GT GreenbergTraurig

China Newsletter | 2026 Q2/Issue No. 68

In This Issue:

Data Privacy & Cybersecurity | Foreign Investment | Intellectual Property | International Trade

---

This China Newsletter provides an overview of key Q2 2026 developments in the following areas:

1. Data Privacy & Cybersecurity

- *China Releases Measures on Network Data Security Risk Assessment.*

2. Foreign Investment

- *China Issues New Rules on Outbound Investment.*

3. Intellectual Property

- *China Revises the Trademark Law (2026 Amendment).*

4. International Trade

- *New PRC Regulations on Supply Chain Security and Anti-Foreign Extraterritorial Jurisdiction.*

Data Privacy & Cybersecurity

China Operationalizes Network Data Security Risk Assessments Measures

《网络数据安全风险评估办法》（国家网信办、工信部、公安部令第 24 号）

On 18 June 2026, the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS) jointly issued the Measures for Network Data Security Risk Assessment (the Measures), effective 20 August 2026. The Measures are China's first dedicated operational rulebook for data security risk assessments. They implement and operationalize the risk assessment requirements under the Data Security Law and the Network Data Security Management Regulations, filling a longstanding gap on assessment triggers, procedures, and reporting requirements. Their joint issuance by three regulators may also signal closer cross-agency coordination in enforcement.

The Measures convert what has been a largely principle-based statutory duty into a concrete, auditable compliance process: who must assess, how often, through whom, in what form, and with what reporting and remediation follow-through.

Key Highlights

Who Must Assess — and When

The Measures apply broadly to "network data processors" (网络数据处理者), while imposing enhanced obligations on network data processors that process important data, and in certain cases, core data. Network data processors that process important data must conduct a comprehensive risk assessment at least once annually and should consider conducting ad hoc assessment where a major change could adversely affect data security. According to official government commentary, examples of such changes could include a sharp increase in data volume, a change in processing purpose, a change in cross-border transfer scenarios, or the deployment of new technology such as AI model training. Network data processors that process general data (not important data) are encouraged, but not required, to assess at least once every three years. Core data remains subject to separate rules yet to be specified, and important data involving encryption also requires a commercial cryptography security assessment under separate rules.

Who Conducts the Assessment

Assessments may be self-conducted or performed by a third-party assessment institution. Certification of assessment institutions is encouraged but not mandatory — except where a regulator mandates an assessment. Institutions may not subcontract, and the same institution (including its affiliates) may not perform a network data processor's annual assessment for more than three consecutive years.

Reporting, Retention, and Regulatory Verification

Assessment reports must follow the competent authority's requirements or, absent such requirements, national standards. Reports must be retained for at least three years, and the annual report must be submitted within 20 working days of completion — to the competent authority. Reports are shared among the CAC, telecommunications, public security and state security authorities, and regulators may verify their authenticity and accuracy through spot checks.

Regulator-Mandated Assessments

Where processing activity poses a significant risk that may endanger national security or the public interest, or where a security incident has caused large-scale data breach or unlawful disclosure of important data or personal information, authorities at the provincial level or above may order the network data processor to engage a certified assessment institution. The processor must then provide access to systems, data, operation logs, and premises; complete the assessment within the prescribed timeframe; submit the signed and chopped report; and — if issues are identified — rectify and file a rectification report within 15 working days. The same incident or risk cannot be used to justify a repeat mandated assessment.

Enforcement Through Existing Penalty Tiers

The Measures do not create any standalone monetary penalties; violations are enforced through China's Data Security Law. Under the Data Security Law, failures to fulfil statutory data-security obligations attract correction orders and warnings plus fines of RMB 50,000–500,000 on entities and RMB 10,000–100,000 on responsible individuals, rising to RMB 500,000–2,000,000 and RMB 50,000–200,000 respectively where the entity refuses to correct or a large-scale data leak results — with possible business suspension or license revocation. Core-data violations endangering national sovereignty, security, or development interests carry fines of RMB 2,000,000–10,000,000 and potential criminal liability.

Parallel — Not a Substitute — to Other Assessment Regimes

An assessment under the Measures does not replace other assessment, review, or filing obligations that apply in parallel, such as the CAC's security assessment for cross-border data transfers, personal information protection compliance audits, cybersecurity review under the Cybersecurity Review Measures, or multi-level protection scheme (MLPS) filings. Unlike cybersecurity review, which is a transaction- or event-driven national security review mechanism, the Measures establish a recurring risk-management and compliance framework focused on the ongoing security of network data processing activities. Compliance programs should treat these as distinct workstreams.

