GT GreenbergTraurig

China Newsletter | 2025 Q2/Issue No. 64

In This Issue:

Antitrust | Compliance | Corporate | Data Privacy & Cybersecurity | Foreign Investment

This China Newsletter provides an overview of key developments in the following areas:

- *China Proposes Updated Regulations on Exporting Automobile-Generated Data*

5. Foreign Investment

- *Three Authorities Jointly Issue the Market Access Negative List (2025 Edition)*
- *China Proposes New Foreign Exchange Policies to Boost Cross-Border Investment and Financing*
- *China's New Tax Incentive Policy for Foreign Investors' Domestic Reinvestment*

Antitrust

Latest Development in China's Anti-Unfair Competition Law 2025

年《反不正当竞争法》修订要点解读

On June 27, 2025, China passed the second major revision of its Anti-Unfair Competition Law (AUCL), which takes effect on Oct. 15, 2025. This update reflects China's commitment to addressing challenges in the digital economy while strengthening traditional competition rules. These changes introduce new compliance requirements, but may also offer opportunities for companies looking to protect their business interests.

Key Updates in the 2025 AUCL Revision

The 2025 revision introduces several changes to regulate competition in both digital and traditional markets:

1. **Regulating Internet Activities**: The revised AUCL targets unfair practices in the digital economy, particularly:
   - **Illegal Data Acquisition**: Businesses are prohibited from using fraudulent, coercive, or technical means (e.g., web crawlers) to illegally obtain or use data from other businesses if it harms their rights or disrupts market order. Key criteria include whether the data use creates "substantial substitution" of services or unreasonably increases operational costs.
   - **Malicious Transactions (Reverse Brushing)**: The law bans practices like fake reviews, fraudulent transactions, or malicious returns that harm competitors or disrupt fair competition.
2. **Platform Operator Responsibilities**: Online platforms, such as e-commerce sites or app stores, face new obligations:
   - **Ban on "Race-to-the-Bottom" Pricing**: Platforms cannot force or indirectly coerce merchants to sell below cost, addressing "vicious competition." Violations may lead to fines ranging from RMB 50,000- RMB 2 million, with higher penalties for severe cases.
   - **Active Management**: Platforms must establish fair competition rules, set up complaint mechanisms, and actively monitor and address merchants' unfair practices. Failure to do so may result in joint liability for damages under related laws, such as the Civil Code or E-Commerce Law.
3. **Abuse of Relative Advantage**: A new provision regulates large enterprises (even those without market dominance) that abuse their advantages—such as financial strength, technology, or industry

influence—to impose unfair terms or delay payments to smaller businesses (SMEs). Offenders are given a "limit period amendment" to correct violations before facing fines up to RMB 5 million.

4. **Protecting Commercial Identifiers**: The 2025 revision of AUCL expands protection for new commercial identifiers, such as online usernames and app icons, and addresses confusion caused by:
   - Using another's trademark or well-known mark in a business name or as a search keyword.
   - Other actions that mislead consumers about a company's identity or offerings.
5. **Stricter Anti-Bribery Rules**: Both bribe-givers and takers now face penalties. Individuals may face a monetary fine up to RMB 1 million for violation.
6. **Long-Arm Jurisdiction**: Unfair acts done abroad that disturb the Chinese market may be pursued in China.
7. **Enhanced Enforcement**: The 2025 revision introduces several updates in enforcement measures:
   - **Interview**: Authorities now can hold "interviews" with suspected violators to encourage compliance without formal investigations, seeking to balance enforcement with fairness.
   - **Adjusting Monetary Fines**: The 2025 revision also adjusts the upper and lower limits of the monetary fines to certain violations:

Activities	Upper Limit (RMB)		Lower Limit (RMB)	
	Before	2025 revision	Before	2025 revision
Serious Trade Secret Theft	5 million		500,00	1 million
Commercial Defamation	• 500,000 for normal case; • 3 million for severe case	• 1 million for normal case; • 5 million for severe case	500,000 for severe case	1 million for severe case
Obstructing enforcement and investigation by authorities	• Individual: 5,000 • Entity: 50,000	• Individual: 10,000 • Entity: 100,000		

Considerations for Businesses

- Brand and Marketing: Run a trademark/keyword search of Chinese brand names, social-media handles, app icons and seek to ensure contracts with agencies ban unauthorized use of third-party marks.
- Anti-Bribery: Expand policies to cover receiving as well as giving bribes. Record all discounts, commissions, and hospitality in company books.
- Online Sales: Audit platform stores for fake reviews, phantom orders, and malicious returns. Review platform agreements for below-cost pricing clauses.

- Supply-Chain and Payments: Check payment terms with Chinese SME suppliers—seek to avoid one-sided or delayed terms.
- Cross-Border Campaigns: Confirm that overseas promotions targeting Chinese buyers comply with the AUCL.
- Governance: Train legal representatives and senior managers on personal liability risks.

