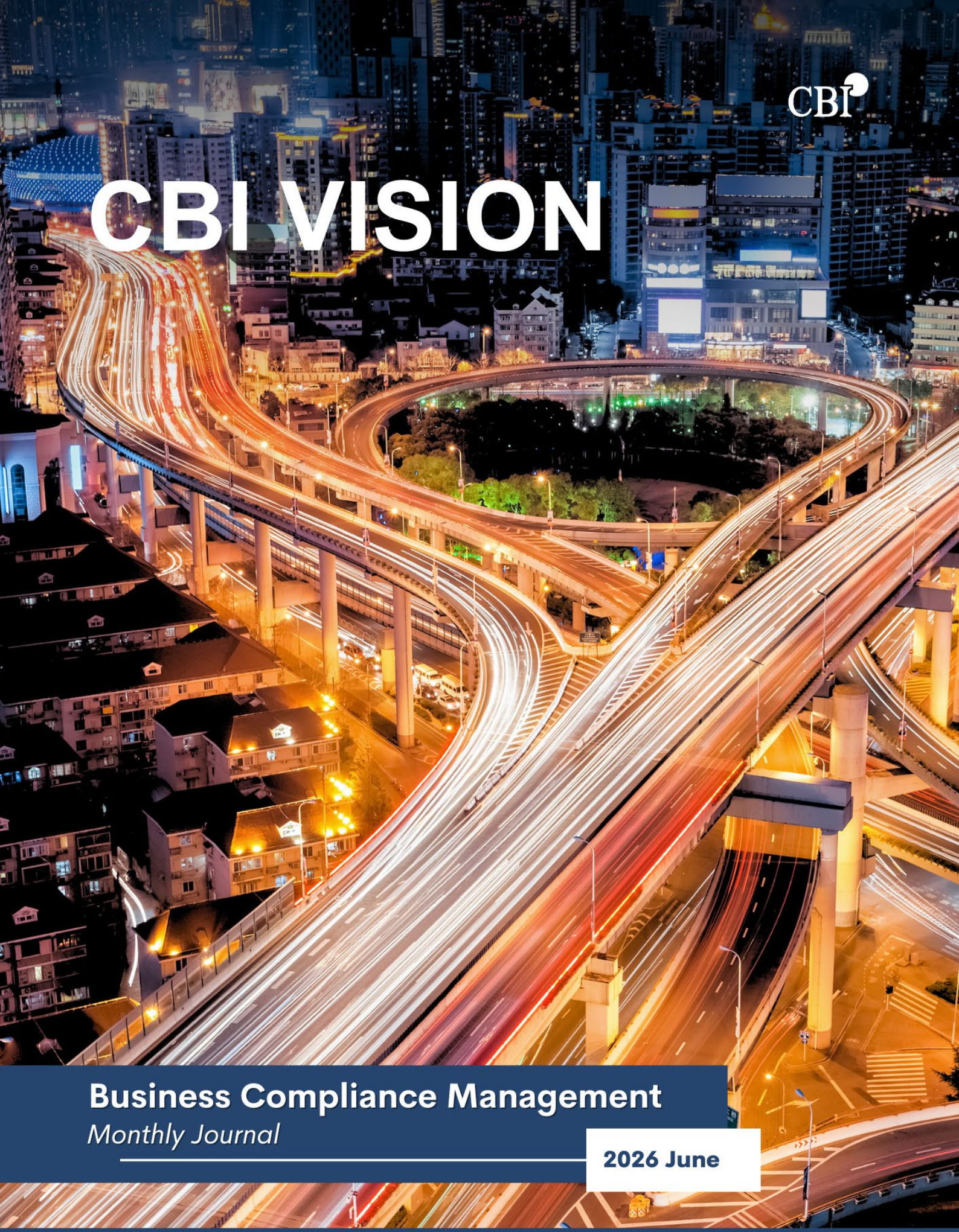

CBI VISION

Business Compliance Management

Monthly Journal

2026 June

Pursuing **Truth** · Building **Trust**

HONG KONG
BEIJING
SHANGHAI
GUANGZHOU
XI'AN
SHENZHEN
PENANG
LONDON

CONTENTS

PREFACE

First Administrative Regulation on Outward Investment Takes Effect: Implementation Begins July 1

On May 5, 2026, Premier Li Qiang of the State Council signed State Council Order No. 837, promulgating the Regulations of the State Council on Outward Investment. The Regulations were published on June 1 and will take effect from July 1.

