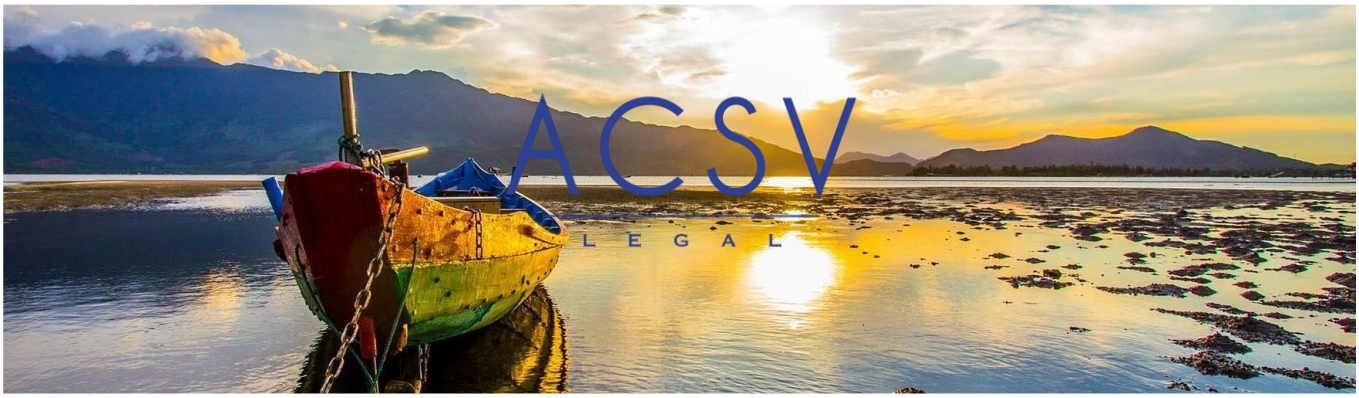


LEGAL UPDATE

BEYOND PERSONAL DATA PROTECTION: WHAT BUSINESSES NEED TO DO TO COMPLY WITH THE 2024 LAW ON DATA?

In recent years, beginning with the introduction of Decree No. 13/2023/ND-CP on personal data protection in 2023, many companies in Vietnam have prioritised compliance with personal data protection requirements, including fulfilling the reporting obligations ("**PDP Regulations**").

However, for certain companies, compliance with the PDP Regulations alone may not be sufficient. With the Law on Data No. 60/2024/QH15 ("**2024 Law on Data**"), Decree No. 165/2025/ND-CP ("**Decree 165**"), Decree No. 169/2025/ND-CP ("**Decree 169**") and other relevant implementing guidance taking effect from 1 July 2025 (collectively, "**Data Regulations**"), businesses are now subject to a broader and more comprehensive data governance framework that extends beyond personal data and applies to all digital data generated, managed or processed in the course of business operations.

The Data Regulations introduce additional obligations relating to data classification, data governance, data security, and certain data-related activities, which operate alongside, rather than replace, the personal data protection regime. As a result, businesses that have already taken steps to comply with the PDP Regulations may still need to assess whether further measures are required to meet their obligations under the Data Regulations.

This legal update outlines selected areas where businesses may need to take additional or separate compliance steps under the Data Regulations, building on their existing personal data protection compliance efforts.

1. General and baseline obligations

Businesses engaging in digital data activities are subject to a set of baseline obligations under the Data Regulations, to the extent such activities fall within the scope of the 2024 Law on Data. These include the followings:

- **Data processing principles**: The collection, updating and processing of data must ensure accuracy, integrity, reliability, security and safety throughout the data lifecycle.
- **Responsibility for data collection**: Businesses may collect data for their operational purposes, but remain responsible for the integrity and accuracy of the data they collect and use.
- **Provision of data to competent authorities**: Businesses are required to provide data to competent state authorities upon request in emergency situations, or circumstances involving threats to national security, as well as for disaster response or the prevention and suppression of riots or terrorist activities even without the consent of the data subject.

2. Identifying data categories and the company's role

From a business perspective, the obligations under the 2024 Law on Data primarily attach to two key roles, namely the data owner and the data administrator. More stringent obligations apply where these entities create, collect, manage or process digital data classified as important data or core data. Accordingly, as a first step, businesses should focus on the following:

