

Making Sense of Vietnam's Latest Data Protection and Governance Regime: The Law on Protection of Personal Data and the Law on Data

Authors: Sakshi Shivhare, Josh Lee Kok Thong, and Dominic Paulger
December 2025

Table of Contents

1. Introduction.....	2
2. The new PDP Law elevates and enhances data protection in Vietnam by preserving much of the existing regime while introducing important refinements.....	3
a. The PDP Law refines the territorial scope of the PDP Decree.....	4
b. The PDP Law takes a different, unique approach towards defining “basic” and “sensitive” personal data.....	5
c. The PDP Law continues to adopt a consent-focused regime, with clearer conditions for what constitutes valid consent.....	6
d. The PDP Law outlines enhanced sector-specific obligations for high-risk processing activities.....	7
e. The PDP Law’s cross-border data transfers rules maintain significant similarities with the existing regime, and remain significantly different from global equivalents like the GDPR.....	9
f. The Ministry of Public Security remains the focal agency for data protection within a governance structure unique to Vietnam’s context and needs.....	11
g. The PDP Law introduces a structured penalty framework covering organizational and individual liability.....	12
h. The PDP Law is a unique legislative instrument that seeks to meet Vietnam’s digital economy needs while navigating its development trajectory.....	13
3. The intersection of the PDP Law and the Data Law creates compliance implications for organizations navigating cross-border data transfers.....	13
4. Navigating the fast-transforming Vietnamese data regulatory landscape requires active monitoring, caution and curiosity.....	15

1. Introduction

Vietnam is undergoing a sweeping transformation of its data protection and governance framework. Over the past two years, the country has accelerated its efforts to modernize its regulatory architecture for data, culminating in the passage of two landmark pieces of legislation in 2025: the [Law on Personal Data Protection](#) (Law No. 91/2025/QH15) (PDP Law), which elevates the Vietnamese data protection framework from an executive act to a legislative act, while preserving many of the existing provisions, and the [Law on Data](#) (Law No. 60/2025/QH15) (Data Law). Notably, the PDP Law is expected to come into effect on January 1st, 2026.

The Data Law is Vietnam's first comprehensive framework for the governance of digital data (both personal and non-personal), and applies to all Vietnamese agencies, organizations and individuals, as well as foreign agencies, organizations and individuals either in Vietnam or directly participating or are related to digital data activities in Vietnam. The data law became effective in July 2025. Together, these two laws mark a significant legislative shift in how Vietnam approaches data regulation, addressing overlapping domains of data protection, data governance, and emerging technologies.

This Issue Brief analyzes the two laws, which together define a new, comprehensive regime, for data protection and data governance in Vietnam. The key takeaways from this joint analysis show that:

- The new PDP Law elevates and enhances data protection in Vietnam by preserving much of the existing regime, while introducing important refinements, such as taking a different, unique approach towards defining “basic” and “sensitive” personal data, or providing more nuance on the cross-border data transfers regime with new exceptions, even if it still revolves around Transfer Impact Assessments (TIAs).
- However, the PDP Law continues to adopt a consent-focused regime, even as it provides clearer conditions for what constitutes valid consent.
- The PDP Law outlines enhanced sector-specific obligations for high-risk processing activities, such as employment and recruitment, healthcare, banking, finance, advertising and social networking platforms.
- The intersection of the PDP Law and the Data Law creates compliance implications for organizations navigating cross-border data transfers, as the present regulatory regime doubles down on the state-supervised model for such transfers.

- Finally, risk and impact assessments are emerging as a central, albeit uncertain, aspect of the new regime.

This Issue Brief has three objectives. First, it summarizes key changes between the PDP Law and Vietnam’s existing data protection regime, and draws comparison between the PDP Law and the EU’s [General Data Protection Regulation](#) (GDPR) (**Section 2**). Second, it analyzes the interplay between the Data Law and the PDP Law (**Section 3**). We then provide key takeaways for organizations as they navigate the implementation of these laws (**Section 4**).

