology, among others); and
- deploy modern and advanced digital technology,

in order to ensure the comprehensive and effective implementation and enforcement of the Prevailing PDPL Law.

National Portal for Personal Data Protection

The National Portal for Personal Data Protection (the "**National Portal**") is the official online platform, managed and administered by the A05 Department, which is designed to facilitate:

- compliance with the Prevailing VN-PDP Law; and
- effective and efficient interface between PDPL Regulated Entities and the A05 Department.

The National Portal:

- was initially established under Decree 13;
- was launched in 2023 and later upgraded pursuant to Decision No. 2623/QD-TTg of the Prime Minister dated 29 November 2025;
- has been further expanded and enhanced under the PDPL;
- is integrated with the National Public Service Portal in order to provide real-time compliance tools for PDPL Regulated Entities; and
- is scheduled to be further enhanced by the MPS during 2026 to 2027, in order to:
  - provide information in relation to and disseminate State policy guidelines, policies, laws in relation to personal data protection;
  - provide support and guidance and enhance awareness and skills in relation to personal data protection for PDPL Regulated Entities and relevant State authorities;
  - receive and process feedback and suggestions from PDPL Regulated Entities and relevant State authorities; and
  - perform and facilitate such other functions as may be prescribed by applicable law relating to personal data protection from time to time.

Vietnam National Data Association

In preparation for the entry into force of the Law on Data No. 60/2024/QH15 (passed by the National Assembly of Vietnam on 30 November 2024 and having entered into force and effect on 1 July 2025) (the "**Law on Data**") and related legislation, (including the the prevailing VN-PDP Law), the Vietnam National Data Association (the "**VNDA**") was founded on 10 January 2025 and launched on 22 March 2025 by the MPS and key industry stakeholders (such as technology companies and legal professional organisations), in order to:

- promote best practices in relation to personal data protection;
- offer compliance training in relation to personal data protection; and
- advocate for the development and adoption within Vietnam of personal data protection standards.

VNDA role and functions

As a self-regulating body, the VNDA:

Bridge function

Provides a bridge between A05 Department oversight and private sector needs

Certifications focus

Focusses on certifications and awareness campaigns

Voluntary membership

Operates on a voluntary membership basis

Compliance assistance

Assists PDPL Regulated Entities in demonstrating proactive compliance with the Prevailing VN-PDP Law and its implementing legislation.

Strategic significance

In Vietnam's flourishing digital economy, driven primarily by e-commerce, fintech, and cross-border services (amongst other key drivers), personal data protection is now more important and high-profile than ever before. Personal data protection has become a matter of national security interest and a key strategic differentiator in Vietnam's continued development, international integration, and international status, as well as being a key factor in relation to Vietnam's competition with comparable countries for international investment and business collaboration.

PDPL Regulated Entities who demonstrate robust, GDPR-level personal data protection practices stand to gain significant advantages as a result. Examples of such advantages include:

Market trust

Building confidence with Vietnamese consumers and governmental bodies.

Partnership enablement

Facilitating smoother and more integrated business interactions with international counterparts from fully developed jurisdictions who demand high personal data protection standards.

Anti-corruption compliance

Strong personal data protection compliance (in particular in relation to access controls, documentation, and evidence of retention):

- directly supports compliance with global anti-corruption laws;
- ensures that data accessed during anti-corruption compliance reviews and internal investigations of Vietnam-based entities is handled lawfully and securely; and
- minimises the risk of non-compliant data access or transfer that may complicate legal proceedings relating to corruption or bribery.

M&A readiness

Personal data protection due diligence is now critical in relation to many M&A transactions, particularly where buyers from fully developed jurisdictions are involved. Undisclosed breaches or non-compliant data processing or transfer practices can lead to deal termination, imposition of specific indemnity liability, or significant price adjustments. Buyers routinely demand comprehensive data-mapping, DPO readiness, and personal data protection gap analyses before signing and/or completing M&A transactions.

Financing risk management

Lenders (particularly foreign lenders) increasingly consider that personal data protection non-compliance on the part of borrowers constitutes a material credit risk. Strict personal data protection compliance is an increasingly important factor for aspiring borrowers seeking to demonstrate their creditworthiness, in particular in connection with sophisticated international lenders.