Adopted at the 83rd executive meeting of the State Council on April 17, 2026, the Regulations comprise 34 articles and represent China's first unified regulation of outward investment activities in the form of administrative rules.

NetEase Pay Case Highlights Compliance Red Lines on Data Handling and Due Diligence in the Payment Industry

On June 8, 2026, the People's Bank of China Zhejiang Branch publicly released administrative penalty information. NetEase Payment (Hangzhou) Co., Ltd. received a warning and a fine of RMB 2.204 million for four violations. Two directly responsible persons were also fined RMB 45,000 and RMB 24,000 respectively. The penalty decision was dated June 2, with a three-year disclosure period.

This penalty, which covers both the institution and individuals, reflects the normalization of the "dual penalty system" in the financial industry's regulatory approach.

New Commercial Secrets Protection Regulations Take Effect: Data and Algorithms Now Legally Protected

On June 1, 2026, the new Provisions on the Protection of Trade Secrets issued by the State Administration for Market Regulation officially took effect. The new Provisions replace the 1995 Several Provisions on Prohibiting Acts of Infringing Trade Secrets, which had been in force for thirty years.

Formulated in accordance with the Anti-Unfair Competition Law of the People's Republic of China, the new Provisions closely address emerging trends such as the development of the digital economy and increased personnel mobility.

Compliance Hotspot

First Administrative Regulation on Outward Investment Takes Effect: Implementation Begins July 1

On May 5, 2026, Premier Li Qiang of the State Council signed State Council Order No. 837, promulgating the Regulations of the State Council on Outward Investment. The Regulations were published on June 1 and will take effect from July 1.

Adopted at the 83rd executive meeting of the State Council on April 17, 2026, the Regulations comprise 34 articles. This is China's first unified regulation of outward investment activities in the form of administrative rules, marking the elevation of outward investment supervision from the level of departmental rules to national law. The Regulations establish a full-chain compliance system characterized by "combining deregulation with regulation, controllable risks, and protection of rights and interests," providing enterprises with clear compliance boundaries for "going global" and offering solid institutional safeguards.

I. Legislative Background and Core Positioning

In recent years, China's outward investment has continued to grow in scale, with investment entities, sectors, and models becoming increasingly diversified. However, previous regulatory rules were scattered across departmental regulations issued by multiple authorities such as the NDRC and the Ministry of Commerce. These rules suffered from low legal hierarchy, inconsistent standards, and fragmented supervision, making it difficult to meet the needs of high-level opening-up and complex international risk prevention and control.

The Regulations were formulated in accordance with higher-level laws such as the Foreign Relations Law and the Foreign Trade Law. Grounded in the core principles of "balancing development and security" and "coordinating domestic and international efforts," the Regulations elevate the regulatory experience and reform outcomes in outward investment since the 18th National Congress of the Communist Party of China into national institutions. They represent both a legal affirmation of market-oriented investment autonomy and a firm safeguard for national sovereignty, security, and development interests, while providing systematic protection for investors' legitimate rights and interests. The Regulations lay a solid compliance foundation for high-quality joint construction of the "Belt and Road" and the promotion of international industrial chain and supply chain cooperation.

