KPMG

Legal Alert

February 2025

VIETNAM'S DRAFT DECREES ON DATA REGULATION

Vietnam is entering a pivotal phase in data governance, with new regulations set to shape the future of data activities. Recognising data as a strategic national asset essential to security, defence, and economic stability, the Government is strengthening regulations to better oversee sensitive data, prevent unauthorised data trading, and provide clear legal guidelines for businesses in the data economy. These changes seek to balance three key priorities: national security and defence, the growth of data-driven businesses - including maximising business value in the digital economy - and the protection of personal data as a fundamental human right.

In November 2024, Vietnam's National Assembly passed the Law on Data, which establishes a legal foundation for digital data management, security, processing, and use. It also mandates the creation of a National Data Centre and integrated National Database to improve state management and transparency.

Following this, the Government released important draft instruments in January 2025 to implement the law, including:

- Draft Decree on Detailed Regulations and Implementation Measures for the Law on Data.
- Draft Decree on Scientific, Technological, and Innovative Activities and Data-Related Services.
- Draft Decree on the National Data Development Fund.
- Draft Decision on Core and Critical Data Classification.

These drafts are open for consultation until mid-March 2025.

Key Takeaways for Businesses

- Stricter compliance for organisations and businesses handling Core or Critical Data, including risk assessments, regulatory filings, and government approvals for cross-border transfers.
- Data service providers - including data intermediaries, data analytics, and data exchange platforms - must adhere to rigorous licensing and compliance standards.
- Clear regulations on the mandatory provision of data to state authorities are now established.
- Expected improvements in accessibility will allow businesses to obtain high-quality data more efficiently in terms of both time and cost.

Who Will Be Affected and How?

The draft regulations cover all major data categories - governmental, business, and personal data - with significant impacts on businesses handling sensitive data. The strictest provisions apply to Core Data and Critical Data, requiring self-regulation, impact assessments, and mandatory regulatory filings.

- Core Data includes highly sensitive information affecting national security, defence, foreign affairs, economic stability, public health, and social order.
- Critical Data covers data with potential impacts on these same domains, requiring heightened security and compliance measures.

According to the Draft Decision on Core and Critical Data, most regulated data pertains to government activities, including national security, emergency response, financial systems, healthcare, infrastructure, and environmental incidents. However, certain private sector data also falls under these classifications, such as:

- ***Core Data:***
  - Cross-border banking transactions exceeding 50,000 transactions.
- ***Critical Data:***
  - Health records and biometric data of 10,000+ individuals.
  - Confidential banking data, corporate accounts, and loan transactions of 1,000,000+ individuals.
  - Insurance contracts, claims, and payouts of 10,000+ customers.
  - Internet behaviour data of 100,000+ users.
  - Basic personal data of 1,000,000+ individuals and other sensitive data of 10,000+ individuals.

Businesses managing such data are required to perform risk assessments and submit impact assessment reports to the Ministry of Public Security or the Ministry of National Defence prior to transferring or processing Core or Critical Data across borders.

Transfers of Core Data require government approval with a 10-day review period, while Critical Data transfers require a five-day prior notification, with authorities able to halt transfers if security risks arise. Businesses must also conduct biannual risk assessments for Core Data and annual assessments for Critical Data, updating reports when significant changes occur.

Impact on Data-Related Businesses

Businesses engaged in data processing, analysis, and exchange services face new compliance requirements. Key areas of impact include:

- Data intermediary service providers - such as companies offering data storage, hosting, API management, and integration services - must meet business investment, personnel, technical, security, and financial requirements, though only those facilitating data exchange between private users and state agencies require licensing.
- Data analysis and aggregation service providers must obtain a Business Eligibility Certificate if they:
  - Offer Level 3 or Level 4 data analysis services within critical national information systems (e.g., security, defence, healthcare, transportation, and justice), where Level 3 supports decision-making under human supervision, while Level 4 operates autonomously without oversight; or
  - Utilise national or specialised databases to provide data analysis services for individuals or organisations.
- Data exchange platforms - organisations engaged in data trading, brokerage, valuation, technical support, negotiation, auctions, and other data-related transactions - can only operate if they are state-owned or public service units that meet licensing conditions.

The recognition of “data exchange platforms” in Vietnamese laws marks a significant advancement in the accessibility of data for research and development (R&D) and high-tech activities. This legal acknowledgement is poised to facilitate more efficient data sharing and reduce the costs associated with accessing essential data. By establishing clear legal frameworks, the likelihood of illegal data trading will be minimised, ensuring that data is exchanged securely and ethically. This development is expected to boost innovation and technological growth as researchers and developers gain easier access to the data they need. Furthermore, the legal requirements for data exchange platforms - such as state ownership or public service unit status and meeting specified licensing conditions - ensure that these platforms operate with a high level of accountability and

transparency. This regulatory oversight is designed to protect the interests of data providers and users alike, fostering a trustworthy environment for data transactions.

Mandatory Data Provision to State Authorities

A noteworthy provision in the Draft Decree on Data Law Implementation concerns mandatory data sharing with government agencies. The decree encourages voluntary data sharing for public benefits (e.g., healthcare, climate change, and transportation improvement). However, in special cases, businesses must comply with mandatory data requests from competent authorities, provided the request is clearly defined, legally justified, and time-bound.

Data requests must:

- Be documented and specify purpose, duration, and legal basis.
- Allow data owners to request modifications or withdrawals before the designated deadline.
- Be revoked if found unlawful or if the requested data is no longer available.

What's Next?

Vietnam's evolving data regulatory landscape presents both challenges and opportunities for businesses. While stricter controls aim to enhance national security and data integrity, a clearer legal framework may also help businesses operate more confidently in the digital economy. Businesses should stay informed, proactively assess compliance risks, and adapt to new regulatory expectations.

With public consultations ongoing until mid-March 2025, businesses should:

- Assess if their data falls under Core or Critical Data classifications and prepare for compliance.
- Review data handling and transfer processes to align with regulatory requirements.
- Engage in industry discussions and feedback sessions to influence the final regulations.

As a market leader in data, privacy, and security regulation, KPMG is well-positioned to support your company during this early preparation and advocacy stage. Please feel free to contact us for any inquiries or assistance requests.

Contact us

Email: info@kpmg.com.vn

Scan to visit our website: kpmg.com.vn