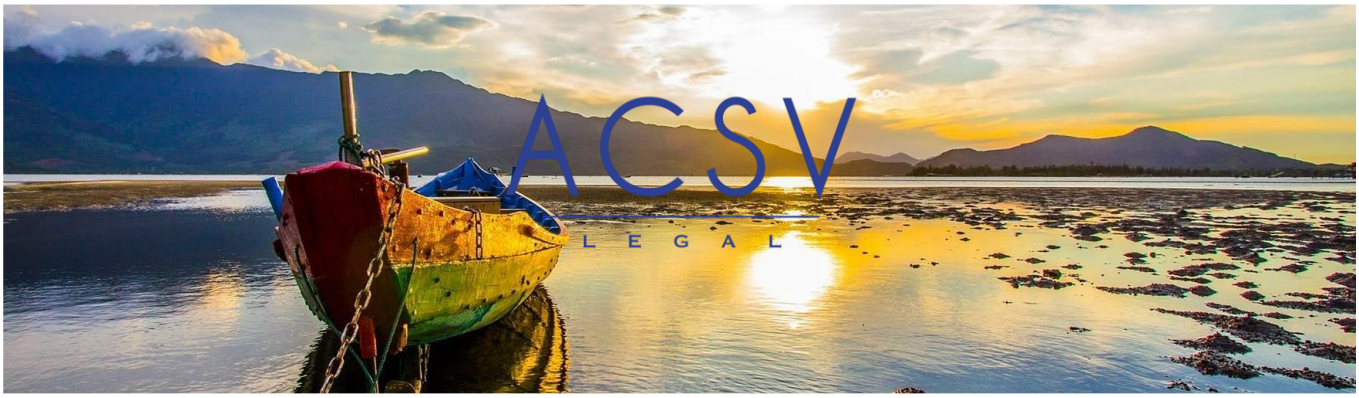
- **Determining the company's role**

  Specific obligations under the 2024 Law on Data vary depending on the role that a company plays in relation to a particular data activity. In this regard:

  - A data owner is an agency, organisation or individual that has the right to decide on the creation, development, protection, governance, processing, use and value exchange of the data it owns.
  - A data administrator is an agency, organisation or individual that builds, manages, operates or exploits data at the request of the data owner.

  Based on these definitions and their actual data-related activities, businesses should determine their role on an activity-by-activity basis to identify the corresponding obligations under the Data Regulations.

  Businesses should also note that these concepts are not equivalent to, and should not be conflated with,



the roles of personal data controller and personal data processor under the PDP Regulations.

- **Data classification**
  Unlike the PDP Regulations, which classifies personal data primarily by reference to sensitivity, the 2024 Law on Data requires data owner and data administrator to classify all digital data that they create, collect, manage or process into core data, important data, or other categories of data.

  To support this classification exercise, the Vietnamese Government has issued criteria for determining important data and core data, together with a formal list of important data and core data, which the data owner and data administrator may use as a reference when assessing the nature of their data.

  Based on this list, the following categories are particularly notable:

Data type	Important data	Core data
Non-public basic data of Vietnamese citizens	From 100,000 to 999,999 Vietnamese citizens	1,000,000 Vietnamese citizens or more
Non-public sensitive data of Vietnamese citizens	From 10,000 to 99,999 Vietnamese citizens	100,000 Vietnamese citizens or more
Non-public data relating to bank accounts, payment history and debt obligations	From 10,000 to 99,999 Vietnamese enterprises or organisations	100,000 Vietnamese enterprises or organisations or more

  Based on the above thresholds, sectors such as banking and finance, telecommunications, healthcare, education, transportation, technology, fintech and e-commerce are more likely to be impacted, particularly where data is processed at a large scale.

3. Cross-border transfer of core data or important data

As a general rule, prior to the cross-border transfer or processing of core data and/or important data, the data owner and the data administrator are required to prepare and regularly update a data impact assessment dossier and submit it to the Ministry of Public Security ("**MPS**") or the Ministry of National Defense ("**MND**"), as applicable, in accordance with the procedures applicable to each category of data, for approval, inspection and assessment before such transfer or processing is carried out.