Considerations for Stakeholders

Stakeholders subject to the Measures may wish to consider the following action items:

- **Confirm scope first:** determine whether an entity or individual's China operations qualify as a network data processor that processes "important data" under applicable catalogues or regulator notice. If so, the annual assessment is a statutory duty — stakeholders should consider adding it to the calendar and budgeting ahead of the 20 August 2026 effective date.
- **Plan the assessment model:** choose between self-assessment and third-party assessment; if relying on external vendors, plan for the three-year rotation cap in advance.
- **Flag ad hoc triggers internally:** new AI deployments, changed processing purposes, and changed cross-border scenarios may need to be treated as escalation points, not folded silently into the annual cycle.
- **Extend existing programs:** because enforcement runs through the Data Security Law's penalty tiers, stakeholders should consider extending existing DSL compliance programs to cover the new assessment and reporting mechanics.

- **Prepare for routine checks:** companies in regulated sectors may see risk-assessment compliance being examined as part of regular sector oversight, not only after incidents.

Foreign Investment

China Issues New Rules on Outbound Investment

《国务院关于对外投资的规定》（国务院令第 837 号）

On 1 June 2026, China's State Council issued the Regulations on Outbound Investment (Order No. 837), which took effect 1 July 2026. The Regulations establish China's first comprehensive administrative framework governing outbound investment, elevating and consolidating existing departmental rules and regulatory practices into a unified framework.

The Regulations reshape China's outbound investment compliance landscape by expanding the scope of regulated investors, codifying national security review, strengthening ongoing compliance obligations, and introducing a comprehensive liability regime.

Background

China's outbound investment regime has historically been governed by a combination of departmental rules issued by the National Development and Reform Commission (NDRC), the Ministry of Commerce (MOFCOM), the State Administration of Foreign Exchange (SAFE), and other authorities. While these rules established approval, filing, and foreign exchange procedures, China previously lacked a unified administrative regulation governing outbound investment.

The Regulations consolidate the existing regulatory framework into a single State Council legislation. Beyond codifying current practice, they also reflect China's increasing emphasis on balancing outbound investment facilitation with national security, overseas compliance, risk management, and protection of national interests.

Key Highlights

Broader and More Penetrating Coverage

The Regulations apply to all Chinese "investors," including enterprises, other organizations, and for the first time at this regulatory level, PRC resident individuals.

The Regulations' definition of investors is noteworthy because previous outbound investment rules primarily focused on enterprises. The inclusion of resident individuals may signal the government's intention to establish a more comprehensive legal framework for individual outbound investment. However, implementing rules for resident individuals have not yet been issued.

The Regulations define outbound investment broadly as activities whereby investors acquire, directly or indirectly, ownership, control, management rights, or other interests in overseas enterprises or assets through capital contributions, equity investment, provision of financing, guarantees, or other investment arrangements. The definition therefore captures not only traditional acquisitions and greenfield investments, but also many financing structures that may confer control or economic interests overseas.

Compared with previous outbound investment rules, the Regulations also extend, with appropriate modifications, to investments in Hong Kong, Macau, and Taiwan, and — together with other applicable state provisions — to offshore financial-market investment using self-owned, raised, or entrusted funds and the overseas reinvestment of outbound investment returns. Dedicated implementing rules for these categories have not yet been issued. Inbound foreign direct investment into China falls outside the scope of the Regulations and continues to be governed by the Foreign Investment Law regime. Notably, companies established in China — including foreign-invested enterprises — are covered when they invest abroad.

Policy-Based Classification of Outbound Investment

The NDRC and MOFCOM, together with other authorities, are tasked with designating outbound investments as encouraged, restricted, or prohibited, by reference to national development needs and the investment environment and risk profile of host countries and regions. The specific catalogue or criteria for the restricted and prohibited categories have not yet been published. In the interim, the existing departmental approval and filing tracks under NDRC Order No. 11 and MOFCOM Order No. 3 continue to operate. How those filing tracks will be reconciled with the Regulations — including whether they will be amended or repealed — remains to be clarified.

Likely Sector and Country Impact

In practice, the impact may be most visible in technology-, data- and resource-intensive sectors — including advanced manufacturing and mobility, semiconductors and electronics, AI and other data-intensive technology, life sciences, energy and critical minerals — particularly where the transaction involves transferring IP, production know-how, technical data, source code or specialist personnel offshore.

Deal-level friction may be particularly acute in the U.S. corridor: Chinese acquisitions of, or investments in, U.S. targets may now face PRC outbound security review and export-control constraints in parallel with CFIUS review. That is a regulatory overlay, not a designation of the United States as a "sensitive country." Destinations with substantial Chinese deal flow, such as Australia, Singapore, Germany and Japan, etc., according to EY's H1 2026 review of announced Chinese overseas M&A, may also see the most immediate operational impact even where the host country is not sensitive.