PDPL – scope of application

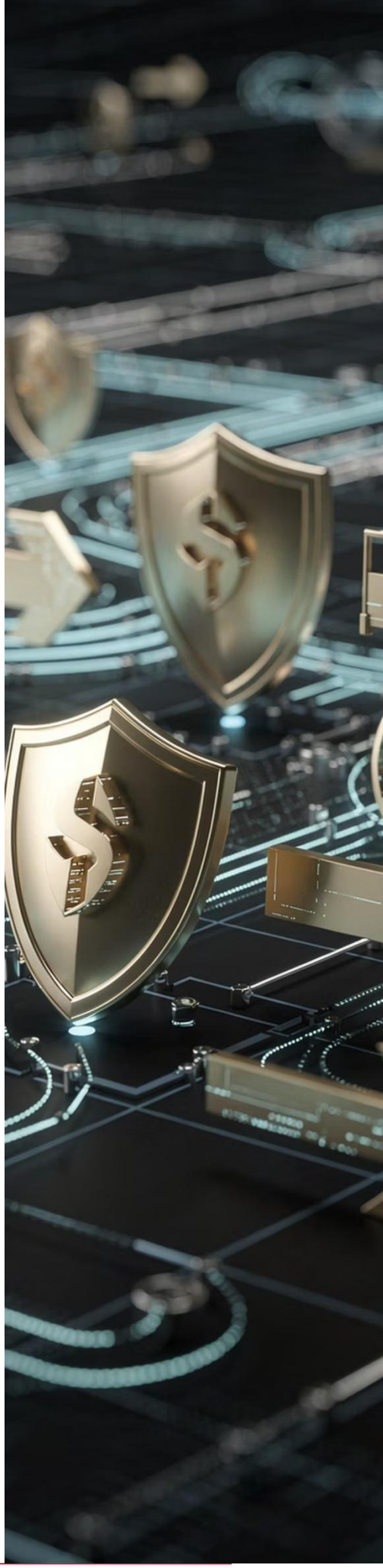
Like the legacy Decree 13, the PDPL applies to regulate the PDPL Regulated Activities of all PDPL Regulated Entities, which include:

- Vietnamese citizens and domestic Vietnamese companies and other organisations (regardless of whether they operate inside and/or outside of Vietnam); and
- citizens of foreign countries and foreign companies and other organisations who are physically present or based in Vietnam.

The PDPL also applies extraterritorially to citizens of foreign countries and foreign companies and other organisations who are not physically present in or based in Vietnam, to the extent that they engage directly in any PDPL Regulated Activities.

The PDPL therefore provides a clear and robust formulation as to the scope of the PDPL's application, which represents a significant improvement as compared with the corresponding framework under the legacy Decree 13.

The PDPL also provides targeted relief for startups and small businesses, to ease their compliance burdens, thereby fostering innovation. Startups and small businesses are entitled to the benefit of a five-year "grace period" (commencing as from 1 January 2026), during which they may opt out of the DPIA Dossier and DTIA Dossier preparation and lodgement requirements as well as the DPO appointment requirements. In addition, micro-enterprises and household businesses qualify for full exemptions from the aforementioned requirements, provided that they do not collect, process, or transfer sensitive data or large volumes of data, or supply personal data processing services.



Sensitive personal data

The PDPL sets out a broad list of categories of VN Personal Data which qualify as "sensitive personal data", extending beyond the categories of personal data which are recognised as being "sensitive" by international data protection frameworks such as the GDPR. Categories of VN Personal Data which are deemed by the PDPL as constituting "sensitive personal data" include VN Personal Data which constitutes or concerns:

- geolocation;
- identification credentials;
- banking and/or financial information; and/or
- online behaviour.

In addition, under the PDPL, "sensitive personal data" may include (but is not limited to) any VN Personal Data that is:

- legally required to be kept confidential; or
- subject to security protection measures.

PDPL Regulated Entities are obliged to apply additional safeguards when collecting, processing, and/or transferring "sensitive personal data", including:

- access restriction;
- formalised processing protocols; and
- secure transfer practices.

Further, individuals who are the subject of VN Personal Data ("**Data Subjects**") must be notified when any of their VN Personal Data which is collected, processed, and/or transferred by a PDPL Regulated Entity is of a sensitive nature.

