

The Andersen logo features a stylized white wing above the word "ANDERSEN" in a white, serif, all-caps font. The background of the entire page is a satellite-style image of Earth from space, showing the curvature of the planet and the glowing lights of cities and infrastructure across Asia and the Pacific region.

ANDERSEN®

# VIETNAM

**Legal and Tax Digest**

September 2025

## Digital Assets

*Resolution No. 05/2025/NQ-CP on the “Implementation of a Pilot Crypto Asset Market in Vietnam” promulgated on September 9, 2025*

This resolution, which enters into effect immediately, establishes Vietnam’s first pilot program for a regulated crypto asset market, aiming to foster a transparent, safe, and controlled environment for the issuance, trading, and servicing of crypto assets. It applies to Vietnamese issuing organizations, licensed service providers, and both domestic and foreign investors, and aligns with laws on anti-money laundering, terrorism financing, network security, data protection, and electronic transactions.

Key highlights of the program are discussed below.

### **Crypto assets defined**

Crypto assets are now recognized as a type of digital asset under the Civil Code, represented in digital data form and authenticated using encryption or similar digital technologies during creation, issuance, storage, and transfer. They do not include securities, digital forms of fiat currency, or other financial assets regulated by civil or financial laws.

This definition aligns with provisions of the **Digital Technology Industry Law** (effective January 1, 2026).

### **Issuance and offering requirements**

Issuing organizations must be Vietnamese enterprises structured as limited liability companies or joint-stock companies under the Enterprise Law. Crypto assets must be backed by underlying real assets (excluding securities or fiat currency).

Offerings and issuances are limited to foreign investors, with trading permitted only among foreign investors through licensed service providers.

### **Licensing for crypto asset service providers**

Service providers (handling trading markets, self-trading, custody, or issuance platforms) must obtain a license from the Ministry of Finance.

Key conditions include having:

- **Minimum charter capital of VND 10 trillion** (approx. US\$ 400 million). At least 65% of the capital must be contributed by organizations, with at least two such contributors are banks, securities companies, insurance firms, or technology enterprises. Organizational contributors must have been profitable for the prior two years. Foreign ownership is **capped at 49%**, and no individual or organization may contribute to more than one licensed provider.
- **Adequate office facilities, technical equipment, and an IT system meeting level 4 information security standards**, including risk management, security, and customer asset protection processes.

- **Qualified personnel**, including the General Director, who must have at least two years' experience in finance, securities, banking, insurance, or fund management; the Chief Technology Officer, who must have at least five years' experience in IT; at least 10 IT staff with network security qualifications; and at least 10 staff with securities practice certificates.

### **Trading platforms and custody**

Trading must occur through licensed providers' platforms, which aggregate orders, facilitate exchanges, and handle settlements.

Licensed providers' custody services involve storing, preserving, and transferring assets on behalf of clients.

Domestic investors must transfer existing crypto assets to licensed providers for centralized custody and trading **within six months** after the first license is issued; non-compliance may result in penalties.

### **Investor obligations and protections**

Foreign investors must open dedicated VND accounts at authorized Vietnamese banks for transactions, including foreign currency conversions, asset sale proceeds, and interest. Banks managing these accounts must verify documents, store records, and report periodically to the regulatory authorities.

Both domestic and foreign investors must declare transaction details accurately and comply with anti-money laundering, anti-terrorism financing, and tax evasion prevention rules.

All transactions must be conducted in VND, and the tax treatment of crypto assets will follow the policies set out for securities until specific crypto asset regulations are issued.

The program, which runs for a five-year period, emphasizes caution, risk control, transparency, efficiency, and the protection of participants' rights and interests. After the pilot ends, the market will continue operating under this resolution until amended or replaced by new legislation.

## **AI and Personal Data**

---

*Draft "Law on Artificial Intelligence" released for public consultation in September 2025*

This law establishes Vietnam's first comprehensive legal framework for the research, development, provision, deployment, and use of artificial intelligence ("AI") systems. It aims to promote innovation, ensure safety, ethics, and the protection of rights while balancing technological advancement with risk management.

The draft has been released for public consultation and is scheduled for enactment during the National Assembly's 10th session starting October 20, 2025, with phased implementation to begin January 1, 2026, and key obligations from 2027.