Compliance

The SAMR Issues Medical Advertising Supervision Guidelines

市场监管总局制发《医疗广告监管工作指南》

The State Administration for Market Regulation (SAMR) issued the Medical Advertising Supervision Guidelines, which comprise 18 articles and are based on relevant laws and regulations to standardize medical advertising oversight. The guidelines clearly state that only legally established medical institutions are permitted to publish medical advertisements. If an advertisement is released without prior review but contains basic information consistent with the institution's practice license, no penalty will be imposed. However, if the content is misleading or inconsistent with licensing information, enforcement action will be taken. Advertisements that imitate the names of well-known hospitals will also be subject to investigation. Ads published after the expiration of their review certificate may be exempt from penalties if the content remains consistent with both the certificate and the institution's actual operations.

Minor modifications to advertisement content—such as changes in background design, font color, or the addition or removal of accurate contact details—are generally not considered violations. Where the content falls within the scope of publicly disclosed information, is supported by valid documentation, or accurately reflects the structure of a medical alliance, penalties may be reduced, mitigated, or waived altogether. In cases where no penalty is imposed, educational guidance will be provided.

In terms of enforcement, the use of spokespersons for endorsements is subject to penalties under Article 58 of the Advertising Law. False or impersonated endorsements that constitute criminal offenses will be referred to public security authorities. Advertisements making definitive claims about efficacy, especially those involving serious diseases, will face heavier penalties. Fabricated or distorted scientific theories, as well as false claims about key institutional information, may also be treated as criminal offenses and referred to law enforcement. Medical advertisements targeting minors, including cosmetic ads that promote appearance anxiety or recommend non-treatment services, will be penalized under Article 57 of the Advertising Law. The use of absolute language (e.g., "guaranteed cure") will be addressed in accordance with relevant enforcement guidelines.

If a single advertisement contains multiple violations that constitute one offense, penalties will not be duplicated. However, if the violations represent distinct offenses, penalties may be combined depending on the circumstances. Entities that are not licensed medical institutions but claim to provide medical services may be investigated for practicing without a license and referred to health authorities. Internet platforms that fail to verify advertisers and allow non-medical entities to publish medical ads will be penalized under Article 63 of the Advertising Law, and in severe cases, may be ordered to suspend related services.

Corporate

China Further Clarifies Rules on Using Reserve Funds and Non-Monetary Capital Contribution

关于公司法、外商投资法施行后有关财务处理问题的通知

On June 27, 2025, China's Ministry of Finance issued new guidelines for financial compliance requirements under the revised Company Law (which took effect July 1, 2024) and Foreign Investment Law (which took effect in 2020). Here's what foreign investors and foreign invested enterprises (FIEs) should keep in mind:

1. FIE-Specific Funds Transitions

- Beginning Jan. 1, 2025, FIEs must stop allocating new funds to reserve funds (储备基金), bonus and welfare funds (职工奖励及福利基金), and venture expansion funds (企业发展基金) (collectively Three Funds). Any post-2025 allocations must be reversed.
- Reserve fund balances should be reclassified into statutory common reserves, while venture expansion fund balances should be reclassified into discretionary common reserves.
- Bonus and welfare funds should be used for the purposes, conditions, and procedures determined at the time of allocation.

2. Non-Monetary Asset Contributions

- **Valuation**: Contributions of non-monetary assets (e.g., equity, land use rights, intellectual property, etc.) must undergo independent valuation by third-party appraiser;
- **Due Diligence**: Companies must assess risks affecting asset rights and are encouraged to seek legal opinions when necessary.

3. Using Common Reserves to Offset Losses

- **Basis**: Companies may offset losses using capital reserves, limited to the negative undistributed profits in the audited prior-year financial statements (no earlier than 2024).
- **Sequence**: Losses must be offset with the following resources in order:
  - statutory common reserves;
  - discretionary common reserves;
  - capital reserves from non-monetary contributions (e.g., intellectual property, equity, land use rights); and
  - capital injections via debt exemptions or donations (monetary/non-monetary).
- **Restrictions**:
  - Shareholder-specific capital reserves cannot be used without shareholder consent.
  - Contingent capital reserves require finalization before use.

- **Procedures**:
  - The company board should review and approve the loss offset plan and submit to shareholders' meeting for approval.
  - Notify creditors/public within 30 days of shareholder resolution (except certain financial institutions).
  - Disclose amounts in financial statement notes under "Undistributed Profits."
- **Retroactive Compliance**: Adjustments required for actions since July 1, 2024, if non-compliant.

Data Privacy & Cybersecurity

The CAC released Draft Amendment to the Cybersecurity Law for Public Comment

国家网信办就《网络安全法（修正草案）》再次征意

The Cyberspace Administration of China (CAC) released the Cybersecurity Law of the People's Republic of China (Draft Amendment for Second Public Comment) (Draft) and solicited public comments through April 27, 2025.

Compared to the current Cybersecurity Law, the Draft proposes the following key changes:

- **Enhanced Legal Responsibilities for Cybersecurity Operations**
  - **Higher Penalties for General Network Operators (Non-CII Operators)**

    First-time violations that previously lacked clear fine amounts would now carry fines of ¥10,000–¥50,000. If an operator fails to rectify or causes harmful consequences, fines increase to ¥50,000 - ¥500,000. Responsible individuals may be fined ¥10,000 - ¥100,000 (up from ¥5,000 - ¥50,000).
  - **More Detailed Penalties for Critical Information Infrastructure (CII) Operators**

    If a CII operator fails to fulfill its cybersecurity obligations, both the current Cybersecurity Law and the Draft provide that a first-time violation may result in a warning. If the CII operator refuses to rectify the violation or causes harmful consequences, fines range from ¥100,000 to ¥1 million, and responsible individuals may be fined ¥10,000 to ¥100,000.