Consent

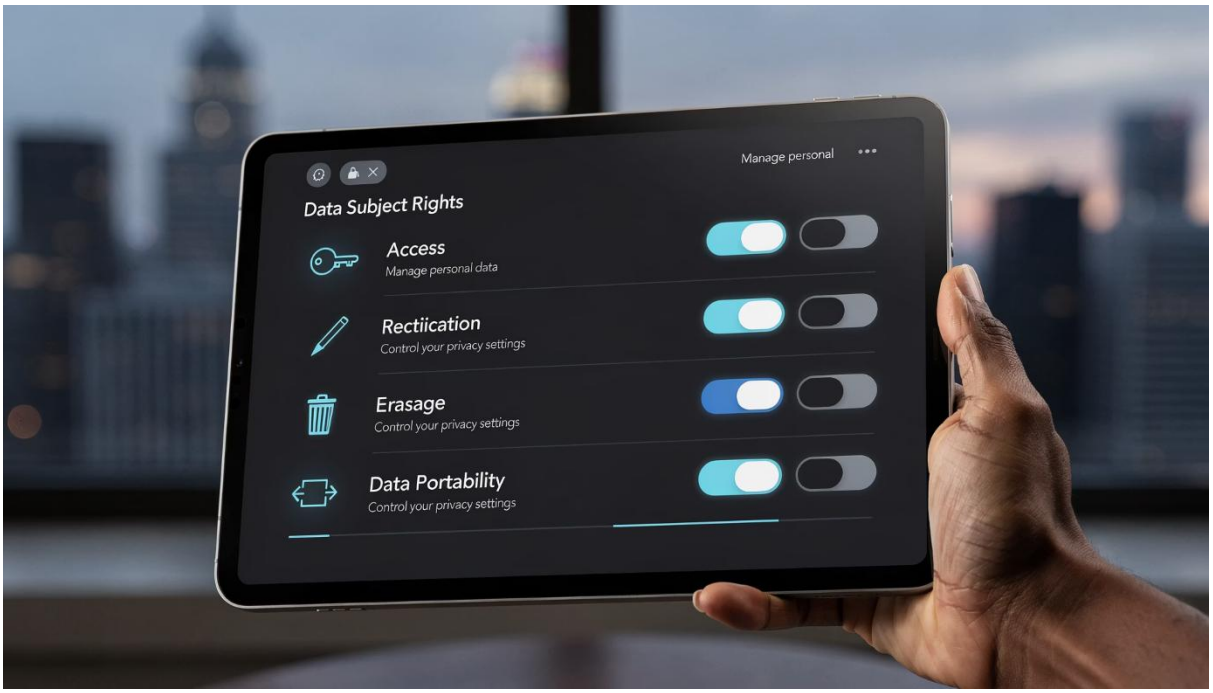
Vietnam is a consent-focussed jurisdiction in which consent is the primary legal basis for collecting, processing, and/or transferring VN Personal Data.

In order to be considered valid, consent must be:

- specific, voluntary, and affirmative; and
- provided on the basis of the Data Subject's full understanding of:
  - the purposes of the relevant VN Personal Data collection, processing, and/or transfer;
  - the types of VN Personal Data to be collected, processed, and/or transferred;
  - the information of the PDPL Regulated Entity(ies) involved in the collection, processing, and/or transfer of the relevant VN Personal Data; and
  - their legal rights and obligations as Data Subjects.

Under the PDPL, pre-ticked boxes, implied acceptance, and default opt-ins are not regarded as constituting or evidencing valid consent.

Where VN Personal Data is processed for multiple purposes, valid consent must be obtained by the PDPL Regulated Entity separately for each distinct purpose, without being conditional upon unrelated services.



In relation to disputes concerning personal data protection matters, the burden of proof sits with the PDPL Regulated Entity to demonstrate that valid consent has been properly obtained.

Consent Exemptions and Special Cases

The PDPL sets out a number of exemptions to its general requirement for valid consent in respect of VN Personal Data collection, processing, and/or transfer. Although the scope of these exemptions is broader as compared with the corresponding provisions of Decree 13, they are nevertheless narrowly confined to:

- protection of vital interests, including, among others:
  - life, health, and/or personal dignity in emergency situations;
  - national security and fraud prevention; and
  - State operations, and
- where necessary for the purpose of contract performance.

Audio and video recordings in public places may also be exempted from the general consent requirement in certain cases, subject to notification and the purpose of collection, provided that the collected VN Personal Data is retained only for such duration as is necessary to fulfil the applicable purpose.

Unlike the GDPR, the PDPL does not explicitly recognise the concept of "legitimate interests" as a standalone basis for the collection, processing, and/or transfer of VN Personal Data. As a result, PDPL Regulated Entities need to exercise a high degree of caution when seeking to rely on any of the legislated exemptions to the general PDPL for valid consent requirement. Collection, processing, and/or transfer of VN Personal Data under any of the legislated exemptions subjects the PDPL Regulated Entity to a burden of proof to demonstrate:

- the lawful basis of the relevant collection, processing, and/or transfer of the relevant VN Personal Data; and
- its maintenance and application of robust monitoring and audit mechanisms.

The PDPL does afford to PDPL Regulated Entities a degree of flexibility, in allowing negotiated agreements between PDPL Regulated Entities and Data Subjects (and/or other relevant persons or entities) in certain limited circumstances, subject to monitoring and risk assessment.

Children and Vulnerable Individuals

Vulnerable individuals, including children and individuals with limited civil capacity, necessitate the application of enhanced safeguards in relation to VN Personal Data collection, processing, and/or transfer. For example:

- processing children’s VN Personal Data requires the procurement of valid consent from their lawful guardian; and
- in respect of children aged seven years and above, dual consent from the child and his or her lawful guardian is required.