2. The new PDP Law elevates and enhances data protection in Vietnam by preserving much of the existing regime while introducing important refinements

On 26 June 2025, Vietnam marked a significant milestone in its data protection landscape by enacting its long-awaited PDP Law. The PDP Law will come into force on 1 January 2026. It replaces the existing [Decree on Protection of Personal Data](#) (Decree No. 13/2023/ND-CP) (PDP Decree), which acted as Vietnam’s *de facto* data protection regime since 1 July 2023. You can read a guest-authored FPF blog post analyzing the PDP Decree [here](#).

This shift from the PDP Decree to the PDP Law is significant for two reasons. **First, it elevates Vietnam’s data protection regime to the status of a national law.** While the existing PDP Decree was Vietnam’s first attempt at establishing a comprehensive data protection regime, the PDP Decree was inherently limited by its legal status: in Vietnam’s statutory hierarchy, a “decree” is subordinate in legal authority to a “law”. Decrees can be promulgated just by executive action and need not be approved by Vietnam’s National Assembly. **Second, and relatedly, the shift addresses important issues around the PDP Decree’s effect and enforceability.** While the PDP Decree’s promulgation was accelerated (as there was no need for approval from the National Assembly), its subordinate legal status meant that in the event of conflicting regulations on the same issue, codes and laws would prevail over the PDP Decree. This was perhaps why Prime Minister Pham Minh Chinh had [announced](#) as early as January 2022 that the Government’s ultimate goal was to enact a comprehensive and robust law for personal data protection.

While the PDP Law retains the broad structure and spirit of the PDP Decree (for instance, a focus on consent; impact assessment requirements for cross-border data transfers; and the data breach

response framework), there are notable refinements: a strengthening of the penalty framework, the introduction of certain sector-specific data protection requirements, and increased flexibility for small businesses and start-ups. Nevertheless, practitioners should note that several key implementation details, including procedural rules, also remain subject to future implementing regulations. In this regard, between 16 and 26 September 2025, Vietnam’s Ministry of Public Security (MPS) consulted on a [draft decree](#) to implement the PDP Law (Draft Implementing Decree), which sets out detailed provisions operationalizing key aspects of the PDP Law. In any case, these two factors – substantial continuity from the PDP Decree and delegating key implementation details to future rules – possibly explain the PDP Law’s relatively quick development (from February 2024 to June 2025).

The sections below cover key and notable changes and elements in the PDP Law, and, where relevant, compare them to the GDPR – chosen as a comparator due to its use by many companies as a global regulatory frame of reference.

a. The PDP Law refines the territorial scope of the PDP Decree

The PDP Law’s territorial scope is a refinement from the existing PDP Decree. While both instruments apply to all entities (including individuals) – Vietnamese or foreign – processing personal data within Vietnam, Article 1 of the PDP Law specifies application to “foreign agencies, organizations and individuals directly involved in or related to the processing of personal data of Vietnamese citizens and people of Vietnamese origin whose nationality has not yet been determined living in Vietnam (and) have been granted identity certificates”. The table below provides a comparison for reference.

The change essentially means that rather than covering all foreign agencies, organizations and individuals processing personal data in Vietnam, the PDP Law only covers foreign agencies, organizations and individuals *processing personal data of Vietnamese citizens and stateless persons of Vietnamese origins, and who are residing in Vietnam and possess an identity certificate*. While the reasons for the change are not clear, the change arguably strengthens the nexus between the PDP Law and Vietnamese citizens and persons of Vietnamese origin.

Notably, compared to the Decree, the scope of application is further narrowed down as it now eliminates “Vietnamese agencies, organizations and individuals that operate in foreign countries” from its scope (former Article 1.2.c. of the Decree).