Codification of Outbound Investment Security Review

The Regulations establish a dedicated security review regime for outbound investment. Outbound investments that affect or may affect national security — as well as subsequent transfers or disposals of the related overseas assets or interests — are subject to review, and parties must cooperate with the review and comply with its outcome. The Regulations further provide that such security review may arise not only before the commencement of outbound investment but also at exit or restructuring stages. The scope, procedure, and reviewing authority for the mechanism await implementing rules. The new regime complements China's existing inbound investment security review.

Integration of Export Controls

The Regulations build export-control compliance directly into outbound investment activity. Investors may not export or use export-prohibited goods, technology, services, or related data, and must obtain a license for export-restricted items — including where the transfer occurs indirectly through cross-border secondment of personnel, technical guidance, or overseas training. Other intersecting regimes — foreign

exchange, cross-border data flows, merger control, export control, cybersecurity, tax, and state-asset supervision — continue to apply under their own rules.

Investor Protection and Countermeasures

The Regulations pair supervision with protection. They establish an overseas service system and consular protection for Chinese investors and their China-national employees, authorize investment-barrier investigations into host-country obstacles, and create a countermeasures framework: where a foreign state, organization or individual imposes discriminatory restrictions on Chinese investors, PRC authorities may respond with retaliatory measures — including listing under the Anti-Foreign Sanctions Law and restrictions on the foreign party's imports and exports, inbound investment, transactions with PRC persons, or entry into China.

A Liability Regime With Teeth

The Regulations raise the stakes compared with the prior departmental-rule regime, introducing percentage-of-investment fines and multi-year activity bans that were not previously available. These are summarized in the table below.

Violation	Penalty on Entity	Penalty on Individuals	Other Consequences
Making an outbound investment on the State's prohibited list	Order to stop the investment; forced divestiture of shares/assets within a deadline; confiscation of illegal gains; if non-compliant, fine of 0.5%–1% of investment amount	RMB 50,000–100,000	—
Failure to complete required approval/filing; or submission of false materials/ concealment in an approval/filing application	Order to correct; confiscation of illegal gains; fine of 0.1%–0.5% of investment amount; if uncorrected — order to stop + divest + fine of 0.5%–1%	RMB 20,000–50,000	—
Obtaining approval/filing through bribery or fraud	Revocation of approval/filing document; confiscation of illegal gains; fine of 0.1%–0.5%; if already invested — order to stop + divest + fine of 0.5%–1%	RMB 20,000–50,000	—
Follow-on consequence for the three violations above	—	—	Authorities may bar new approval/filing applications for up to three years, or prohibit outbound investment activity

Violation	Penalty on Entity	Penalty on Individuals	Other Consequences
			for one to three years
Non-cooperation with, provision of false materials to, or non-compliance with a decision under, the security review mechanism	Order to correct; confiscation of illegal gains; fine; if national security is harmed — order to eliminate the impact; may order stop + divest	—	May prohibit outbound investment activity for one to three years
Breach of investor conduct obligations (unfair competition, trade-secret infringement, dumping, bribery, etc.)	Order to correct within a deadline	—	If harm results, may prohibit outbound investment activity for one to three years
Personal injury or property loss; public-security offenses; criminal conduct arising from outbound investment activity	Civil liability; public security administrative penalty; criminal liability, as applicable	Same as entity, as applicable	—
Public officials: abuse of power, dereliction of duty, malpractice for personal gain, or unauthorized disclosure of state secrets/trade secrets/ personal information	—	Disciplinary sanction; criminal liability if applicable	—

Implications for Stakeholders

- **Multinationals with PRC subsidiaries:** Outbound investment by a PRC-incorporated subsidiary — and by PRC-resident employees through SPVs or equity incentive plans — may now fall within scope. Impacted stakeholders should consider reviewing their compliance programs against the new individual-investor language.
- **Counterparties to Chinese outbound investors (M&A targets, JV partners, lenders):** Stakeholders may wish to factor the new security review layer and potential export-licensing requirements into deal timelines, closing conditions, cooperation covenants, and long-stop dates — and may wish to account for review at the disposal stage in exit structures.

- **All stakeholders:** Given the materially higher penalties, stakeholders may wish to elevate PRC-side compliance diligence for pending or planned outbound transactions.

Intellectual Property

China Adopts First Comprehensive Trademark Law Revision in Over Four Decades

《中华人民共和国商标法（2026 年修订）》

On 26 June 2026, the Standing Committee of the National People's Congress adopted the comprehensive revision of the Trademark Law of the People's Republic of China (the 2026 Revision), effective 1 January 2027. This marks the first full revision since the law's enactment in 1983 — the four earlier changes in 1993, 2001, 2013, and 2019 were piecemeal amendments — and it expands the law from 73 to 87 articles across nine chapters, including a new dedicated chapter on registration conditions.