    Meanwhile, the Draft adds higher penalties for aggravated outcomes:
    - For serious consequences, such as large-scale data breaches or a partial loss of CII functionality, fines range from ¥500,000 to ¥2 million, authorities may suspend the business, and responsible personnel may be fined ¥50,000 to ¥200,000.
    - For extremely serious consequences, such as the complete loss of major functions, fines range from ¥2 million to ¥10 million, while directly responsible personnel may be fined ¥200,000 to ¥1 million.
  - **New Penalties for Unsafe Product Sales**

    Selling or providing critical network equipment or cybersecurity products that are not certified or tested may result in a warning and confiscation of products and illegal gains.
    - If illegal gains exceed ¥100,000: additional fine of one to three times the gains;

  - If gains are below ¥100,000: fine of ¥30,000 - ¥100,000

- **Adjustments to Information Security Responsibilities**
  - **Consolidated Content Management Rules**

    Under the current Cybersecurity Law, penalties for failing to manage prohibited information have been comparatively light in some cases.

    The Draft tightens enforcement measures, permitting public reprimands and increased fines ranging from ¥50,000 to ¥500,000. For uncorrected or serious violations, fines may rise to ¥500,000 – ¥2 million, and authorities may suspend business operations. Responsible personnel may be fined ¥50,000 - ¥200,000.

    In cases resulting in particularly severe impact or consequences, fines may range from ¥2 million to ¥10 million, with responsible individuals facing penalties of ¥200,000–¥1 million.
  - **Clarified Responsibilities for Service Providers**

    According to the Draft, providers of electronic messaging services and application download services who fail to fulfill their cybersecurity management obligations would be penalized under the provisions applicable to network operators.
- **Personal Information and Cross-Border Data Transfer**

  The Draft shifts the Cybersecurity Law's personal information protection and cross-border data transfers to a referential liability framework. Conduct such as disseminating prohibited content, violating personal information rights, or unlawful cross-border data transfer would be sanctioned under applicable laws, including the Data Security Law and the Personal Information Protection Law.
- **Leniency for Minor or First-Time Offenses**

  Consistent with the Administrative Penalty Law, penalties may be mitigated or waived where a network operator proactively reduces harm, promptly rectifies minor violations, or commits a first-time violation with limited impact.

The TC260 Releases Two Compliance Guidelines for Personal Information Protection Audit

网安标委发布两份个人信息保护合规审计指南

With the CAC-issued Measures for Personal Information Protection Compliance Audits (Audit Measure) now in force (effective May 1, 2025), organizations have initiated related compliance audit activities. The National Cybersecurity Standardization Technical Committee (TC260) has also developed two guidelines to help organizations navigate the compliance audit requirement under the Personal Information Protection Law (PIPL) and the Audit Measure, with operational, actionable guidance to help standardize audit practice and improve audit quality, and also serve as a practical reference when selecting and engaging professional institutions to conduct the audits. Multinational companies that process personal information of individuals in China may wish to take them into account when designing compliance programs and when engaging third-party auditors. These two sets of guidelines are:

- Guidelines for Cybersecurity Standards Practice – Compliance Audit Requirements for Personal Information Protection (Audit Guidelines), and
- Guidelines for Cybersecurity Standards Practice – Service Capability Requirements for Professional Institutions Conducting Compliance Audits on Personal Information Protection (Professional Institution Capability Guidelines).

Audit Guidelines

The Audit Guidelines set out the scope, principles, processes, and frequency of audits. They apply both to personal information handlers (similar to the "data controller" concept) and to professional institutions conducting audits. The guidelines require audits to cover processing legality, complying with internal rules, protecting individual rights, management systems, and security measures. Audit frequency depends on the number of individuals affected: at least once every two years for processors handling 10 million or more individuals, once every three to four years for one to 10 million, and at least once every five years (recommended) for fewer than one million.

- **Scope of Application** applies to personal information processors and professional institutions conducting compliance audits on personal information protection.
- **Audit Principles** include legality, independence, objectivity, fairness, professionalism, and confidentiality.
- **Implementation Process** covers five stages: audit preparation, audit execution, audit reporting, issue rectification, and archiving management. The process involves defining audit objectives and scope, collecting evidence through both on-site and off-site methods, compiling an audit report with findings and recommendations, supervising the correction of non-compliant issues, and properly storing working papers and audit reports.
- **Audit Content** covers various aspects, including the legality of personal information processing activities, the compliance of processing rules, protecting personal information rights and interests, internal management systems and operational procedures, and security technical measures.
- **Audit Frequency**
  - Processors handling personal information of over 10 million individuals: At least once every two years
  - Processors handling between one million and 10 million individuals: At least once every three to four years
  - Processors handling fewer than one million individuals: Recommended at least once every five years

Professional Institution Capability Guidelines

The Capability Guidelines establish baseline requirements for audit institutions. These include being legally registered in China, maintaining sound compliance records, and demonstrating expertise in personal information protection. Institutions must employ at least 17 certified professionals (two senior, five mid-level, and 10 junior), led by a full-time senior manager. They must also maintain secure facilities, compliant tools, and structured management systems. Prohibited conduct includes conflicts of interest, concealing findings, unauthorized access, and subcontracting without approval.