When compared to the GDPR, the PDP Law similarly adopts an extraterritorial scope – albeit in the case of foreign entities abroad, the PDP Law has a narrower scope that is based on the nationality / origin and status of the data subject.

b. The PDP Law takes a different, unique approach towards defining “basic” and “sensitive” personal data

The PDP Law retains the PDP Decree’s distinction between “basic” and “sensitive” personal data (see Article 2). However, while the PDP Decree sets out lists of examples of personal data considered “basic” or “sensitive”, the PDP Law simply provides a general definition of both categories. A detailed list of types of sensitive data can be found in the Draft Implementing Decree, although it remains to be seen if the final version will retain the list, or if the items in the list will be kept the same. Notable points include:

1. **Basic personal data (Article 2.2):** Defined as personal data “reflecting common personal and background factors, regularly used in transactions and social relations”. The Draft Implementing Decree adds that basic personal data is what is *not* on the specified list of sensitive personal data.
2. **Sensitive personal data (Article 2.3):** Defined as “personal data associated with the privacy of individuals, which, when infringed upon, will directly affect the legitimate rights and interests of *agencies, organizations and individuals*”.

Notably, the definition refers to the legitimate rights and interests of agencies and organizations – something that was not in the PDP Decree. It is unclear what the implications would be in practice as it might significantly expand the range of datasets that may be considered “sensitive”.

The current list of examples of sensitive personal data in the Draft Implementing Decree also goes beyond the existing list in the PDP Decree, and includes telecommunications subscription data and data on the use of social networks, online communication services and other cyberspace services.

The PDP Law, like the PDP Decree, also **subjects the sensitive personal data to stricter requirements**, although these remain to be finalized in implementing regulations. In the current Draft Implementing Decree, these requirements include: (a) notification to the data subject that sensitive personal data is to be processed; and (b) the need for security measures for storage and transmission devices used to transfer sensitive personal data. In addition, while start-ups, small enterprises, business households and micro-enterprises are effectively exempted from requirements on data protection impact assessments, transfer impact assessments and the need for the appointment of data protection officers / departments (see Article 38, read with Articles 21, 22 and 33.2), these exemptions do not apply if such organizations are processing sensitive personal data (see Article 38.2).

When compared to the GDPR, Article 2 of the PDP Law shares some similarities – but also carries notable differences from – Article 9.1 of the GDPR. Based on the current list in the Draft Implementing Decree, Vietnam’s data protection regime would encompass all that is considered sensitive personal data under the GDPR, and go beyond to cover financial data, location data, telecommunications data and data on cyberspace activities.

c. The PDP Law continues to adopt a consent-focused regime, with clearer conditions for what constitutes valid consent

Both the Decree and the PDP Law emphasize consent as the default legal basis for processing. However, the PDP Law introduces clearer conditions for valid consent and places greater emphasis on specificity and transparency (Article 9). Under the PDP Law, consent must be given freely. Consent is also only valid if data subjects have been informed of what personal data is being collected, for what purposes, by whom, and what their rights and obligations are (Article 9.2). The PDP Law also prohibits bundled consent mechanisms, requiring separate consent for each specific purpose of processing (Article 9.4). Specific rules on valid consent will be detailed in implementing regulations (at present, this can be found at Article 6 of the Draft Implementing Decree).

Like the earlier Decree, the PDP Law also recognises a limited set of alternative legal bases for processing (Article 19). Specifically, personal data may be processed without consent in the following cases:

- Protecting life, health, dignity, and legitimate rights and interests of data subjects in urgent cases (Article 19.1(a));
- Emergency situations and national security threats (Article 19.1(b));
- State agency activities and management functions (Article 19.1(c));
- Performance of a contract (Article 19.1(d)); and
- Other cases prescribed by law (Article 19.1(e)).

This narrower, consent-focused framework differs from regimes such as the GDPR, which permit a broader range of bases, such as legitimate interests and public interest (as found in Article 6 GDPR). The absence of a “legitimate interests basis” equivalent in the PDP Law points to a more restrictive regulatory environment, potentially creating operational challenges for businesses seeking to scale

globally. That said, the proviso “other cases prescribed by law” (Article 19.1(e)) leaves room for other bases for processing personal data other than consent being laid out in the future.

d. The PDP Law outlines enhanced sector-specific obligations for high-risk processing activities