II. Key Compliance Points

(1) Clarifying the Scope of Application to Achieve Full Coverage of Investment Entities

Article 2 of the Regulations explicitly states that domestic enterprises, other organizations, and resident individuals all qualify as compliant investors. Investment activities covered include all forms of direct or indirect acquisition of ownership, control, or management rights in overseas enterprises or assets, encompassing the contribution of assets, equity, financing, guarantees, and similar actions. Article 32 provides that investments in the Hong Kong, Macao, and Taiwan regions shall be implemented with reference to the Regulations.

It is noteworthy that resident individuals have, for the first time, been included within the outward investment regulatory framework at the level of administrative regulations. However, Article 33 stipulates that "specific administrative measures for outward investment by resident individuals and similar entities shall be formulated by the investment and commerce authorities under the State Council," meaning that detailed implementation rules for individual outward investment have yet to be issued and are currently incorporated at a framework level only.

(2) Improving the Security Review and Classified Tiered Management System

1. **Mandatory Security Review Requirements**: Article 15 explicitly establishes a sound national security review system for outward investment. Overseas investments and related transfers or disposals of assets and equity that affect or may affect national security are subject to security review. Relevant organizations and individuals must provide assistance and cooperation, must not refuse or obstruct the process, and must comply with security review decisions.
2. **Classified and Tiered Approval and Filing System**: Article 11 states that relevant State Council departments shall "formulate, adjust, and implement outward investment policies, clearly identifying encouraged, restricted, and prohibited outward investments," and implement full-process supervision under a classified and tiered approach. Article 12 requires investors to complete approval, filing, information reporting, cross-border fund registration, and other procedures in accordance with relevant national regulations, and to submit materials truthfully. In line with current institutional practice, sensitive projects are subject to an approval system, while non-sensitive projects follow a filing system.
3. **Strengthened Investor Accountability**: Article 16 requires investors to improve their governance structures, establish and refine systems for compliant operations, internal controls, workplace safety, and emergency response, and strengthen risk identification, prevention, and mitigation.

(3) Strengthening Compliance Obligations and Establishing Clear Behavioral Boundaries

While Article 5 of the Regulations affirms that investors enjoy "independent decision-making, self-assumed risks, and self-responsibility for profits and losses," it also imposes mandatory compliance obligations: investors must comply with domestic and foreign laws and regulations as well as international practices, respect local customs and cultural traditions, uphold business ethics, act with honesty and good faith, engage in fair competition, fulfill social responsibilities, and safeguard the national image. They must not disrupt market competition order, damage the ecological environment, or infringe upon the legitimate rights and interests of workers, nor may they endanger China's national security, harm national interests, or undermine public interests.

Article 13 imposes prohibitive provisions on the cross-border transfer of technology, data, and personnel. Investors must not export or use goods, technologies, services, or related data whose export is prohibited or restricted by the State under the guise of outward investment, nor may they circumvent such restrictions through methods such as cross-border dispatch of technical personnel, provision of technical guidance, or arrangement of cross-border training. Article 14 stipulates that matters concerning cross-border data flows shall be handled in accordance with relevant laws, administrative regulations, and national provisions, ensuring consistency with the Data Security Law, Personal Information Protection Law, and other related legislation.

(4) Improving Rights Protection and Violation Penalties to Balance Rights and Responsibilities

1. Rights Protection Mechanisms: The Regulations dedicate a special chapter to establishing an investment protection system. This includes mechanisms for risk monitoring and early warning, consular protection, investment dispute resolution (encouraging consultation, mediation, arbitration, litigation, and other methods), and investigation and countermeasures against investment barriers, providing comprehensive protection for the rights and interests of compliant investors.