While not expressly mandated by the PDPL, these specific requirements in relation to children’s VN Personal Data imply that PDPL Regulated Entities must also conduct age verification before processing children’s VN Personal data, in order to ensure compliance.

Third party risk management

As at the date of publication of this VN-PDP Guide, many PDPL Regulated Entities manage VN Personal Data sharing with third parties on the basis of simple legal grounds such as general contractual provisions or confidentiality undertakings, as opposed to the deployment of comprehensive and specifically tailored personal data processing agreements. This approach often gives rise to a critical compliance gap, thereby jeopardising adherence to the Prevailing VN-PDP Law and increasing the likelihood of regulatory sanctions for failing to establish an adequate contractual framework for VN Personal Data collection, processing, and/or transfer.

Two key requirements

Third party risk management under the Prevailing VN-PDP Law consists of two key requirements, namely:

Adequate contractual safeguards

A requirement for the deployment of adequate contractual safeguards.

Appropriate processor selection

A requirement for the deployment of appropriate Data Processor selection.

In particular, the PDPL requires PDPL Regulated Entities to:

- execute personal data processing agreements with their externally engaged Data Processors, setting out clearly defined roles and responsibilities; and
- select "appropriate" external Data Processors to undertake any VN Personal Data processing activities.

While the Prevailing VN-PDP Law is silent as to specific criteria for external Data Processor selection, the selection process typically involves assessment of:

- technical and organisational security measures; and
- the compliance history of candidate Data Processors, depending on the nature and volume of the proposed VN Personal Data processing.

strong contractual arrangements combined with a thorough selection process will enable PDPL Regulated Entities to mitigate risks effectively when sharing VN Personal Data with external Data Processors, as Data Controllers remain primarily accountable and directly liable to Data Subjects for the compliance by external Data Processors with the Prevailing VN-PDP Law. Conversely, externally engaged Data Processors will also benefit from clear contractual terms which establish a transparent framework for contracted Data Processing activities conducted strictly under the instructions of the relevant Data Controllers. Of note, copies of relevant data processing agreements are required to be submitted to the A05 Department as part of any applicable DPIA Dossier and/or DTIA Dossier.

In specific cases of transfers of VN Personal Data to third parties as mentioned below, whether or not fees are involved, a formal data transfer agreement must be entered into, and details of the relevant VN Personal Data transfers must be incorporated into the applicable DPIA Dossier and/or DTIA Dossier. Such specific cases include any of the following:

- transfers of VN Personal Data made with the consent of the Data Subject;
- transfers of VN Personal Data to facilitate its continued processing in connection with an organisational restructuring; or

- transfers of VN Personal Data between a Data Controller and a Data Processor (or other relevant third party).

Additionally, for multinational companies having subsidiaries operating in various jurisdictions (including Vietnam), formal corporate policies and procedures should be established to:

- enshrine the principles governing the transfer of personal data within their corporate group; and
- demonstrate the existence and application of adequate data protection standards according to the applicable laws in each relevant jurisdiction, including Vietnam.

Such formal corporate policies and procedures should also be incorporated into any DTIA Dossier which is lodged with the A05 Department.

Data Subject requests

Under the PDPL, PDPL Regulated Entities must respond promptly and accurately to any requests which they may receive from any Data Subjects, in order to facilitate Data Subjects' exercise of their key legal rights in relation to VN Personal Data protection. These key legal rights of Data Subjects include the rights to:

- be informed about all relevant PDPL Regulated Activities involving their VN Personal Data;
- give or withdraw consent in relation to any PDPL Regulated Activities involving their VN Personal Data;
- access their VN Personal Data;
- rectify or complete inaccurate or incomplete VN Personal Data;
- require the deletion of their VN Personal Data;
- restrict processing in respect of their VN Personal Data;
- object to any PDPL Regulated Activities in respect of their VN Personal Data (particularly in relation to direct marketing);
- lodge complaints with State authorities; or
- seek judicial remedies.

Response timelines

While the legacy Decree 13 imposed a strict 72-hour deadline for responding to most Data Subject requests, the PDPL removes this rigid timeline to provide greater flexibility, thereby aligning more closely with international standards. Under the Prevailing VN-PDP Law, PDPL Regulated Entities generally have:

1

Initial Response

Two working days within which to provide an initial response to the request

2

Request Fulfilment

10 to 20 days to fulfil the request, extendable on one occasion by a period of a further 10 to 20 days, depending on the specific type of request.

If an extension is needed to fulfil a Data Subject request, PDPL Regulated Entities:

- must notify the Data Subject, explaining the grounds for extension; and
- bear the burden of proof to demonstrate that such extension is necessary and reasonable.