Unlike the earlier Decree, the PDP Law introduces enhanced obligations for several sector-specific high-risk data processing activities (Chapter II, Section 2 of the PDP Law), such as employment and recruitment, healthcare, banking, finance, advertising and social networking platforms. These obligations include:

Activity	Enhanced Obligations under PDP Law
Employment and recruitment (Article 25)	<p>In recruitment, entities may only require candidates to provide personal data that is necessary for recruitment purposes and may only process the data for those purposes unless otherwise prescribed by agreement or law. Entities must also delete or destroy the data of candidates who are not recruited, unless otherwise agreed.</p> <p>In the employment context, employees must be made aware of any technological or technical measures used to process their personal data for managing their employment. Employee data may only be retained for a period required by law or agreement and must be deleted or destroyed upon contract termination, unless otherwise prescribed by agreement or law.</p>
Healthcare and insurance (Article 26)	<p>Entities may only provide personal data to third-party health care or insurance service providers at the data subject's written request, or in situations where consent would not be required to process the data (see Section 1(c) above).</p> <p>For insurance activities, any transfer of personal data for reinsurance must be clearly stated in the contract with the customer.</p>
Banking, finance, and credit information (Article 27)	<p>Organizations must obtain data subjects' consent to process their credit information for scoring or rating purposes.</p> <p>Organizations conducting credit information activities must only collect necessary data from lawful sources, apply measures to prevent unauthorized</p>

	access and recover lost data, and maintain confidentiality when assessing credit.
Advertising (Article 28)	<p>Customers must be clearly informed about the content, method, and frequency of advertising and give express consent. They must also be allowed to opt out, in which case providers must stop advertising to them.</p> <p>Where a controller transfers its customers' personal data to a third-party advertising service provider, that third-party provider may only use the data as agreed with the controller, and may not engage subcontractors to process the data.</p> <p>For targeted or personalized advertising, consent is required to collect personal data via monitoring of website or app usage. A method to refuse data sharing must be established, and personal data must be deleted when no longer needed.</p>
Social networking platforms and online communications services (Article 29)	<p>Providers of social network and online communication services must clearly notify users about data collection on first installation and use of their services. They must also publish a clear privacy policy detailing user rights to access, correct, and delete data.</p> <p>Providers are prohibited from requiring images or videos of identity papers for account authentication.</p> <p>Providers must provide an opt-out for cookies and tracking and may only monitor usage with users' consent.</p> <p>Providers are prohibited from accessing device audio or text messages without data subjects' consent, unless required by law.</p>
Emerging technologies (Article 30)	<p>Organizations must only process personal data using big data, AI, blockchain, the metaverse, or cloud computing where necessary. They must also ensure that the processing observes ethical principles and upholds data subjects' rights and interests.</p> <p>Such organizations must also ensure that their systems integrate appropriate</p>

	<p>security measures, including authentication and access controls. Risk levels with appropriate protection measures must also be employed when processing personal data via AI.</p> <p>Organizations are also prohibited from developing or using these technologies with personal data in any way that harms national defense, security, or social order, or infringes on the life, health, honor, or property of others.</p> <p>The Government is tasked with issuing more detailed regulations for processing personal data via these advanced technologies.</p>
--	--

e. The PDP Law’s cross-border data transfers rules maintain significant similarities with the existing regime, and remain significantly different from global equivalents like the GDPR

Unlike the GDPR’s more developed system of transfer mechanisms (e.g., assessment of equivalence (also known as “adequacy”), standard contractual clauses, and binding corporate rules), Vietnam’s approach towards cross-border data transfers remains state-supervised and tightly controlled.

Like the PDP Decree, the PDP Law provides only a **single** mechanism for transferring personal data out of Vietnam: organizations must submit a data transfer impact assessment (TIA) to the MPS for all such transfers (Article 20.2). This requirement is not subject to any data volume thresholds, and applies when:

- Transferring personal data stored in Vietnam to data storage systems located outside Vietnam;
- Agencies, organizations or individuals in Vietnam transfer personal data to overseas organizations or individuals; and
- Agencies, organizations and individuals use platforms outside Vietnam to process personal data collected in Vietnam.

