ANDERSEN

VIETNAM

Legal and Tax Digest

January 2026

Data Privacy

> *Decree No. 356/2025/ND-CP dated December 31, 2025 "**Elaborating on Certain Articles and Implementation Measures of the Law on Personal Data Protection**"*

Under the decree, which took effect on January 1, 2026, Vietnam moves from piloting implementation to the formal enforcement of the Law on Personal Data Protection, with stricter documentation and cross-border transfer requirements. Personal data protection is affirmed as an inviolable right, with all processing requiring lawful purposes and data subject to consent except where otherwise provided by law. Key highlights of the decree are summarized below.

Main focus areas

Data processing impact assessment procedures

- Cross-border data transfer requirements
- Data protection officer regulations
- Standardized reporting systems
- Inspection coordination mechanisms

Data classification

Basic personal data: Revised catalog with adjusted categories.

Sensitive personal data: Enhanced catalog requiring stricter protection measures.

Data subject rights

- Consent mechanisms:
  - Controllers must establish verifiable consent processes.
  - There must be a clear timeline for responding to consent withdrawal requests.
  - Procedures must align with processing activities.
- Exercising of rights:
  - The decree specifies mandatory procedures for data access, rectification, and erasure of requests.

Sector-specific regulations

The decree lays out detailed requirements for:

- Financial and banking services (credit information)
- Big data processing operations
- AI and metaverse platforms
- Blockchain applications
- Cloud computing services

Data protection officers

- Requirements:
  - Assigned officers must have legal training and professional data protection skills.
  - There must be a minimum of three qualified personnel.

- Responsibilities: The decree clearly defines their functions, duties, and organizational positioning.

Cross-border data transfers

- Requirements:
  - There must be binding legal agreements with foreign recipients that include protection commitments for Vietnamese data subjects.
  - Immediate notification of changes (partners, purposes, data types) to related parties.

These requirements present a significant compliance burden for multinationals and cloud service users with foreign servers.

Data processing service providers

- Licensing authority: Ministry of Public Security
- Eligibility requirements:
  - Appropriate infrastructure and technology systems
  - Satisfactory impact assessment results
  - Cross-border transfer assessment (if applicable)
  - Full legal compliance
- Grounds for revocation of certificate:
  - Dissolution or bankruptcy
  - Failure to remedy violations
  - Voluntary request
  - Certificates must be returned within five working days of revocation.

Breach notification

- Timeline: Must report within 72 hours of discovery.
- Documentation: Use standardized Form 10 (breach reports) and Form 02a (notifications).

Administrative procedures

- Impact assessment filing:
  - Deadline: Within 60 days of commencing data processing.
  - Submit to: Cybersecurity Department.
  - Standardized forms: 10 templates provided, eliminating documentation ambiguity.

Penalties

- Severe violations: Fines of up to 5% of total revenue from the preceding fiscal year for:
  - Serious cross-border transfer violations.
  - Large-scale data breaches.
- Impact: Significantly enhanced deterrence compared to previous regulations.

Compliance roadmap

- Organizations should immediately:
  - Audit current data flows.
  - Update impact assessments using the decree's templates.

- Appoint or outsource qualified data protection officer personnel.
- Establish 72-hour breach of response procedures.

Labor

*Decree No. 337/2025/ND-CP dated December 24, 2025 on "**Electronic Employment Contracts**"*

This decree, which entered into effect on January 1, 2026, sets out the regulatory framework for using electronic employment contracts ("**eContracts**"). Key highlights are provided below.

Platform infrastructure

- **National platform:** The Ministry of Home Affairs manages centralized data and shared services nationwide.
- **Information system for electronic transactions:** Linked systems enabling contract creation, digital signing, storage, management, and authentication.

eContract provider technical requirements

- Digital signature software compliant with electronic transaction laws
- Security protocols and contingency plans
- Storage solutions maintaining data integrity with search functionality
- Identity verification per electronic identification provisions
- Consent confirmation mechanisms
- Contract authentication before ID assignment
- Format conversion capabilities
- Electronic transaction accounts (Article 46, Electronic Transactions Law)
- Employment reporting functionality
- Statistical and reporting capabilities
- Standard API connection to the national platform
- Information security compliance

Participant eligibility requirements

- **Individuals:** Valid citizen identity card, electronic identity, Level 2 electronic ID account, or passport; visa/visa exemption (foreigners)
- **Organizations:** Incorporation documents, registration certificates, legal representative's valid ID
- **All parties:** Digital signatures and timestamping services
- **eContract providers:** Qualified system, biometric verification technology, business license for data message authentication

Contract execution

- Process:
  - Create the contract, have the contract digitally signed with a timestamp, then authenticated.

- Authentication by the provider on a compliant platform.
- Assign an eContract unique ID within 24 hours of the final signature.

- Effectiveness: Upon final digital signature with timestamp and provider authentication (unless otherwise agreed).

Platform data management

- Collected data:
  - Electronic contracts and amendments
  - Converted contracts
  - Essential contract content
  - Employment utilization information
  - Transaction logs (access, operations, timestamps, IDs, metadata)
- Data sources:
  - eContract providers (automatic synchronization)
  - Employers (direct platform updates)
  - Provincial Home Affairs Departments
  - National/sectoral databases
  - Other legal sources

System connectivity

- Requirements:
  - IT technical standards compliance
  - Minimum Level 3 information security
  - Written agreement with the Ministry of Home Affairs
- Grounds for refusal/suspension:
  - Security requirement failures
  - Unauthorized access or data manipulation
  - Data protection violations

Rights and responsibilities

- Employers
  - Rights: Platform access, data management, reporting functionality.
  - Responsibilities: Execute contracts per the decree, maintain data security, provide employee support, report security risks, and comply with data protection laws.
- Employees
  - Rights: Platform access, contract verification, and data sharing.
  - Responsibilities: Execute contracts per the decree, maintain account security, provide accurate information, and report risks.
- eContract providers
  - Deliver ID-assigned contracts electronically.
  - Maintain secure platform connections.
  - Publicly disclose operations and fees.
  - Ensure data integrity.
  - Submit regular reports.

- Maintain archival compliance.
- Transfer data to the national platform upon termination.

Transitional provisions

- Existing eContracts: Continue under previous laws until expiration with equivalent validity.
- Ongoing contracts: Continue under previous laws unless the parties apply new provisions.
- Provider systems: Must upgrade to integrate compliant digital signature capabilities.

Authors and Contacts

Ho Huynh Thanh Thuy Nga
Legal Associate
nga.ho@vn.andersen.com

Pham Ngoc Thuan
Director
thuan.pham@vn.Andersen.com