- **Scope of Application:** Intended to standardize compliance audit activities related to personal information protection conducted by professional institutions. It also provides guidance for building service capabilities and serves as a reference for personal information processors when selecting professional institutions.
- **Basic Requirements:** Institutions are required to be registered within China, possess independent legal entity status, have legal representatives and senior executives with no criminal records, have had

no cybersecurity-related administrative penalties in the past three years, and have relevant service experience in personal information protection.

- **Management System Requirements:** Institutions should establish core management systems such as responsibility frameworks and personnel management, conduct risk analysis prior to audits, develop emergency response plans, ensure full-process traceability, and enhance service capabilities through annual self-assessments and continuous improvement.
- **Technical Capability Requirements:** Should be proficient in laws, regulations, and standards related to personal information protection, be familiar with industry regulatory requirements, possess the ability to identify the scope of information processing activities, and use compliant audit tools to develop detailed audit procedures.
- **Personnel Capability Requirements:** Should have a team of at least 17 certified professionals, including two senior-level, five mid-level, and 10 junior-level auditors. A full-time senior manager should be appointed to lead the team. Each level of personnel must meet specific requirements for education, professional experience, and certification training.
- **Facilities and Equipment Requirements:** Should have a dedicated office space that complies with security management standards, be equipped with fire prevention systems and specialized audit hardware and software tools, and maintain a structured system for managing equipment records.
- **Prohibited Conduct:** Be prohibited from engaging in misconduct, such as having financial or personal ties with the audited entity, concealing audit findings, accessing data beyond authorized limits, disclosing trade secrets, or subcontracting audit tasks without approval. These restrictions are in place to ensure the independence and fairness of the audit process.

China's Central Bank Releases New Data Security Regulation

央行公布《中国人民银行业务领域数据安全管理办法》

On May 9, 2025, the People's Bank of China (PBOC) released the finalized Administrative Measures on Data Security in the People's Bank of China Business Areas (PBOC Data Measures), effective June 30, 2025. These measures aim to harmonize data security practices across the financial sector, requiring institutions to safeguard sensitive information in line with China's expanding data governance framework.

Additionally, the PBOC issued the Measures on Cybersecurity Incident Report in PBOC Business Areas (Incident Report Measures), effective Aug. 1, 2025, which establish obligations for incident reporting and response. Together, these regulations build on China's broader data protection framework, including the PRC Cybersecurity Law (2017), PRC Personal Information Protection Law (2021), and PRC Data Security Law (2021).

1. **Scope of Application Extends to Non-Bank Fintech Actors**

   The rules apply to any entity that processes "business data" within activities under PBOC's supervision. Covered functions are broadly defined and include: monetary policy execution, macro-prudential oversight, payment and settlement, RMB issuance and circulation, treasury operations, credit reporting, anti-money-laundering and financial statistics.

   Importantly, the PBOC Data Measures extend to non-bank actors— such as fintech platforms, third-party payment providers and data service providers—when their core business falls within these areas. Institutions already regulated by the National Financial Regulatory Administration (NFRA) or the

China Securities Regulatory Commission (CSRC) may face overlapping requirements where these institution's compliance programs may be harmonized to avoid duplication and conflicts.

2. **Data Classification and New "High-Sensitivity" Tier**

   The PBOC introduces a three-tier classification: General, Important, and Core data. Important and Core data require enhanced safeguards.

   In practice, a new concept – "high-sensitivity data fields" (高敏感性数据项) – creates the most immediate compliance challenge. These fields must be individually tagged and include any sensitive personal information, customer trade secrets, or other business data whose unauthorized disclosure could harm individuals, enterprises, or the public interest. Once tagged, such data is subjected to prescriptive controls, encryption at rest and in transit, prohibition on storage on end-user devices or removable media, and restrictions on exporting from strictly controlled production environments except under documented, pre-approved exceptions.

   Furthermore, identity verification must follow a "verify-only" model—returning a simple match/no-match result without revealing underlying data. Displays of such verification data to employees or external parties must be desensitized unless disclosure is legally required or specifically requested by the data subject.

3. **Lifecycle Governance and Mandatory Audits**

   Institutions must maintain an up-to-date, machine-readable data catalogue capturing each item's business relevance, sensitivity tag, storage locations, and authorized uses. The catalogue must be refreshed at least annually. All covered entities—regardless of data tier—must run a full compliance audit at least once every three years; whereas handlers of important data must audit annually and commission independent annual risk assessments and file them with the PBOC and its provincial branch by Jan. 15 every year. Additionally, any "major" or "extremely severe" incident may automatically trigger special audits.