There are, however, at least three notable differences in the PDP Law that did not exist in the old regime under the PDP Decree:

1. **The PDP Law now specifies that only one TIA needs to be submitted for the “entire operation period of such agency, organization or individual” (Article 20.3).** However, this TIA must be updated every six months (if there are changes), or immediately in certain specified cases (such as where the organization is re-organized, where there is a change in information about the organization, or where there is a new business or service line in the organization) (Article 22.2). This change removes one point of uncertainty in the PDP Decree (which did not have this proviso), as it was unclear whether a TIA was needed for *every instance* of a data transfer, or if a TIA could remain in effect as long as there were no material changes.
2. **The PDP Law now provides limited exceptions to the TIA submission requirement (Article 20.6).** These exceptions are: (a) transfers by competent state agencies; (b) agencies and organizations storing employee data on cloud computing services; (c) individuals transferring their own personal data across borders; and (d) other cases as prescribed by the Government.

As at the time of writing, the Draft Implementing Decree supplements this with several more exceptions (Article 18.3 of the draft Decree): (a) prescribed press and media activities; (b) transfers of personal data that “have been made public as prescribed by law”; (c) in emergency situations where it is absolutely necessary to transfer personal data to protect and individual’s life, health and property safety, or to comply with law; (d) to manage cross-border HR or labor agreements as prescribed by law; and (e) to sign contracts or carry out procedures related to cross-border transportation, logistics, money transfers, payment, hotel accommodation and visa applications. If this current exemption list remains, these exemptions would represent a notable easing of TIA requirements. It, however, also reinforces the need for organizations to properly assess their cross-border data needs in order to understand which situations require a TIA or otherwise.

3. **As covered above, the PDP Law provides a five-year exemption from the TIA requirement (among other requirements) for start-ups and small enterprises, as well as a perpetual exemption for business households and micro-enterprises (Articles 38.2 and 38.3).** The exemption does not apply if these entities process sensitive data, offer data processing services, or process personal data of “a large number of personal data subjects” (at the time of writing, the Draft Implementing Decree specifies the number as 100,000 data subjects for start-ups and small enterprises, and 500,000 for business households and small enterprises – which are not large numbers, considering Vietnam’s population of 101 million people).

Non-compliance with the TIA requirement attracts significant penalties: **organizations in breach face fines of up to 5% of their turnover from the preceding year** (Article 8.4). Where there is no prior-year

turnover, or if the calculated fine is lower than VND 3 billion (approximately USD 115,000), a maximum fine of VND 3 billion applies.

At the time of writing this analysis, it should be noted that several important compliance aspects of the cross-border data transfer regime under the PDP Law still remain to be finalized. These aspects include the composition of required dossiers, specific conditions and procedures for conducting impact assessments, and criteria for when transfers may be suspended for national security reasons (Article 20.7). As it is unclear when the Draft Implementing Decree will be finalized and what its final text will be, this uncertainty presents significant challenges for organizations hoping to proactively design compliance programs to meet the new requirements. Organizations may perhaps refer to both the Draft Implementing Decree and the PDP Decree for an idea of what these unfinalized aspects may eventually look like.

At risk of further complicating the compliance picture, it should be remembered that Vietnam's [Decree detailing the implementation of the Law on Cybersecurity](#) (Decree No. 53/2022/ND-CP) (Cybersecurity Decree) maintains **data localization requirements**. Article 26 of the Cybersecurity Decree requires certain types of data to be stored in Vietnam, including personal information of Vietnamese service users, data created by users in Vietnam (such as account names, service usage times, IP addresses, and registered phone numbers), and data on user relationships (friends and groups). The Data Law also contains provisions on cross-border data transfers, which are further covered below. The interplay of these laws means that organizations must have a good understanding of what data they intend to transfer overseas and what purposes they want to transfer it for, to appreciate the compliance requirements they will be attracting.

f. The Ministry of Public Security remains the focal agency for data protection within a governance structure unique to Vietnam's context and needs