2. Tiered Penalty System for Violations: Article 27 establishes three tiers of penalties based on the type of violation:

- For projects in prohibited investment categories: a fine ranging from 5‰ to 10‰ of the investment amount, with directly responsible persons fined between RMB 50,000 and RMB 100,000.
- For failure to complete approval or filing procedures or making false declarations: an initial fine of 1‰ to 5‰ of the investment amount; if not corrected, the fine increases to 5‰ to 10‰ of the investment amount, with responsible persons fined between RMB 20,000 and RMB 50,000.
- For obtaining approval through fraud: revocation of the approval or filing, with a fine of 1‰ to 5‰ of the investment amount (or 5‰ to 10‰ for projects already implemented), and responsible persons fined between RMB 20,000 and RMB 50,000.

From the date the penalty decision takes effect, the competent authorities may refuse to accept approval or filing applications from the violating entity for up to three years, or prohibit the entity from engaging in outward investment activities for a period of one to three years.

III. Compliance Recommendations for Enterprises

1. Conduct Comprehensive Compliance Self-Inspections: Thoroughly review existing overseas investment projects to verify the completeness of filing and approval procedures and security review compliance, with a particular focus on identifying risks related to technology exports, cross-border data transfers, and fund flows.

2. Improve Internal Control Systems: Revise outward investment management policies to clearly define decision-making processes, risk assessment procedures, compliance approval workflows, and record-keeping requirements. Strengthen investor accountability and enhance compliance enforcement mechanisms.

3. Enhance Personnel Training: Organize training for business, legal, and finance teams on the core provisions of the Regulations, with emphasis on approval and filing procedures, security review standards, and the consequences of violations, so as to raise overall cross-border compliance awareness.

4. Establish Dynamic Monitoring Mechanisms: Closely track changes in outward investment policies and updates to host country laws, develop risk early-warning systems, conduct regular compliance audits, and promptly rectify any identified issues.

The introduction of the Regulations represents a significant institutional achievement in China's efforts to advance high-level opening-up, as well as a key measure to regulate outward investment activities and prevent cross-border risks. Starting July 1, 2026, outward investment will enter a new stage characterized by "strong compliance, strict supervision, and robust protection."

Enterprises should proactively adapt to the new requirements, integrate compliance management throughout the entire investment process, seize opportunities arising from opening-up while firmly upholding security bottom lines, and achieve high-quality and sustainable development in outward investment.

Case Sharing

Four Violations Trigger Dual Penalties of RMB 2.2 Million: NetEase Pay Case Highlights Compliance Red Lines on Data and Due Diligence in the Payment Industry

On June 8, 2026, the People's Bank of China Zhejiang Branch publicly released administrative penalty information. NetEase Payment (Hangzhou) Co., Ltd. received a warning and a fine of RMB 2.204 million for four violations. Two directly responsible persons were also fined RMB 45,000 and RMB 24,000 respectively. The penalty decision was dated June 2, with a three-year disclosure period.

This penalty, which covers both the institution and individuals, reflects the normalization of the "dual penalty system" in the financial industry's regulatory approach.

I. Key Violations in This Penalty

The penalty notice lists four violations, all of which are high-frequency compliance issues in the payment industry:

1. Violation of account management regulations;
2. Violation of clearing management regulations;
3. Violation of data security management regulations;
4. Failure to conduct customer due diligence in accordance with regulations.

Interpreted in light of industry regulatory requirements: Violations of account management and clearing management regulations typically involve lax account opening reviews and failure to implement regulatory standards in fund clearing processes. Data security management violations relate to shortcomings in customer information storage and internal data control mechanisms, which fail to meet data security regulatory standards. Customer due diligence violations, a critical component of anti-money laundering efforts, often involve superficial identity verification and qualification checks for merchants and individual customers.

The combination of multiple violations reflects systemic compliance deficiencies in the company's fund operations, data management, and risk control system development, ultimately triggering substantial institutional fines and concurrent penalties on responsible individuals.
It is worth noting that this is not the first time NetEase Payment has encountered regulatory red lines.

In July 2021, its predecessor, NetEase Bao Co., Ltd., was fined RMB 30,000 for violations including failure to retain transaction information in accordance with actual transaction scenarios. The fine has now increased from RMB 30,000 to RMB 2.204 million — a more than 70-fold rise — indicating a significant expansion in both the breadth and severity of compliance issues.