4. **Cross-Border Data Transfers**

   The Measures do not create new outbound data transfer rules but reinforce existing Cyberspace Administration of China (CAC) mechanisms—security assessments, standard contracts, or certification. Circumvention through data-splitting, re-formatting, or tokenization is explicitly prohibited.

   High-sensitivity data may not be transferred abroad by simple "export" (for example, by e-mail attachment or removable drive) unless the recipient is a formally entrusted processor and end-to-end encryption is in place. Institutions must also obtain assurances from any domestic data provider that non-public data has been lawfully collected and is accurate.

5. **Incident Reporting**

   The Incident Measures impose a four-tier severity scale: Extremely Severe, Severe, Material, and General. Any breach involving Core data is automatically deemed Extremely Severe.

   For incidents rated Material or higher, covered institutions must:

   - Submit an initial report within one hour of discovery;
   - File a full report within 24 hours;
   - Provide rolling updates every two hours until resolution; and

- Submit a post-incident report (root-cause analysis, impact, accountability) within 10 working days, extendable to 40 days for complex cases.

  Failure to comply with these timelines constitutes a standalone violation under the Cybersecurity Law and may also trigger penalties under the Data Security Law or Personal Information Protection Law.

6. Governance and Accountability

Boards and senior management must appoint a dedicated data-security officer and embed data-protection responsibilities within business lines under the principle of "whoever manages the business manages the data and its security." Staff with access to high-sensitivity data must sign separate confidentiality agreements where employee handbooks provisions are insufficient. Outsourced processing must be integrated into overall outsourcing-risk frameworks, and activities expressly prohibited from outsourcing may not be delegated—even to affiliates.

Considerations

With the Measures already in force and no transition period being offered by the regulators, covered institutions should consider:

1. Completing a gap analysis against the 30-plus technical controls listed in the Measures;
2. Updating their incident responses plan to meet the new one-hour/24-hour reporting deadlines;
3. Mapping overlapping obligations under NFRA and CSRC rules and prepare for further regulatory coordination; and
4. Updating vendor contracts to impose the required confidentiality, deletion, and audit clauses for processors that may handle high-sensitivity data.

New National Standards for Sensitive Personal Information Processing

国家市场监督管理总局、国家标准化管理委员会发布《数据安全技术 敏感个人信息处理安全要求》

China released a new national standard on requirements for processing sensitive personal information (GB/T 45574—2025, the SPI Standard) on June 17, 2025. The SPI Standard sets out a framework for businesses, regulatory bodies, and third-party assessors to ensure the secure handling of sensitive personal information (SPI).

Key points for companies operating in China or handling China-related data include:

1. Expanded Scope of Sensitive Personal Information

- **Additional Categories**: Genetic data, gait recognition data, and "images/videos exposing private body parts" are explicitly classified as SPI;
- **Granular Classification**: SPI categories now include financial accounts, medical health data, religious beliefs, and minors' data (<14 years), with tailored sub-rules for each;
- **Aggregation Risk**: Non-sensitive data that, when combined, creates SPI-like profiles must be treated as SPI.

2. Consent Mechanisms

- Separate consent must be obtained for any SPI processing.

- **Written Consent**: Written consent is mandatory for biometric data collection without data subject's active cooperation (e.g., CCTV facial recognition), public-space image collection, and genetic/health research data collection that impacts SPI.
- **Dynamic Consent**: Dynamic consent is required for continuous SPI collection (e.g., location tracking), including recurring prompts through icons, notifications, or vibrations.
- **No Bundling**: Consent must be purpose-specific and cannot be consolidated into blanket "all-in-one" opt-ins.

3. Technical and Operational Mandates

- **Biometric Data**: Raw images or videos must be deleted once feature extraction is complete.
- **Location Data**: Prohibited from mapping "sensitive zones" (e.g., military areas).
- **Access Controls**: Structured data must have field-level restrictions, while unstructured data must be restricted at the file level.
- **Encryption and Storage**: SPI must be encrypted at rest and in transit, with encryption keys managed through certified hardware security modules.

4. Accountability and Governance

- **DPO Appointment**: Organizations processing more than 100,000 SPI records must appoint a board-level data protection officer (DPO) and conduct background checks on the DPO and other key personnel.
- **Documentation**: Documentation requirements include maintaining SPI directories, conducting impact assessments, and retaining audit logs for at least three years.

5. Compliance Considerations

- Update SPI inventories to align with classifications with Appendix A of the SPI Standard.
- Revise consent workflows, ensuring separate or written consent is obtained before processing high-risk SPI.
- Implement technical controls such as field-level encryption, access restrictions, and data minimization measures.
- For minors' data, integrate age-verification mechanisms and parental consent and oversight tools.
- Prepare for audits by documenting SPI flows, conducting impact assessments, and maintaining detailed access logs.

China Proposes Updated Regulations on Exporting Automobile-Generated Data

《汽车数据出境安全指引（2025 版）》征求意见

On June 13, 2025, several Chinese government agencies, including the Ministry of Industry and Information Technology (MIIT), the National Internet Information Office (CAC), and others, released the draft "*Guidelines for the Security of Cross-Border Data Transfer in the Automobile Industry (2025 Edition)*" for public comment. As of Aug. 7, 2025, these guidelines are still under consultation but, once finalized, may reshape how automobile data is classified, managed, and exported across borders.