Compared to the PDP Decree, there does not appear to be significant changes as regards governance and enforcement responsibilities under the PDP Law. As before, **MPS remains the “focal agency” responsible for performing the state management of personal data protection**, save for personal data matters falling within the purview of the Ministry of National Defence (Articles 36.2 and 36.3). Perhaps the only notable change is that while the PDP Decree specifically stipulated responsibilities (mainly, providing guidance, handling communications activities and developing personal data protection standards) for two other ministries – the Ministry of Information and Communications and the Ministry of Science and Technology – these specific provisions no longer appear in the PDP Law. One could stipulate that this is because there is either no need or no intention for these agencies to continue

playing these roles. Either way, this change should not result in practical compliance changes for most organizations.

Within MPS, **the specific department responsible for personal data protection remains the Department of Cyber Security and High-tech Crime Prevention and Control** (also known as “A05”) (as stated in Article 28 of the Draft Implementing Decree). A05 is expected to continue to hold significant responsibilities, including reviewing impact assessments for cross-border personal data transfers and personal data processing activities, conducting inspections of cross-border data transfers, requesting the suspension of such transfers, and receiving and processing notifications of personal data protection violations (see e.g. Articles 20 – 23).

The differences in governance and enforcement approaches between the PDP Law and the GDPR could not be much starker. The PDP Law envisions a regulator (MPS) that performs the task of implementing the PDP Law, among other tasks (although A05, as the primary enforcement department, is a specialized department). MPS’ role also means that data protection enforcement continues to be heavily intertwined with national security, public order and cybersecurity objectives. In contrast, under the GDPR, each EU member state has an independent data protection authority (DPA) specifically in charge of implementing the GDPR. These DPAs are designed to act independently from government influence, while cooperating with each other through the European Data Protection Board for greater consistency across the EU (although each retains the power to investigate breaches and impose sanctions).

g. The PDP Law introduces a structured penalty framework covering organizational and individual liability

Unlike the PDP Decree, the PDP Law introduces a structured penalty framework with clearly defined maximum fines (Article 8). This addresses one of the notable gaps previously raised about the PDP Decree: that it did not include a specific penalty structure, but merely provided that violators may be subject to disciplinary action, administrative penalties, or criminal prosecution

For most violations under the PDP Law, organizations face:

- **For administrative violations generally:** Fines of up to VND 3 billion (approximately USD 115,000) (Article 8.5);

- **For violations of cross-border transfer regulations:** Fines of up to 5% of the preceding year's turnover for organizations. Where there is no turnover / the turnover-based calculation is lower than the VND 3 billion above, the maximum fine level of VND 3 billion shall apply (Article 8.4);
- **For violations relating to the act of buying and selling personal data:** Fines of up to 10 times the revenue obtained from the violation. Where there is no revenue / the revenue-based calculation is lower than VND 3 billion, the maximum fine level of VND 3 billion shall apply (Article 8.3).

Individuals who breach the PDP Law's requirements can also face personal liability, set at 50% of the penalties imposed on organizations (Article 8.6). This is one difference between the penalty framework under the PDP Law from the GDPR, which primarily focuses on organizational-based sanctions. (Another difference is that the fine levels under the PDP Law are lower than those of the GDPR, which can go up to 20 million euros). Following usual legislative practice in Vietnam, we can expect the Government to develop a separate sanctions decree regulating administrative penalties for each violation of the PDP Law.

h. The PDP Law is a unique legislative instrument that seeks to meet Vietnam's digital economy needs while navigating its development trajectory

In sum, the PDP Law illustrates the Vietnamese Government's (in particular, MPS) balancing of two aims: (a) ensuring overall consistency and continuity with the existing regime under the PDP Decree; (b) refining the regime based on experience and feedback gained from two years of implementing the PDP Decree. It also shows how the Vietnamese Government is attempting to rationalize a transition of the current data protection regime from that of a decree to a law (by for instance, keeping provisions in the PDP Law at a general level while allocating more administrative specifics to an implementing decree). The upshot is a uniquely Vietnamese data protection regime that seeks to energize socio-economic development and provide greater clarity for the digital economy, while maintaining due control over key issues of national security, cybersecurity and protecting the interests of agencies, organizations and individuals.