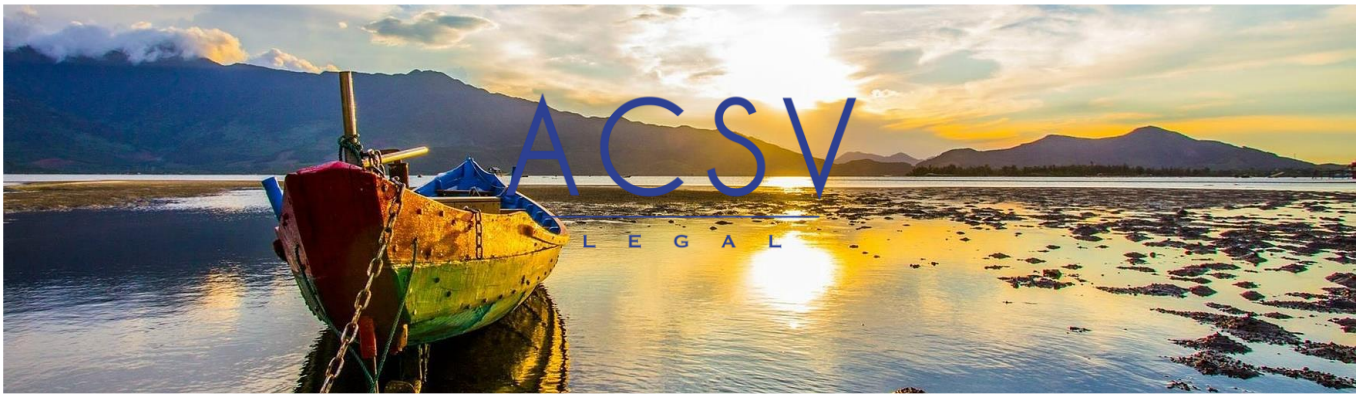
In limited circumstances, certain cross-border transfers or processing of core data and/or important data may be carried out without prior approval or notification, including: (i) emergency situations where the transfer is strictly necessary to protect life, health or property, or to perform statutory duties, (ii) cross-border human resources management conducted in accordance with applicable labour regulations and collective labour agreements, and (iii) transfers strictly necessary for the conclusion or performance of contracts, including those relating to cross-border transportation, logistics, payments, bank account opening, hotel services, visa applications and inspection services. In these cases, a post-transfer impact assessment must be submitted to the MPS, or the MND where applicable, within the statutory timeframe following the commencement of the transfer or processing.

Where the relevant core data or important data entirely consists of personal data, and the data administrator has already completed and submitted a data impact assessment in accordance with the PDP Regulations, a separate impact assessment under the Data Regulations is not required.

4. Key obligations of data owners and data administrators

Set out below are a number of notable obligations applicable to the data owner and the data administrator under the Data Regulations:

- **Data verification processes:** The data owner and the data administrator are responsible for establishing data



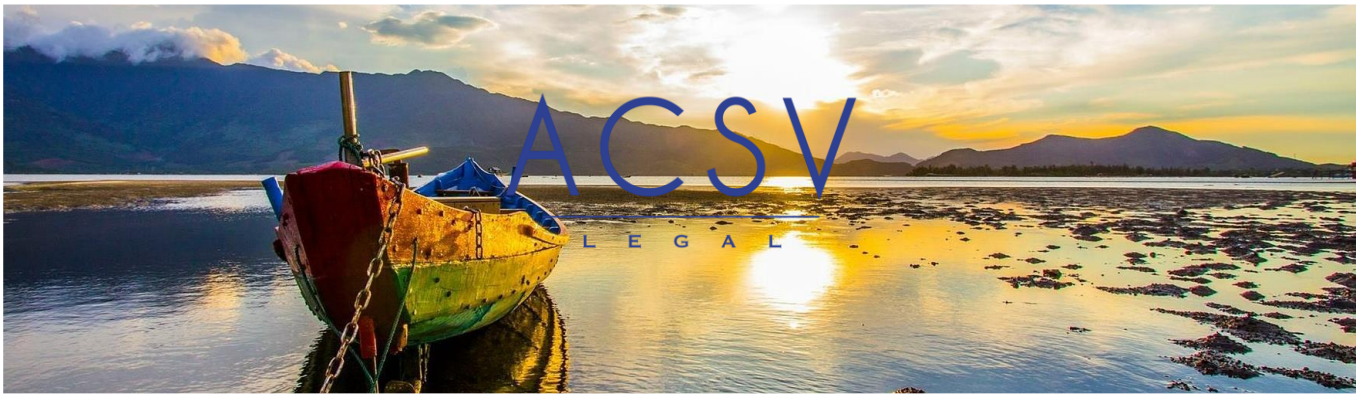
verification processes, including the methods, procedures and organisational arrangements for verifying data.