The law applies to domestic AI activities and holds international entities accountable if their AI systems impact the Vietnamese market, users, or legal interests. It excludes AI systems used solely for national defense, security, or intelligence, which require separate compliance frameworks.

We highlight the main points of the new law (note that the law is still in draft form, so some or all of these provisions are subject to change until it has been officially enacted by the National Assembly).

### **Definitions**

- **AI:** A branch of computer science focused on creating machine-based systems capable of performing tasks requiring human intelligence.
- **AI system:** An autonomous machine-based system that influences physical or digital environments.

### **Classifications of AI systems**

AI systems are classified into the four risk-based categories below; the government will issue in the future detailed criteria, ways to identify them, and examples:

- **Unacceptable risk:** Systems that threaten national security, human rights, or social stability are prohibited.
- **High risk:** Systems in critical sectors (e.g. healthcare, finance, transportation) that could significantly affect life, health, or rights. These require prior government approval, registration, conformity and impact assessments, transparency, and ongoing surveillance.
- **Medium risk:** Systems involving direct human interaction or content generation (e.g. chatbots, generative AI). These are subject to transparency requirements, such as notifying users of artificial content.
- **Low risk:** All other systems that do not fall into any of the above categories. Entities using these systems are encouraged to follow voluntary technical standards, with post-inspection if risks emerge.

Entities must conduct self-assessments, maintain documentation, and register high-risk systems before market entry. Foreign providers must appoint a local legal representative for compliance.

### **Key principles in developing the framework for AI-related activities:**

- **Human-centric:** AI must serve humans, respect dignity, freedom, privacy, and cultural values; it cannot replace humans in critical decisions and must remain under human control, supervision, and accountability.
- **Safety, fairness, transparency, and accountability:** AI systems must be safe, reliable, secure, fair, non-discriminatory, transparent (especially for high-risk systems). Developers and operators bear responsibility for legal and ethical compliance.

- **National autonomy and international integration:** AI activities should foster self-reliance in technology, infrastructure, data, and AI models while harmonizing with international standards and practices.
- **Inclusive and sustainable development:** AI should be aligned with socioeconomic goals, ensure equitable access, protect the environment, and preserve cultural identity.
- **Balance and harmony:** There should be balance and harmony in AI policy formulation and implementation.
- **Risk-based management:** Measures should be applied in proportion to risk levels, mandating regulation only for systems with clear harm potential.
- **Promote innovation:** The framework should create a favorable environment for research, startups, and commercialization.

### **Prohibited acts**

The draft law prohibits AI systems or activities posing unacceptable risks, such as:

- Manipulating human cognition or behavior to cause physical/psychological harm or impair autonomy.
- Exploiting the vulnerabilities of specific groups (e.g. based on age, disability) to encourage detrimental behavior.
- Widespread social credit scoring by state agencies leading to unfair discrimination.
- Real-time remote biometric identification in public spaces for law enforcement (except in authorized serious crime cases).
- Building large-scale facial recognition databases via indiscriminate data scraping from the internet or cameras.
- Using emotion recognition in workplaces or educational institutions (except for permitted medical/safety reasons).
- Producing or disseminating deepfakes or AI-generated content harming the social order, safety, or national security.
- Developing/using AI to oppose the State of the Socialist Republic of Vietnam.
- Other cases as regulated by the government after consultation.

Violations may lead to administrative sanctions, criminal prosecution, or civil liability.

### **Responsibilities of organizations and individuals**

Organizations and individuals have the responsibility to:

- Conduct risk self-assessments and comply with classification requirements.
- Register high-risk systems in the national AI database for transparency and accountability.
- Ensure human oversight, with final control and accountability resting with humans, especially in critical decisions.

- Appoint local representatives (for foreign entities) and handle appeals against government interventions.
- Invest in data security, team capabilities, and ethical protocols; entities contributing data to the national AI data system may receive incentives like tax relief or funding priority.
- Parties affected by AI systems can appeal government actions or pursue legal remedies.

### Regulatory requirements

- High-risk systems require mandatory registration, conformity assessments, and impact evaluations before deployment.
- Authorities can suspend, restrict, or terminate harmful AI activities, with providers notified and able to appeal.