Key New Developments

The 2025 draft guidelines introduce notable changes compared to the 2021 draft, aimed at tightening oversight of automobile-related data exports, including:

1. New Exemption Scenarios for Outbound Data

The guidelines specify three additional scenarios where cross-border data transfers are exempt from mandatory safety assessments.

- **Security Vulnerability Data**: Data reported to MIIT under the Network Product Security Vulnerability Management Regulations.
- **Security Event Data**: Data reported as part of industry emergency plans to MIIT and relevant regulators.
- **OTA Software for Recalls**: Over-The-Air (OTA) upgrade software source code provided for defect recalls, filed with the State Administration for Market Regulation.

2. Scenario-Based Identification of Important Data

The draft guidelines introduce refined guidance for recognizing and identifying "important data" in different business activities.

Scenarios	Important Data
R&D and Testing	• Data related to state-funded projects (national key R&D plans), • sensitive test data (high-precision geo-data, public security imagery), • production control source code, etc.
Autonomous Driving (AD)	• Algorithms: Source code/parameters for AD functions that won provincial/ministerial awards or related to state-funded projects (national key R&D plans), • Training data meeting specific criteria (see below).
Software Upgrades (OTA)	Source code for OTA upgrade packages affecting core vehicle functions (startup, power loss, braking, cruise, lane-keep) on vehicles operating in China.
Connected Operations	Data like cryptographic keys (>100k vehicles), precise mapping data affecting national security, sensitive charging network data, etc.

The following training data/datasets generated in autonomous driving activities would be recognized as important data:

- Scale-Based Thresholds: data or datasets achieving any of the following thresholds would be considered important data:
  - **Raw Image Data**: > 10 million original images.
  - **Raw Video Data**: > 1 million original video clips.

  - **Driving Distance/Time**: Data collected over > 5,000 km or > 2,000 hours of real-world driving.
  - **Vehicle Fleet Size**: Data sourced from > 100,000 vehicles operating in China.
- Sensitivity-Based Recognition: the following data would be recognized as important data even if the above thresholds are not met:
  - **Mapping Sensitive Areas**: Training data revealing geographic coordinates, infrastructure details, or traffic patterns in: (i) military zones, government facilities, or other restricted areas, or (ii) locations designated as "state secrets" under China's geographic data regulations.
  - **Public Security Data**: Scenes capturing law enforcement activities, public gatherings, or emergencies.
  - **Critical Infrastructure**: Detailed imagery of ports, power plants, or communication hubs.

3. Enhanced Safety Management Requirements

The guidelines introduce detailed safety management obligations, including:

- **Organizational Measures**: Appointing a person responsible for data outbound safety, establishing dedicated data management departments, and implementing internal approval processes for data transfers.
- **Technical Measures**: Ensuring secure data transmission (e.g., through encryption), monitoring data flows, and retaining logs for at least three years with tamper-proof mechanisms.
- **Emergency Response**: Developing plans to handle data security incidents and report violations to regulators promptly. These requirements are more comprehensive than the 2021 regulations, which focused primarily on general data handling principles.

4. Broader Applicable Entities

The guidelines apply not only to automobile manufacturers but also to parts and software suppliers, dealers, repair institutions, mobility service providers, telecom operators, autonomous driving service providers, and platform operators.

Considerations for Automotive Businesses:

- *Gap Analysis*: Compare current data handling practices, Important data identification methods, and export processes against the draft guidelines. Identify major discrepancies.
- *Data Mapping Acceleration*: Intensify efforts to map data flows (especially cross-border), focusing on the specific scenarios and data types outlined in the Draft Guidelines (R&D, AD, OTA, V2X).
- *Stakeholder Briefing*: Inform headquarters and relevant global departments (legal, compliance, IT security, product development, manufacturing, etc.) about the potential impact and required resources.
- *Assess CIIO Status*: Confirm if any China operations qualify as CIIO, as this may impact applicability of exemptions and overall requirements.

Foreign Investment

Three Authorities Jointly Issue the Market Access Negative List (2025 Edition)

三部门印发《市场准入负面清单（2025 年版）》

On April 16, 2025, China's National Development and Reform Commission, along with two other government authorities, jointly released the Market Access Negative List (2025 Edition) (2025 List), which took effect immediately.