3. The intersection of the PDP Law and the Data Law creates compliance implications for organizations navigating cross-border data transfers

On 30 November 2024 – just seven months before the PDP Law was enacted – Vietnam’s National Assembly enacted the [Data Law](#) (Law No. 60/2024/QH2015). The Data Law is Vietnam’s first comprehensive framework for the governance of digital data (both personal and non-personal), and applies to all Vietnamese agencies, organizations and individuals, as well as foreign agencies, organizations and individuals either in Vietnam or directly participating or are related to digital data activities in Vietnam (Article 2 of the Data Law). Interestingly, the Data Law underwent a fast-tracked legislative process, with drafting finalized within 9 months. The Data Law came into force on 1 July 2025. This section will specifically highlight intersections between the Data Law and the PDP Law.

As mentioned above, **the Data Law establishes a governance framework for all categories of data**. Article 3 defines these data types, namely, “core data”, “important data”, “original data”, “open data”, “private data”, and “shared data”. The Data Law also establishes Vietnam’s data infrastructure, such as the National Data Centre, and a National Comprehensive Database (Articles 30 to 38 of the Data Law). These measures are aimed at fostering and standardizing data sharing across government agencies in a manner reminiscent of the EU’s [Data Act](#) (effective 12 September 2025) and its [Data Spaces](#) to be created subsequently. This stands in contrast to the PDP Law, which focuses specifically on personal data and sets out the rights of data subjects and the obligations of agencies, organizations and individuals in respect of personal data.

The Data Law’s broad data regulation mandate creates overlaps and potential **points of friction** with the PDP Law:

- a. **Cross-border data transfers.** Cross-border data transfers in Vietnam are governed by both PDP Law (Article 20 of the PDP Law) and Data Law (Article 23 of the Data Law). Overlaps arise when organizations are dealing with personal data that also qualifies as “core” or “important” data.

Under the PDP Law Article 20(5), organizations risk suspension of transfers if the transfer may cause harm to national defense or security. Similarly, the Data Law (Article 23) requires that the transferring and processing of “core” and “important” data ensure national defense and security, while also safeguarding national interests, public interests, and the legitimate rights of data subjects and owners. The key question is how implementation details under Article 23 of the Data Law will align with those under the PDP Law.

To some extent, Article 5(4) of the PDP Law provides relief, as organizations that have already carried out TIAs under the PDP Law are not required to conduct additional assessments under other “data-related” laws. However, under draft guiding decrees for the Data Law, personal data

classified as “core” or “important” data will be subject to requirements in the Data Law’s guiding decrees. Uncertainty therefore remains on this point.

There are also uncertainties relating to assessment frequency. Specifically, the Data Law requires regular periodic assessments for core and important data (Article 25(4)), while PDP Law impact assessments are conducted once for the entire operation period (with updates only when circumstances change) (Article 21(2)), creating a potential mismatch in assessment frequency and scope.

- b. **Alignment in approaches.** The PDP Law calls for consent-driven processing and prioritizes individual autonomy by providing a suite of data subject rights, while the Data Law is more focused on **data as a national asset**, emphasizing state control and national security (Article 6(1)). Organizations may find themselves navigating two competing frameworks: one focused on protecting data subjects’ rights, the other national interests.

Going forward, organizations should prepare to comply with *both* the Data Law and the PDP Law, monitor regulatory developments (such as forthcoming decrees or regulations from the Vietnamese Government), and pre-empt potential overlaps between both laws. To aid in compliance, organizations can proactively review and classify the data they process, paying particular attention to identifying datasets containing “core” and “important” data. Organizations should also assess their existing data processing practices to identify compliance gaps, and review internal procedures, policies and compliance programs in line with both laws.