### Other significant details

- **Public-private partnerships:** AI data and models can serve as capital contributions in infrastructure projects.
- **National AI development fund:** This is a non-budgetary fund for research, innovation, and capacity building, offering grants/loans to startups and small- and medium-sized entities (“SMEs”).
- **Support for SMEs:** Support includes tax incentives, research and development vouchers, regulatory sandboxes, training, and streamlined procedures.
- **AI clusters:** The government may establish innovation zones with access to resources, tax reductions, land incentives, and fast-tracked processes to foster collaboration and commercialization.

---

*Draft Decree “Detailing Certain Provisions of the Law on Personal Data Protection Decree” released for public consultation in July 2025 and open for comments until September 26, 2025*

The decree provides detailed guidance on implementing the Personal Data Protection Law No. 91/2025/QH15 (“PDPL”), operationalizing procedures, timelines, templates, and enforcement mechanisms. It builds on Decree No. 13/2023/ND-CP while expanding definitions, clarifying responsibilities, and introducing new requirements for consent, assessments, transfers, and services. The decree is expected to take effect on January 1, 2026 in line with the PDPL’s effectiveness. We provide highlights of the decree below.

### Definitions

- **Basic personal data:** These reflect a person’s normal personal background and identity used in transactions/social relationships, defined generally rather than an exhaustive list (shifting from the specifics under Decree 13/2023/ND-CP).
- **Sensitive personal data:** These data are related to an individual’s privacy; infringement directly affects the rights/interests of agencies, organizations, or individuals. **The decree**

**provides an expanded list with new categories** — race/ethnicity, religion, health, biometrics/genetics, sexual orientation, criminal data, location, electronic identity (e.g. login ids and passwords), banking/financial/credit/insurance data, telecommunications subscriber activity/history, and data tracking behavior/usage of telecommunications, social networks, online media, or other online services (e.g. analytics, ads, fingerprints).

### **Data subject rights**

- Controllers must establish clear processes and forms to handle data subject's request processing within strict timelines:
  - Acknowledge requests (e.g. withdraw/restrict/object, access/correct, provide/erase) within two working days.
  - Complete processing of requests: Seven working days for withdraw/restrict/object requests; 10 working days for access/correct/provide/erase requests (15 days if processors (such as cloud providers) or other third parties are involved); extendable by up to 10 days with notice to the data subject.
- In the event of a dispute, the burden of proof of consent lies with the controllers/processors.
- Data subjects can authorize representatives (per civil law) to handle procedures, with full information and consent required.
- Rights must be delivered clearly, ensuring regulatory compliance and the prevention of unauthorized disclosure.

### **Responsibilities of controllers and processors**

- Controllers/Data Controller-Processors must:
  - Obtain verifiable consent from the data subject with evidence of method, time, content, and authentication.
  - Develop internal data-sharing policies.
  - Conduct periodic compliance reviews/risk controls.
  - Prepare Data Processing Impact Assessment (“**DPIA**”)/ Data Transfer Impact Assessment (“**DTIA**”).
  - Manage incident reporting.
  - Implement technical security (e.g. encryption at rest/transit, access controls).
  - Designate qualified data protection officers (“**DPOs**”) or departments (optional, but with written appointments, roles, and confidentiality agreements).
  - Handle data subject rights.
  - Engage qualified service providers, if needed.
- DPOs require a university degree, **3+ years relevant experience, a specialized training certificate**, and no criminal record related to data/cybersecurity.
- Processors must ensure appropriate measures in contracts defining roles, data flows, and obligations and they must not store raw personal data on blockchain (only encrypted/hashes are to be used, with annual reviews and DPIA).

- Organizations may outsource to qualified data protection service providers (with public disclosure), who must offer tech/legal advisory, have 3+ qualified staff, and maintain capability profiles.