This Market Access Negative List outlines industries, sectors, and business activities that are either prohibited or restricted for investment and operation within mainland China. It serves as a regulatory framework for all levels of government to enforce appropriate oversight. The Market Access Negative List applies the same standards to both domestic and foreign enterprises and is updated every two to three years. Compared to the 2022 edition, the 2025 List has been streamlined: the number of items has been reduced from 117 to 106, with 17 national-level restrictions and 16 local-level restrictions removed. Key changes and their significance include:

- **Licensing Reforms to Boost Market Access Efficiency**
  - The seal engraving industry has transitioned from a licensing system to a filing system, with the process shortened to one working day. Public security authorities aim to strengthen oversight through backend data monitoring to prevent the risk of forged seals.
  - Sales of computer information system security products now follow a certification process based on national standards. The certification timeline has been cut from 30–60 days to 15 days.
- **Easing Entry Barriers While Maintaining Oversight**
  - Approval requirements for establishing television production companies and for setting up pharmaceutical wholesale and retail businesses have been eliminated, lowering entry thresholds.
  - The approval process for pharmaceutical enterprises has been reduced by 50%, with average processing time shortened from three months to one.
  - Core regulatory standards remain in place—for example, pharmaceutical businesses must employ licensed pharmacists and meet Good Supply Practice (GSP) standards, while TV productions must still undergo content review.
- **Removing Local Restrictions to Promote a Unified National Market**
  - 17 local-level restrictions have been scrapped, including:
    - Special traffic limitations on freight vehicles from other regions; and
    - Local testing requirements for alcoholic products produced outside the region before entering the local market.
- **Including Emerging Industries to Clarify Regulatory Boundaries**
  - For the first time, new business models such as civilian drone operations (excluding micro drones) and the production, wholesale, and retail of electronic cigarettes have been added to the list, helping to improve regulatory oversight.
  - Drone Regulation:
    - Light and heavier drones must obtain an operating certificate.

  - The list aligns with the Interim Regulations on the Administration of Unmanned Aerial Vehicle Flights, which designate no-fly zones.
  - While encouraging drone use in logistics and agriculture, the regulations aim to prevent unauthorized flights that could disrupt civil aviation or compromise sensitive information.
- E-Cigarette Regulation:
  - Production requires a tobacco monopoly license.
  - Products must comply with the national nicotine standard of <20mg/g.
  - Sales to minors are prohibited to maintain orderly market access.

China Proposes New Foreign Exchange Policies to Boost Cross-Border Investment and Financing

国家外汇局就深化跨境投融资外汇管理改革事宜征求意见

On June 18, 2025, China's State Administration of Foreign Exchange (SAFE) released a draft notice titled "Notice on Deepening the Reform of Foreign Exchange Administration for Cross-border Investment and Financing," soliciting public comments until July 18, 2025. Once finalized, these rules may enhance the ease of doing business for foreign investors in China by optimizing foreign exchange management and promoting cross-border investment and financing.

The proposed reforms focus on simplifying foreign direct investment (FDI) procedures, enhancing cross-border financing, and liberalizing capital account use. Below is a detailed breakdown of the key changes:

Key Reforms

1. **Simplifying Foreign Direct Investment (FDI) Procedures**: The draft eliminates several bureaucratic requirements to facilitate FDI.
   - **Eliminating Preliminary Expense Registration**: Foreign investors no longer need to register basic information for pre-establishment expenses when setting up enterprises. They may directly open preliminary expense accounts and remit funds, with banks reviewing expense amounts based on the Application Form for Preliminary Expense Business. If no foreign-invested enterprise (FIE) is established, accounts must be closed, and remaining funds repatriated.
   - **Cancelling Domestic Reinvestment Registration**: FIEs can now reinvest domestically without registration, provided the reinvestment complies with China's Special Administrative Measures for Foreign Investment Access and is genuine. This policy, previously piloted in 19 provinces, is now extended nationwide.
   - **Reinvesting Foreign Exchange Profits**: FIEs and foreign investors can use legally generated foreign exchange profits for domestic reinvestment. This requires a written application, business licenses, authenticity certification (e.g., audited financial reports), and investment agreements for fund remittance to capital or settlement accounts.
   - **Supporting Non-Enterprise Research Institutions**: Domestic non-enterprise research institutions may receive foreign funds following FDI procedures.
2. **Enhanced Cross-Border Financing**: The reforms seek to expand financing opportunities for eligible enterprises.

- **Increased Borrowing Limits**: Qualified high-tech enterprises, small and medium enterprises (SMEs), and those classified as "specialized, refined, distinctive, and innovative" (SRDI) or sci-tech may borrow foreign debt up to USD 10 million. Enterprises selected under the "innovation credit scoring system" may borrow up to USD 20 million. This extends a pilot policy (previously USD 10 million in over 10 regions, USD 5 million elsewhere) nationwide.
- **Streamlined Registration**: The registration process for foreign debt contracts is simplified, eliminating the need for audited financial reports. Required documents include the application form, business license, Eligible Technology Enterprise certification, and loan letter/intent or contract.

3. **Liberalization of Capital Account Use**: The draft reduces restrictions on how capital account proceeds can be used.

- **Reduced Negative List**: The restriction on using capital account proceeds to purchase real estate for non-self-use has been lifted, except for real estate developers and leasing businesses. However, capital account income is still prohibited for:
  - Prohibited expenditures;
  - Securities or high-risk investments (except Level II wealth management products); and
  - Loans to non-affiliates (except in permitted cases).
- **Flexible Bank Oversight**: Banks may independently determine the frequency and proportion of post-payment random checks based on client compliance and risk ratings. Previously, minimum sampling was 5% for "A" rated banks and 10% for "B" rated banks. Banks may now use risk transaction monitoring instead of sampling.
- **Eased Foreign Exchange Settlement for Property Purchases**: Overseas individuals can settle foreign exchange for purchasing real property in China by first making payments with the contract/agreement and later supplementing record-filing documents. This policy, previously piloted in the Guangdong-Hong Kong-Macao Greater Bay Area, is now extended nationwide, with a monthly backup payment limit of USD 200,000.