In addition, the payment business license held by NetEase Payment expires on June 26, 2027, leaving only one year remaining. This penalty is expected to adversely affect the company's classification rating, substantially increasing the pressure for license renewal.

II. Industry Compliance Warnings

This penalty, issued amid tightening data compliance supervision in the financial industry, sends a clear regulatory signal.

On June 8, the Cyberspace Administration of China and five other departments jointly issued the Guidelines on Data Classification and Grading for Financial Information Services, providing systematic guidance on data classification, grading, and identification of important data for financial information service institutions. The guidelines divide data into four levels — core data, important data, sensitive general data, and regular general data. The release of these guidelines marks further refinement of data security standards in the financial industry, requiring financial institutions and payment companies to implement tiered and classified management of their data assets.

In the anti-money laundering field, the Measures for Classified Rating Management of Non-Bank Payment Institutions, which took effect in February 2026, assigns a high weighting of 15 points to anti-money laundering violations. Serious anti-money laundering violations may trigger a "one-vote veto," directly resulting in the suspension or rejection of license renewal applications. As a foundational element of anti-money laundering efforts, customer due diligence has become a key focus of regulatory scrutiny.

According to incomplete media statistics, more than 20 payment institutions have been subject to regulatory penalties since the beginning of 2026, with the total amount of fines and confiscations exceeding RMB 170 million. Cases involving "multiple violations punished together" and the "dual penalty system" have increased significantly. Regulatory enforcement has shifted from single-point spot checks to comprehensive, full-process, penetration-style inspections across all business lines.

On the same day that NetEase Payment was penalized, Yi Ticket Union Payment Co., Ltd. was fined a total of RMB 48.349 million for violations involving payment and settlement, financial technology, anti-money laundering, and other regulations — setting a new record for the highest penalty in the payment industry this year.

III. Corporate Compliance Recommendations

For financial and payment institutions, the following three core compliance measures should be implemented simultaneously:

1. **Establish a Data Classification and Authorization System**: In accordance with the Guidelines on Data Classification and Grading for Financial Information Services, conduct a comprehensive inventory and classification of data assets, implement full-scenario data desensitization requirements, and clearly define access, usage, and transmission permissions for data at different levels.

2. Improve Business Traceability Mechanisms: Fully retain logs of business access and fund operations to ensure every step of the process is traceable, enabling the provision of a complete chain of evidence during regulatory inspections.

3. Strengthen Customer Due Diligence and Anti-Money Laundering Management: Upgrade anti-money laundering monitoring systems, conduct regular customer risk screenings, address gaps in full-process due diligence controls, and ensure that customer identity verification, qualification reviews, risk classification, and other procedures are effectively implemented.

Failure to address long-term institutional deficiencies or implementation gaps will expose both the enterprise and its responsible management personnel to administrative penalties and place them at a significant disadvantage during license renewal reviews.

Facing increasingly stringent data, financial, and cross-border regulatory policies, enterprises urgently need to adopt proactive risk screening and systematic compliance management. Central Business Information specializes in global commercial due diligence and corporate compliance services, with operations covering mainland China and 214 countries and regions worldwide. We offer one-stop services including financial risk control verification, data compliance risk diagnostics, domestic and overseas corporate background investigations, senior executive compliance background checks, and cross-border business risk assessments.

Leveraging our proprietary intelligent background screening system and extensive verification database, we can accurately identify hidden risks in areas such as account management, data flows, customer due diligence, and outward investment in line with relevant industry regulatory requirements. We assist enterprises in establishing long-term compliance control mechanisms and proactively avoiding regulatory penalties and losses.