- **Risk identification and management:** The data administrator is required to assess and identify data-related risks, including risks relating to privacy, cybersecurity, identity and access management, and other relevant risks, and to implement appropriate measures to protect data. The data administrator must promptly address emerging risks and notify data subjects, as well as the relevant agencies, organisations or individuals, where required. In addition, the data administrator must conduct annual risk assessments in respect of the processing of core data and important data and notify the specialised unit of the MPS or the MND, as applicable, unless a data impact assessment for cross-border transfer or processing has already been completed in accordance with Section 3 above.
- **Responding to data subject requests:** The data administrator is required to establish procedures and implement measures to retrieve, delete or destroy data in accordance with applicable laws, including, where required, deleting or destroying data within 72 hours following a request from the data subject.
- **Implementation of data protection measures:** The data owner and the data administrator must establish data protection policies, manage data processing activities, implement appropriate technical solutions, and provide training to personnel involved in data processing. Enhanced technical, organisational and management measures apply where core data or important data is involved, reflecting the higher level of risk associated with such data categories.
- **Data processing logs**: The data administrator handling core data or important data is required to maintain data processing logs throughout the entire data processing lifecycle. Such logs must be retained for a minimum period of six months.
- **Personnel management**: The data owner and the data administrator must designate data protection officer and establish data protection department in relation to core data and important data. They are also required to define data security requirements in recruitment processes, enter into confidentiality responsibility arrangements with personnel involved in data processing, and conduct annual data protection training for relevant staff.
- **Data security monitoring, early warning and emergency management**: The data administrator is responsible for promptly notifying the data owner of data security incidents that may affect the lawful rights and interests of individuals or organisations and proposing mitigation measures; implementing emergency response actions in accordance with the approved incident response plan and reporting incidents involving important data or core data to the MPS or the MND, as applicable, as soon as possible; continuously monitoring and assessing data security risks and adopting preventive measures; timely reporting risks that may lead to major data security incidents to the MPS; and conducting periodic emergency drills for important data and core data at least once every six months, including maintaining records, submitting summary reports and updating back-up plans in response to material changes in data processing systems or the external environment.

5. Sector-specific data services

Certain data-related activities are governed by sector-specific regulatory regimes, with additional requirements set out in specialised implementing decrees, alongside the general data governance and personal data protection framework. In particular:

- Medical data management services are subject to sector-specific requirements set out in specialised implementing regulations, which supplement the general framework on data governance and personal data protection. These rules introduce additional obligations in relation to the access, processing and protection of digital medical data, with particular focus on consent standards, data subject rights and compliance responsibilities applicable to both domestic and foreign entities involved in medical data-related activities in Vietnam.
- Data-related services under the 2024 Law on Data, including data intermediary services, and data analysis and synthesis services are likewise governed by additional regulatory requirements under specialised implementing decrees. Depending on the nature of the service and the category of data involved, these requirements may include licensing, operational and security conditions, reflecting heightened regulatory attention to activities



involving large-scale data sharing, aggregation or commercial use.

6. Sanctioning framework

As of the date of this legal update, the Government has released the second draft decree on administrative sanctions in the data sector for public consultation in December 2025 (the "**Draft Sanctioning Decree**"). The timeline for its issuance has not yet been announced.

In terms of scope, the Draft Sanctioning Decree broadly follows the structure and key regulatory contents of the 2024 Law on Data, and largely reflects the obligations set out in Decree 165 on data governance, classification and security, as well as Decree 169 on data-related services. Violations are organised by reference to different types of data activities, providing enforcement authorities with a degree of flexibility in addressing non-compliance.

At the same time, this approach results in a relatively high level of detail and fragmentation, under which a single course of conduct may fall within multiple violation categories, particularly in areas relating to data governance and data security. In the absence of consistent enforcement guidelines, this may create challenges in delineating violations and increase the risk of overlapping sanctions.

In view of the proposed sanctions, the monetary fines are high and strongly deterrent, with clear differentiation based on the type of data involved and the magnitude of the violation. Breaches involving core data and important data are subject to the highest penalty thresholds. Notably, violations relating to transactions conducted on the data exchange platform, including the organisation of tradings involving core data, important data or personal data without legitimate consent, may attract fines of up to VND 2 billion.

In addition to monetary fines, the Draft Sanctioning Decree places significant emphasis on supplementary sanctions and remedial measures, including suspension of operations, revocation or restriction of certain rights relating to data access or databases, and corrective actions such as mandatory remediation of violations, technical system upgrades or security enhancements, disgorgement of unlawfully obtained benefits, and public notification of violations. For data-driven businesses, these measures may have a material operational impact, potentially exceeding the financial consequences of the fines themselves.

7. Conclusion

The Data Regulations do not replace or override the personal data protection regime, but instead introduce an additional layer of obligations relating to data governance, data use and data protection at an organisational level.

For many businesses, particularly those that do not operate data-driven models or process data at a large scale, the impact of the Data Regulations may be limited to a set of baseline requirements. By contrast, for businesses acting as data owners or data administrators, or those involved in the processing of important data or core data, the compliance obligations become more complex. In such cases, closer attention is required in relation to data classification, governance structures, security measures and cross-border data arrangements.

Against this background, businesses that have already taken steps to comply with personal data protection requirements are encouraged to assess whether their activities give rise to additional obligations under the Data Regulations. Proactive review and early preparation at this stage can help mitigate legal risks and ensure operational readiness for future regulatory inspection, audit and enforcement activities.

For further information or assistance in understanding the implications of the Data Regulations, please contact:

Minh Nguyen / Special Counsel
minh.nguyen@acsvlegal.com

Ly Nguyen / Associate
ly.nguyen@acsvlegal.com