While the PDPL expressly recognises the rights of Data Subjects, the exercise of such rights is subject to boundaries established by broader legal and societal interests. Specifically, Data Subjects' rights must be exercised for the purposes of protecting their own legitimate interests, without causing undue difficulties or obstructing the lawful obligations and/or operations of PDPL Regulated Entities. Furthermore, the exercise by Data Subjects of their rights cannot infringe upon the legitimate rights and interests of the State or other organisations or individuals. This framework implies that PDPL Regulated Entities may validly refuse certain data requests, if they have clear and robust legal grounds upon which to do so.

Impact assessments

Unlike some international privacy frameworks that apply a risk-based or threshold-based approach, Vietnam's PDPL mandates that PDPL Regulated Entities must submit DPIA Dossiers and/or DTIA Dossiers (as applicable) to the A05 Department within 60 calendar days of having commenced the relevant PDPL Regulated Activities, irrespective of the volume or nature of those activities. Exceptions to these requirements are limited to startups and small businesses as mentioned in Section 8 above.

Dossier requirements

PDPL Regulated Entities are required to submit as part of their:

DPIA Dossier, an assessment in relation to the impacts of their VN Personal Data processing activities, using the template prescribed under Decree 356; or

(where applicable – if there is any Cross-Border Data Transfer engaged in or proposed) DTIA Dossier, an assessment in relation to the impacts of their Cross-Border Data Transfer activities.

The requirements for preparation and lodgement of DPIA Dossiers and DTIA Dossiers previously existed under the legacy Decree 13, but the applicable requirements have been clarified and enhanced under the Prevailing VN-PDP Law.

DPIA Dossiers and DTIA Dossiers need only be prepared and lodged with the A05 Department on one occasion, although there is an obligation for them to be updated on a bi-annual basis (for routine changes), or an ad-hoc basis (for major changes, including, among others, any event of restructuring, liquidation, or change of registered business lines related to VN Personal Data processing).

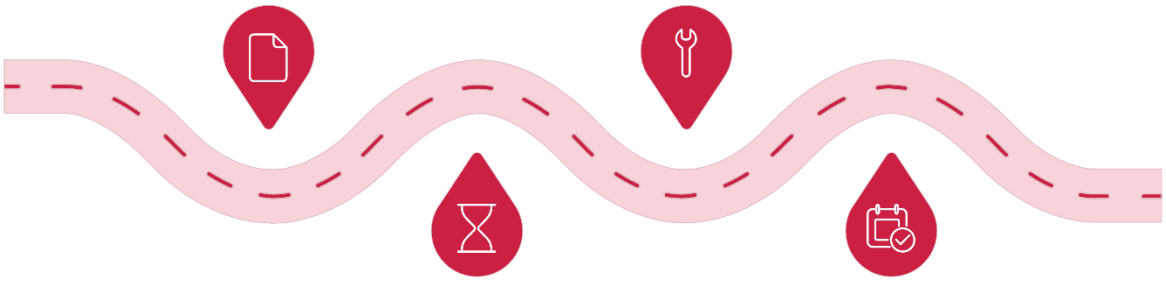
Assessment and approval process

Submission

PDPL Regulated Entities submit DPIA Dossier and/or DTIA Dossier within 60 calendar days of commencing activities.

Amendments if needed

In the event of failure, PDPL Regulated Entities have 30 days to make necessary amendments and/or supplementations.



A05 assessment

Within 15 days, the A05 Department assesses dossiers on a "pass or fail" basis.

Sanctions for non-compliance

Failure to satisfy requirements within the 30 day deadline can give rise to administrative sanctions.

Where any PDPL Regulated Entity has lodged any DPIA Dossier or DTIA Dossier with the A05 Department prior to 1 January 2026 (under the legacy Decree 13 framework), they are not required to lodge any fresh DPIA Dossier or DTIA Dossier (as applicable) under the Prevailing VN-PDP Law – although they are of course required to comply in all other respects with the requirements of the Prevailing VN-PDP Law.

Notably, where any PDPL Regulated Entity is subject to specific compliance obligations with regard to “core data” and “important data” under the Law on Data and those compliance obligations also fall under the oversight of the MPS (including but not limited to the A05 Department) – where to prepare and submit a DPIA Dossier and/or a DTIA Dossier under the Prevailing VN-PDP Law would give rise to duplication of compliance obligations, the PDPL exempts such PDPL Regulated Entities from the requirements to prepare the risk assessments and cross-border transfer impact assessments required under the Law on Data, if they have already lodged a DPIA Dossier and/or a DTIA Dossier in accordance with the PDPL.

Sectorial safeguards

Unlike the GDPR's technology-neutral principles, the PDPL establishes sector-specific safeguards in respect of data-sensitive activities, generally requiring:

Explicit consent	Data minimisation
Enhanced anonymisation and encryption	Strict retention limits

Innovative healthcare solutions, fintech applications, social networks, advertising services, location tracking, and biometrics are among the data-intensive sectors which are subject to these heightened obligations. In addition, frontier technologies such as artificial intelligence, cloud computing, blockchain, virtual reality, and “big data” are also captured by the sector-specific safeguard provisions of the PDPL, which impose specific safeguards in relation to Data Subjects' lawful rights and interests, in compliance with applicable Vietnamese laws, ethical standards, and cultural customs.