### **Consent requirements**

The decree provides details on how consent is obtained from data subjects, as below:

- **Methods:** Written, voice, SMS, email/website/app with verification mechanisms, or other verifiable/authenticable ways.
- **Prohibitions:** Pre-ticked boxes, default settings, confusing instructions, dark patterns, or misleading tactics; defaults must respect privacy and uphold rights.
- **For sensitive data:** Data subjects must be explicitly informed of the sensitivity of the data. Controllers/processors must obtain an opt-in; no pre-consent tracking is allowed (e.g. block scripts until consent).
- Consent is valid until withdrawn or ordered otherwise; exemptions include contractual/legal obligations, vital interests, emergencies, or narrow legitimate interests (with monitoring/safeguards).

### **Sensitive data processing**

- There must be restricted access, specific procedures, strict security (e.g. encryption/anonymization for transfers).
- Behavioral tracking (e.g. on online services) is treated as sensitive and needs an explicit opt-in and no pre-consent loading.
- As discussed above, the categories of what constitutes sensitive data have been expanded, impacting digital operations like ads and analytics.

### **Personal data processing services**

- This is a new conditional business sector requiring a certificate of eligibility from the Ministry of Public Security (“**MPS**”).
- Services included under this category are: automated systems/software for processing; credit scoring/ranking; online data collection from websites/apps/social networks; surveys/market research; health monitoring/medical services; educational apps with monitoring (e.g. attendance, behavior/emotion recognition); data analysis/mining (e.g. trends, predictions, optimization); encryption; AI/blockchain/virtual reality-based processing; and location data platforms.

### **Other significant details**

- **Blockchain:** Encryption/hashes only; annual reviews and DPIA required.
- **Big data:** Apply encryption, anonymization, tight access controls, and real-time monitoring.
- **Enforcement:** The MPS has suspension powers for transfers and is responsible for inspections and training. No specific penalties for violations are detailed in the decree, but

we assume they will follow those under the PDPL (up to 5% of revenue or VND3 billion (approx. US\$120,000)).

## Investment

---

*Draft “**Business Investment Law**” released for public consultation by the Ministry of Finance in 2025 and open for comments as of October 2025.*

The Business Investment Law will replace the current Investment Law 2020, it is still in draft form but is expected to enter into effect from July 1, 2026.

Updates include simplified administrative procedures, reduced conditional business lines, enhanced flexibility in investment incentives, and the delegation of detailed regulations to the government to allow it to adapt to socioeconomic changes.

### **Simplified procedures**

- The current order of establishment procedures for foreign investors has been reversed—foreign investors first obtain an enterprise registration certificate to establish the project company and then apply for an investment registration certificate (“**IRC**”). This allows a commercial presence before project approval but introduces uncertainties around interim operations and liquidation if the IRC application is rejected.
- Exemption from having to obtain investment policy approval (“**IPA**”) is now applicable to projects detailed in national/provincial plans (e.g. name, scale, location, timeline); those won via land auctions, project bidding, mineral rights auctions, or industrial cluster assignments; and other government-specified cases. IPA is limited to high-impact projects only.
- IPA adjustments are required only for changes in principal objectives, additions in approval-scope objectives, or increases in State-allocated land without auction/bidding. Adjustments are no longer required for location, capital, or technology changes.
- Projects of less than VND20 billion (approx. US\$800,000) are exempted from having to obtain an outbound investment registration certificate—only foreign exchange registration with the State Bank of Vietnam is required for capital transfers. Projects of VND 20billion and more fall under the Ministry of Finance’s authority.

### **Conditional sectors**

- The number of business lines has been reduced, eliminating: accounting services; rice exportation; frozen food importation/re-exportation; foreign goods trading; employment/labor subcontracting; automobile maintenance; vessel/shipbuilding/repair; unmanned aircraft activities; foreign construction; cremation operations; overseas study consultancy; film distribution; performing arts/contests; and printing/minting (with proposals to narrow others like animal feed trading).

### Investor rights and obligations

- Foreign investors can establish entities before obtaining an IRC, subject to market access conditions.
- Project termination grounds have been expanded to include land recovery (any reason, per the Land Law), enterprise dissolution/bankruptcy/cessation, or investor death/declaration of death without a will.

## Authors and Contacts



**Ha Kim Quyen**  
Legal Associate  
[quyen.ha@vn.Andersen.com](mailto:quyen.ha@vn.Andersen.com)



**Pham Ngoc Thuan**  
Director  
[thuan.pham@vn.Andersen.com](mailto:thuan.pham@vn.Andersen.com)