Implications for Foreign Investors

These reforms signal China's commitment to creating a more investor-friendly environment, particularly for FDI. By reducing bureaucratic hurdles and increasing flexibility in fund management, the policies aim to attract more foreign capital, especially in high-tech and innovative sectors. Key benefits include:

- *Easier Market Entry*: Simplified procedures for setting up enterprises and reinvesting profits seek to reduce time and costs for foreign investors.
- *Increased Financing Access*: Higher borrowing limits and streamlined registration processes may allow eligible enterprises to secure foreign debt more easily.
- *Greater Flexibility in Capital Use*: The liberalization of capital account restrictions may allow investors to allocate funds more freely, including for real estate investments.
- *Support for Innovation*: The focus on high-tech and SRDI enterprises aligns with China's push for technological advancement, offering opportunities for investors in these sectors.
- *Enhanced Property Investment*: The eased foreign exchange settlement for property purchases may encourage more overseas individuals to invest in China's real estate market.

The reforms may increase investment flows into China, particularly in industries prioritized under the 2025 Action Plan, such as manufacturing and biomedicine. However, their success will depend on effective implementation and the global economic environment.

Next Steps

The draft is currently under review, and the final version may incorporate feedback received during the public comment period, which closed on July 18, 2025. Foreign investors should review the draft and stay updated on the final rules. Engaging with legal and financial advisors familiar with China's foreign exchange regulations may also help investors prepare for the changes.

China's New Tax Incentive Policy for Foreign Investors' Domestic Reinvestment

三部门出台境外投资者以分配利润直接投资税收抵免政策

On June 27, 2025, China introduced a new tax credit policy to encourage foreign investors to reinvest profits from Chinese resident enterprises into the domestic market. Detailed in a joint announcement by the Ministry of Finance, State Taxation Administration, and Ministry of Commerce (Announcement No. 2, 2025), and further clarified by the State Taxation Administration (Announcement No. 18, 2025), this policy offers a 10% corporate income tax credit for eligible reinvestments made between Jan. 1, 2025, and Dec. 31, 2028.

Key provisions of the policy include:

1. **10% Tax Credit for Reinvested Profits**: Foreign investors reinvesting profits from Chinese resident enterprises into qualified domestic projects may claim a tax credit of 10% of the reinvested amount.
   - *Credit Usage*: Offsets corporate income tax (CIT) on dividends, interest, or royalties from the same profit-distributing enterprise. Unused credits carry forward indefinitely.
   - *Tax Treaty Benefit*: If a bilateral tax treaty stipulates a dividend tax rate below 10%, the lower rate applies.
2. **Eligible Reinvestments**: Reinvestments must target sectors listed in China's "Encouraged Catalogue" for foreign investment, such as high-tech and strategic industries. Eligible activities include:
   - Increasing capital in existing Chinese resident enterprises;
   - Establishing new resident enterprises in China; or
   - Acquiring equity in Chinese resident enterprises from non-related parties.
3. **Holding Period**: A minimum five-year (60-month) holding period is required, starting from the month of reinvestment as recorded in the "Profit Reinvestment Statement" that commerce authorities issue. The period ends when the investment is withdrawn or legal formalities (e.g., equity change or deregistration) are completed. Early withdrawal triggers a proportional reduction of the tax credit.
4. **Tax Treatment for Withdrawal After Five Years**: If the reinvestment is withdrawn after five years, the deferred withholding tax on the corresponding profit distribution must be paid within seven days. Any remaining tax credits may be used to offset taxes on dividends, interest, or royalties from the same profit-distributing enterprise.

5. **Withdrawal Within Five Years**: If the reinvestment is withdrawn before five years, the following applies:
   - The deferred withholding tax must be paid within seven days.
   - The tax credit is reduced proportionally to the withdrawn amount.
   - If more credit has been used than permitted after the reduction, the excess must be repaid within seven days, with penalties calculated from the date the credit was applied.
6. **Retroactive Application from Jan. 1, 2025**: Investments made between Jan. 1, 2025, and the announcement date may apply retroactively for the tax credit, but only for taxes due post-announcement.

The new tax credit policy for reinvestment signals China's commitment to encouraging foreign investment, reducing tax burdens for long-term investors while imposing stricter requirements. The upgraded tax incentives, paired with enhanced supervision, require foreign investors to conduct self-assessments and reviews. Additionally, the domestic reinvestment tax credit may affect effective tax rates under Pillar Two, urging multinational enterprises to evaluate its impact.

** This GT Newsletter is limited to non-U.S. matters and law.*

Read previous issues of GT's China Newsletter.

Authors

This GT Newsletter was prepared by:

- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Dawn Zhang | +86 (0) 21.6391.6633 | zhangd@gtlaw.com
- Philip Ruan | +86 (0) 21.6391.6633 | ruanp@gtlaw.com
- Sherry Xiaoxuan Ding | +1 415.655.1300 | dings@gtlaw.com