Specifically, the PDPL requires PDPL Regulated Entities to apply, review, and update on a continuous basis appropriate security measures, while certain high-risk sectors demand heightened protections. Examples include the following:

Employment and Recruitment:

Employers are only allowed to collect VN Personal Data relating to employees through lawful technological and technical measures, ensuring the rights and interests of employees on the basis that employees are fully informed of these measures. The VN Personal Data of employment applicants must be deleted or destroyed if the recruitment does not proceed to employment, unless otherwise agreed by the applicant.

Banking and Finance:

In addition to complying with the PDPL, organisations and individuals engaged in credit information activities must implement strict measures to protect customers’ VN Personal Data and prevent data leakage. Furthermore, organisations operating in these sectors must have solutions in place to restore customers’ VN Personal Data. Credit information must not be processed for the purposes of credit scoring, ranking, or assessing creditworthiness without the Data Subject's consent.

Frontier Technologies:

Systems and services utilising big data, artificial intelligence, blockchain, virtual reality, and/or cloud computing must integrate appropriate VN Personal Data security measures. These systems must also implement suitable authentication, identification, and access control mechanisms in the processing of VN Personal Data. In addition, VN Personal Data processed by artificial intelligence must be classified according to risk levels, ensuring the application of appropriate and effective protection measures.

Healthcare and Insurance:

Entities operating in the healthcare sector must not disclose VN Personal Data to third-party healthcare or insurance providers, except with the Data Subject's consent or as expressly permitted by applicable law. Additionally, reinsurance and retrocession businesses must explicitly disclose in customer contracts any transfers of VN Personal Data to their partners.

Advertising:

Advertising activities require the customer's consent in respect of the content, methods, format, and frequency of VN Personal Data collection and/or processing. Advertisers must comply with anti-spam and advertising laws, provide opt-out mechanisms, prohibit outsourcing of VN Personal Data-driven services, and bear the burden of proof for demonstrating compliance.

Social media platforms and online communications:

Providers of social media platforms and online communication services must refrain from requiring identity documents for account verification and unauthorised eavesdropping of calls or messages. Users must have the option to refuse cookies and tracking. Additionally, providers must:

- publish clear privacy policies;
- enable user access, correction, deletion, and privacy settings;
- report breaches;
- protect Vietnamese citizens' data in cross-border transfers; and
- implement effective violation-handling procedures.

Location tracking:

Location tracking via radio-frequency identification cards or other technologies is only permitted with the consent of the Data Subject or in accordance with legal requirements and regulations. Mobile application platforms must inform users about the use of personal location data, implement measures to prevent unauthorised collection of location data by unrelated organisations or individuals, and provide users with options for location tracking.

Biometrics:

PDPL Regulated Entities collecting and processing biometric data must ensure physical security for data storage and transmission devices, restrict access rights, maintain monitoring systems to prevent and detect breaches, and comply with applicable laws and relevant international standards.

Data retention

The PDPL prohibits retaining VN Personal Data "just in case" and requires that VN Personal Data be deleted, destroyed, or irreversibly de-identified once the processing purpose is fulfilled or the retention period expires, or upon the Data Subject's request. PDPL Regulated Entities are also strictly prohibited from intentionally restoring deleted VN Personal Data without authorisation.

The PDPL further specifies retention periods for certain cases as follows:

Employee Personal Data

VN Personal Data of employees must be deleted upon termination of the

Advertising Data

VN Personal Data used for advertising must have a defined retention period and must be deleted when no longer needed.

Public recordings

VN Personal Data obtained from public audio or video recording activities (for example, security CCTVs) may only be retained for the time necessary to achieve the collection purpose and must be deleted once the retention period expires in accordance with the PDPL.

Review of existing policies and practices in relation to data retention periods is crucial to ensure compliance with the PDPL.

DPO

The PDPL mandates that every PDPL Regulated Entity must formally appoint a qualified DPO or establish a data protection department ("**DPD**"), subject to the exemptions for startups and small businesses as outlined in Section 8 above.

Notably, the PDPL explicitly allows the outsourcing of DPO and/or DPD functions to duly licensed professional service providers.

Qualification requirements in respect of the appointed DPO generally require:

- at least two years of substantive experience in legal and/or compliance affairs, information technology, information security risk management or human resources; and
- the DPO to have been trained in data protection law and professional skills.