Compliance Information

New Commercial Secrets Protection Regulations Take Effect: Data and Algorithms Now Legally Protected — Signing Confidentiality Agreements Alone Is No Longer Sufficient

On June 1, 2026, the new Provisions on the Protection of Trade Secrets (SAMR Order No. 126, hereinafter referred to as the "Provisions") issued by the State Administration for Market Regulation officially took effect. The new Provisions replace the 1995 Several Provisions on Prohibiting Acts of Infringing Trade Secrets, which had been in force for thirty years.

Formulated in accordance with the Anti-Unfair Competition Law of the People's Republic of China, the new Provisions closely address new developments such as the characteristics of the digital economy and increased personnel mobility. They fill regulatory gaps in traditional trade secret protection regarding digital assets, online office environments, and cross-border cooperation scenarios. The Provisions serve as a core guiding document for corporate intellectual property protection, data confidentiality, and cross-border business compliance, and carry significant compliance implications for technology companies, R&D-oriented enterprises, and businesses engaged in overseas operations.

I. Key Breakthrough: Digital Assets Formally Included in the Statutory Scope of Trade Secret Protection

The most significant institutional upgrade in the new Provisions is the explicit inclusion of digital elements such as data, algorithms, computer programs, and code within the scope of trade secret protection (Article 5). At the same time, the old requirement of "practicality" has been removed, with the three core criteria for protection now clearly defined as "not known to the public, having commercial value, and for which corresponding confidentiality measures have been taken."

The scope of protection has been comprehensively expanded: in terms of technical information, it covers structure, raw materials, formulas, processes, methods, data, algorithms, computer programs, and code; in terms of business information, it extends to creativity, management, sales, finance, planning, customer information (including customer names, addresses, contact details, transaction habits, intentions, and content), and data.

Notably, Article 7 of the new Provisions clarifies that commercial value includes both actual and potential value. Stage-by-stage R&D achievements, failed experimental data, undeveloped technical solutions, and other information with potential value are now legally protected. This overturns the traditional view that "trial-and-error data has no protective value.

AI models can be protected under the trade secret framework through their constituent elements, such as algorithms, training data, and code. However, the “model” itself is not listed as an independent object of protection in the regulations. Enterprises must therefore ensure that appropriate confidentiality measures are implemented separately for the algorithms, data, and other elements involved in the model.

II. Focus on Risk Scenarios: Refining Rules for Digital Infringement and Cross-Border Compliance

The new Provisions address high-frequency trade secret leakage risk scenarios by strengthening the following systems:
In terms of digital infringement, the Provisions explicitly include electronic intrusion within the scope of improper means, covering unauthorized access, technical intrusion, illegal transmission, and other forms of digital infringement. They also clarify that instigating, inducing, or assisting others in infringing trade secrets constitutes joint infringement. Third parties who know or should know that trade secrets were obtained illegally and nevertheless acquire, disclose, or use them will be deemed to have committed infringement.

In cross-border and remote collaboration scenarios, the Provisions list “remote access control” as one of the eight types of reasonable confidentiality measures, requiring enterprises to establish control mechanisms for remote access to confidential operations. They also introduce extraterritorial application clauses, allowing regulatory authorities to pursue accountability for infringing acts committed overseas that disrupt the domestic market order or damage the legitimate rights and interests of domestic business operators. When conducting business collaboration with overseas partners, enterprises should implement confidentiality approval, information desensitization, and access control requirements before providing confidential data or algorithms, and should sign confidentiality agreements that clearly define the obligations and liabilities of all parties.

III. Clarifying Compliance Standards: Statutory Recognition of Eight Categories of Confidentiality Measures

For the first time, the new Provisions list eight categories of reasonable confidentiality measures in the form of departmental rules. Measures such as tiered authorization, data desensitization, and full-process logging are established as statutory standards for determining “reasonable confidentiality measures.” This marks a shift in corporate confidentiality management from traditional institutional constraints to digitalized and systematic compliance management:

1. Institutional Development: Formulate confidentiality rules and regulations;
2.Personnel Management: Sign confidentiality agreements and non-compete agreements;
3.Physical Isolation: Implement isolation and control over confidential areas and carriers;
4.Technical Protection: Adopt digital confidentiality measures including tiered authorization, data desensitization, and operation log retention;
5.Carrier Management: Identify and control confidential documents and storage media;
6.Equipment Control: Manage the use and access of confidential equipment;
7.Departure Management: Promptly revoke access rights of departing personnel and clear confidential information;
8.Catch-All Clause: Cover other reasonable confidentiality measures.