4. Navigating the fast-transforming Vietnamese data regulatory landscape requires active monitoring, caution and curiosity

Within Southeast Asia and the Asia-Pacific (APAC) region, Vietnam stands out as a relatively active jurisdiction in reforming its digital regulatory landscape. As an illustration, when FPF published (in August 2022) a [jurisdictional report on Vietnam’s regulatory regime for consent](#), we observed:

“Vietnam’s existing data protection framework is highly fragmented. Vietnam does not currently have a comprehensive law regulating data protection and privacy, and instead, provisions on these issues (including several provisions on consent) are spread across various legal instruments.”

The present picture could not be more different. Since then, Vietnam has introduced two personal data protection regimes (first under the **PDP Decree**, followed by the PDP Law). It has introduced the **Data Law** to govern digital data. In June 2025, Vietnam also enacted a **Law on Digital Technology Industry** (which regulates digital technology industry activities, products and services – including AI, digital assets and semiconductors).

Most recently, in December 2025, Vietnam’s National Assembly [passed](#) the [Law on Artificial Intelligence](#) (AI Law) – the country’s first comprehensive national AI legislation. Effective from March 2026, the AI Law adopts a dual-purpose approach: It institutes a risk classification framework – covering high, medium, and low risk categories, while also prohibiting certain uses of AI – that determines compliance obligations for AI systems. At the same time, it also establishes a legal basis for the state to provide significant support to enable AI innovation, including establishing a National AI Development Fund.

This “promotion-plus-governance” approach closely aligns with that of other APAC AI laws passed in 2025, including [South Korea’s AI Framework Act](#), and [Japan’s AI Promotion Act](#). However, given its three-month implementation timeline, it remains to be seen whether Vietnam can successfully operationalize the AI Law – especially its complex conformity assessment provisions for high-risk AI systems – by the time that the Law enters into force.

While these instruments establish a more structured and comprehensive legal framework, they also introduce considerable complexity and potential points of friction for regulated entities (such as in the aspect of cross-border data transfers). Stepping back, however, we draw the following takeaways from the present regulatory framework (particularly, the PDP Law and Data Law).

First, cross-border data transfers is perhaps the *cause célèbre* of the inherent complexity in Vietnam’s digital regulatory landscape. The present regulatory regime doubles down on the state-supervised model for such transfers. The new PDP Law’s sole TIA mechanism for transfers, along with overlapping rules in the Data Law and data localization requirements under the Cybersecurity Decree demonstrate a continuing intent to ensure control over what data can leave Vietnam, while where possible, prevent compliance from becoming overly onerous.

Second, risk and impact assessments are emerging as a central, albeit uncertain, aspect of the new regime. Risk and impact assessments play a key role in both the PDP Law and the Data Law, but also inject potential uncertainties for organizations when these need to be submitted to MPS for inspection and assessment. As a related aside, the introduction of a risk-based classification system for AI systems under the Law on Digital Technology Industry and draft Law on AI further emphasizes this approach. It is

perhaps inescapable that organizations operating within Vietnam’s digital regulatory regime will need to act with a degree of **caution and curiosity** – caution in case something is unexpectedly flagged by the authorities, and curiosity to find out what seems to work (or not) from the experience of other organizations.

Third, there appears to be significant reliance on detailed secondary / implementing regulations, although this also perpetuates legal and business uncertainty. Throughout the PDP Law, for instance, numerous references are made to how the Government “shall detail / prescribe” more information in subsequent regulations. On one hand, this reduces time needed in the short-term for regulatory drafting. On the other hand, operational details for many key provisions, such as for categories of sensitive data, procedures for cross-border transfers and other compliance mechanisms remain uncertain. It is unclear if the Draft Implementing Decree will be finalized in time for the coming-into-force of the PDP Law (1 January 2026), but organizations should in any case prepare for a compressed compliance timeline for the incoming regulatory regime.

To ease pressure, organizations should perhaps bear two final points in mind. First, that the need for organizations operating in Vietnam to act with caution and curiosity is perhaps a feature, and not a bug, of the regime. Two, that rather than giving in to a “wait-to-rush, rush-to-wait” mindset, organizations can take some of the proactive steps outlined above to prepare themselves.



Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org