The question of whether or not a DPO may serve the applicable requirements under the PDPL across two or more corporate group entities remains unclear under the Prevailing VN-PDP Law. Further implementing legislation which clarifies this matter would be welcomed by corporate groups who have two or more group entities who fall within the regulatory ambit of the PDPL.

Personal data processing services

Under Decree 356, nine categories of activities related to VN Personal Data processing will be subject to regulatory oversight and require the certificate of eligibility to conduct VN Personal Data processing services. These include:

- automated systems operation;
- credit scoring services;
- online data collection services;
- health and/or medical monitoring applications;
- education monitoring services;
- data analytics services;
- encryption in data transmission and/or storage;
- artificial intelligence driven automated processing services; and
- geolocation services.

In order to provide VN Personal Data processing services lawfully, enterprises must meet specific requirements relating to:

- qualified personnel;
- appropriate infrastructure and facilities; and
- favourable outcomes from DPIA Dossier and/or DTIA Dossier submissions.

From the perspective of businesses operating in Vietnam, this shift means that reliance on third-party suppliers for any of the regulated services will now require an assessment of supplier's eligibility, to ensure that they hold appropriate licences and meet compliance obligations.

Breach notification

Under the legacy Decree 13, PDPL Regulated Entities were subject to a broad obligation to notify the A05 Department of any VN Personal Data protection breach – encompassing unauthorised access, disclosure, alteration, or loss of VN Personal Data – within 72 hours of occurrence, regardless of impact severity, thus representing a stringent regime that burdened businesses with obligations to report minor incidents.

In contrast, the PDPL refines the applicable notification obligations by imposing a materiality threshold, requiring notification to the A05 Department only for breaches posing risks to national security, public order, or Data Subjects' life, health, dignity, or property, with the 72-hour notification deadline now commencing as from the time of detection, as opposed to the time of occurrence (this being a more pragmatic and realistic approach which is akin to the approach taken under the GDPR).

Data Processors must promptly alert Data Controllers upon discovering qualifying breaches, thus enabling coordinated responses.

This targeted approach reduces administrative overload for low-risk events while prioritising high impact threats, although sector-specific rules (for example, mandatory notifications to Data Subjects in instances of breaches relating to finance, banking, location tracking, or biometrics) may apply in addition.

Audits and internal review

Audits and internal review are integral to ensuring lawful collection, processing, and/or transfer of VN Personal Data, particularly in relation to high-risk activities such as sensitive data handling and Cross-Border Data Transfers. Key aspects include the following:

Authority and scope of audits

Role of the MPS:	Scope:	Focus areas:
The MPS may conduct annual audits in respect of data protection compliance, including Cross-Border Data Transfers, and has authority to conduct random inspections or inspections arising from specific incidents (for example, data leaks, breaches, or complaints). Audits may cover all stages of data lifecycle, including collection, processing, storage, transfer, and deletion and/or destruction.	Target organisations processing VN Personal Data.	Consent validity, DPIA Dossier and/pr DTIA Dossier accuracy and compliance, security measures, third party safeguards, internal policies and processes, and DPO effectiveness.

Audits may involve on-site reviews, document requests, and/or interviews.

Mandatory internal review and assessment activities

DPIA Dossiers and DTIA Dossiers:	Periodic Compliance Reviews:
PDPL Regulated Entities must perform internal reviews as part their DPIA Dossier assessment and lodgement obligations (applicable in respect of domestic collection, processing, and/or transfer activities) and/or DTIA Dossier assessment and lodgement obligations (applicable in respect of Cross-Border Data Transfer activities) and then on the basis thereof prepare and lodge with the A05 Department the requisite DPIA Dossier and/or DTIA Dossier within 60 days of having commenced the relevant PDPL Regulated Activities. Auditable records of the risks, safeguards, and mitigation measures identified and reported as a result of such internal reviews must be kept.	The PDPL implies that PDPL Regulated Entities must implement ongoing monitoring and periodic internal audits, to verify their adherence to principles such as legal compliance and data minimisation. This includes obligations to track consent and breach responses and to retain auditable records of such tracking.

The PDPL requires proactive risk management and it is expected that the MPS' levels of proactive investigation, auditing, and enforcement will increase over time, commencing as from 2026.

Cross-Border Data Transfer

Cross-Border Data Transfer activities are defined by the PDPL as including the following:

VN Personal Data stored in Vietnam is transferred to a data storage system located outside of Vietnam.	Organisations or individuals located in Vietnam transfer VN Personal Data to organisations or individuals located outside of Vietnam.	Organisations or individuals (whether located inside or outside Vietnam) use foreign-based platforms to process VN Personal Data.

Any person or entity conducting a Cross-Border Data Transfer must comply with the obligation to submit a DTIA Dossier to the A05 Department. There are, however, legislated exemptions to this requirement, including Cross-Border Data Transfers implemented in connection with:

- journalistic or media activities;
- cross-border human resources management;
- storage of employees' data on cloud computing services; or
- cross-border logistics, remittances, payments, hotel bookings, visa applications, and/or scholarships.