It is particularly noteworthy that the new Provisions explicitly state that information protected solely by a confidentiality agreement, without the implementation of substantive control measures, will have difficulty qualifying as a trade secret. This means enterprises cannot fulfill their statutory confidentiality obligations with a confidentiality agreement alone. Instead, they must establish an integrated “human defense + technical defense + institutional defense” confidentiality management system.

IV. Optimizing Burden of Proof Rules and Increasing Penalties

In terms of burden of proof rules, the new Provisions implement a shift in the burden of proof: if the rights holder can prove that the infringer had access to the trade secret and that the information in question is substantially similar to the rights holder’s trade secret, the burden shifts to the alleged infringer to prove that the information has a legitimate source. This rule effectively lowers the threshold for rights holders to protect their rights, though it does not constitute an absolute presumption of infringement — the alleged infringer may still provide counter-evidence.

Regarding penalties, general infringement acts are subject to fines ranging from RMB 100,000 to RMB 1 million; for serious circumstances, fines range from RMB 1 million to RMB 5 million. “Serious circumstances” include cases causing substantial direct losses to the rights holder, seriously adversely affecting the rights holder’s production and business activities, endangering national interests or public interests, or where the infringer commits another infringement within two years after previously receiving an administrative penalty for trade secret infringement. Cases involving technical secrets are uniformly handled by market supervision departments at the level of cities with districts or above. Suspected criminal offenses shall be transferred to judicial authorities for criminal liability in accordance with the law.

The new Provisions also explicitly outline five categories of legitimate non-infringing scenarios, providing enterprises with a “safe harbor”: independent discovery or self-development; reverse engineering of products obtained through public channels; former employees using general knowledge and skills in their work; and lawful disclosure to expose illegal or criminal acts. These provisions protect corporate rights and interests while accommodating reasonable talent mobility.

V. Implementation Recommendations for Corporate Compliance

1.**Inventory Confidential Digital Assets**: Compile a ledger of enterprise data, algorithms, code, and R&D materials; classify and grade them, clearly define the scope of confidential items and control levels, with particular attention to previously overlooked intangible digital assets such as stage-by-stage R&D achievements and trial-and-error experimental data.

2.Revise Internal Policies and Cooperation Agreements: Add specific compliance clauses covering digital asset confidentiality, remote access control, and cross-border data transmission, ensuring that confidentiality agreements are supported by substantive control measures.

3.Improve Technical Control Systems: Establish digital confidentiality mechanisms for tiered authorization, data desensitization, and operation auditing, with dedicated protection for high-value digital assets such as algorithm systems, core datasets, and R&D achievements.

4.Conduct Company-Wide Compliance Training: Strengthen employees' awareness of digital confidentiality and cross-border information security to prevent human-induced leakage risks.

5.Leverage Administrative Rights Protection Channels: When infringement occurs, prioritize administrative avenues to balance efficiency and cost in rights protection.

The implementation of the new Provisions on the Protection of Trade Secrets establishes a trade secret protection system adapted to the digital economy and cross-border operations. Enterprises should proactively align with the new requirements, integrate digital confidentiality and cross-border information compliance into daily business management, strengthen the security defense line for core assets, and avoid compliance risks and economic losses arising from infringement and leakage.

Thanks for reading

HOTLINE

400 0806 099

marketing@chinacbi.com

www.chinacbi.com

CBI (Beijing) Business Information Limited