While no pre-approval is required for Cross-Border Data Transfers, the MPS retains oversight power over the submitted DTIA Dossiers and may decide to suspend non-compliant Cross-Border Data Transfers which threaten national security. In addition, the MPS may conduct Cross-Border Data Transfer audits annually, or on an ad hoc basis if a violation or incident is detected.

Actions to ensure compliance with the PDPL

All PDPL Regulated Entities should take immediate action to ensure their compliance with the Prevailing VN-PDP Law, unless they are startups or small businesses entitled to the benefit of the exemptions outlined above in this VN-PDP Guide.

Set out below is an indicative action plan which represents a prudent approach to pursuing and achieving compliance with the PDPL and its implementing legislation.

Treat Vietnam as a "GDPR-Level" jurisdiction

Immediately adopt a GDPR equivalent compliance standard for all PDPL Regulated Activities.

Conduct a comprehensive gap analysis

Initiate a detailed data inventory and gap analysis (with the assistance of duly qualified and experienced legal counsel) in order to identify, having regard to the requirements of the Prevailing VN-PDP Law:

1	2	3
Data Inventory All VN Personal Data collected and/or held (categorising that VN Personal Data into sensitive and non-sensitive categories).	*Data Flows* All VN Personal Data flows, in particular Cross-Border Data Transfers (including, for example, HR systems, CRM, ERP, cloud storage, chat platform logs, marketing databases, and	*Legal Basis* The legal basis for all existing Data Collection, Data Processing, Domestic Data Transfer, and/or Cross-Border Data Transfer activities involving any VN Personal Data.

Appoint a qualified Vietnam DPO:

The DPO:

- must have at least two years of relevant experience and preferably an international privacy certification;
- should report directly to both the management team of the PDPL Regulated Entity and (where applicable) the chief privacy officer (or similar role) of the relevant corporate group; and
- should be the only person authorised under the Prevailing VN-PDP Law to communicate with the A05 Department.

Establish clear internal governance and accountability

Corporate Directive

Issue a corporate directive that makes the Vietnam DPO the sole point of contact for the A05 Department and defines roles for Legal, HR, IT, Compliance and executive management.

Training Program

Launch mandatory VN Personal Data protection training for all employees and key third-party business partners (especially sales teams).

Develop an effective and compliant operational framework

An effective and compliant operational framework should include the following elements:

Adopt and roll out formal corporate policies and procedures and (where applicable) robust intra-group data transfer agreements that explicitly cover the requirements of the Prevailing VN-PDP Law.

Deploy automated consent and preference management tools that work seamlessly in the Vietnamese language and store proof of valid consent.

Implement robust technical and organisational safeguards to prevent attacks, loss, leakage, damage, and unauthorised access to VN Personal Data.

Adopt and roll out clear and strict policies and procedures applicable to all collection, processing, and transfer of VN Personal Data (in particular, consent collection and management, third party risk management, cross-border transfers, preparation, submission and monitoring of DPIA Dossier and DTIA Dossier compliance, handling Data Subject requests, data retention and disposal, and breach notification).

(If not done already), prepare and lodge with the A05 Department a DPIA Dossier and/or a DTIA Dossier (as required, depending on whether or not any cross-border transfers of VN Personal Data are engaged in by the PDPL Regulated Entity).

Authors

Justin Gisz
Partner
E: justin.gisz @asia-counsel.com

Mai Nguyen
Senior Associate

About Asia Counsel

Asia Counsel, in association with Kinstellar Southeast Asia, is a Ho Chi Minh City based law firm with more than a decade of experience advising international and Vietnamese investors. With a team of over 30 lawyers, we combine strong local insight with international standards to deliver clear, practical and business-focused advice. Our partners are internationally trained and have practised at leading global and regional firms, supporting multi-jurisdictional mandates efficiently.

Our data protection and compliance practice advises clients on legal and regulatory requirements affecting the collection and use of data, governance, and internal controls. We support clients with compliance assessments, policy and contract reviews, data protection documentation, cross-border data transfer considerations, vendor and outsourcing arrangements, and incident preparedness. We also assist with regulatory engagement, internal reviews, and remediation.

We advise multinational corporates and large Vietnamese groups, financial institutions, technology companies, and investors across sectors such as energy, infrastructure, real estate, manufacturing and consumer. We work closely with in-house legal, compliance and business teams to provide pragmatic advice that helps manage risk and supports day to day operations.

Asia Counsel Vietnam Law Company Limited

www.asia-counsel.com

Level 9, Deutsches Haus, 33 Le Duan Boulevard, Sai Gon Ward, Ho Chi Minh City