China is the world's largest trademark filing jurisdiction, but has long grappled with trademark squatting, speculative hoarding, and low utilization rates for registered marks. The 2019 amendment to the Trademark Law addressed bad-faith filings in principle, but enforcement remained inconsistent. The 2026 Revision converts those principles into specific legal standards, procedural tools, and administrative penalties, while adapting the regime to digital-economy practice.

Key Highlights

An Objective Test Against Hoarding — With Standalone Fines

Applications filed "without intent to use and clearly beyond the needs of normal production and business operations" will be refused, replacing the vaguer "malicious filing" standard with an objective inquiry into whether the filing matches the applicant's real business needs. The 2026 Revision also broadens the protected baseline from "prior rights" to "prior legitimate rights and interests", which can capture influential trade names, packaging, trade dress and similar business identifiers, not only formal registered rights. A new standalone administrative penalty will allow fines of up to RMB 100,000 for bad-faith filings that cause adverse effects — including knowing filings of prohibited signs, filings clearly exceeding business needs, and intentional violations of prior rights. Although not defined in the Trademark Law or its implementing regulations, it is generally understood that "adverse effects" in this context would include adverse effects on market order or public interest, or other adverse social impact, which the trademark enforcement agencies would have considerable latitude to determine. Defensive registrations will remain possible but will require a demonstrable commercial rationale.

Stronger Anti-Squatting Standards

The 2026 Revision tightens the rule against trademark squatting: the act of applying to register a mark that another party has already used and that has a certain influence. The test shifts from "improper means" to "intentional" preemption, so disputes will turn more directly on whether the applicant knew, or should have known, of that prior use. Article 20 also now states in a single provision that a later application may be refused if it is identical or similar to an earlier-filed — not only an earlier-registered — mark on the same or similar goods.

Faster and Cleaner Procedures

The opposition window following preliminary approval will be shortened from three months to two. Suspension rules will be unified across opposition, review, and invalidation proceedings. The one-year bar on identical or similar refilings will be narrowed to voluntary cancellations only — marks cleared through non-use cancellation or invalidation will no longer block refilings, which may accelerate the cleanup of squatted marks.

Use It Properly — or Lose It

Under the 2026 Revision, trademark use expressly includes use through the internet and other information networks, and dynamic (motion) marks will become registrable. Misleading use of a registered mark will be a new offense punishable by fines of up to five times unlawful gains (or RMB 250,000 where gains are low), with revocation for failure to correct. Unauthorized alteration of a registered mark will carry fines of up to RMB 50,000. The trademark authority may also cancel marks for three consecutive years of non-use or genericide (where a mark has become the common name for the goods or services) on its own initiative — previously, cancellation required a third-party request.

Broader Well-Known Mark Protection

Cross-class, anti-dilution protection — previously limited to registered well-known marks — is extended to unregistered well-known marks in appropriate circumstances, which may be a meaningful gain for foreign brands not yet registered in China. Well-known status recognition will also become available in unfair-competition proceedings, and the trademark authority may confirm a mark's well-known status in China for use in trademark proceedings.

Tighter Agency Regulation

Trademark agencies and practitioners will be required to act in good faith and with due diligence and warn clients against filings that may violate the law's prohibitions. Trademark practitioners will not be able to simultaneously work for multiple agencies or accept instructions outside of their agency relationship. Agencies involved in fraud, conflicted representation, or facilitation of bad-faith filings may face fines of RMB 10,000-200,000 (escalating for serious cases), parallel fines on responsible individuals, and possible suspension of their right to file before the China National Intellectual Property Administration (CNIPA).

Fair Use and Anti-Abuse Boundaries

Descriptive fair use is broadened, and a new statutory "indicative use" defense will protect genuine aftermarket activities — including spare parts "for Brand X," independent repair services, and genuine resale — absent a likelihood of confusion. An express anti-abuse principle is added, and parties that pursue trademark litigation through malicious collusion or fabrication of facts may face court sanctions plus civil liability for resulting losses. Licensors, meanwhile, will gain a statutory right to terminate licensees that breach quality obligations.

Damages Clarified, Not Expanded

The damages ceilings remain unchanged: punitive damages of one to five times will remain available for willful, serious infringement, and the statutory cap stays at RMB 5 million. What will change is calibration — actual loss and infringer's profit will become co-equal rather than sequential measures; courts will

retain the power to order production of an infringer's accounts with adverse inferences for non-compliance; and the three-year non-use defense to damages is clarified to run backward from the occurrence of the alleged infringing act. Administrative enforcement powers are widened to cover electronic data and evidence preservation, and administrative-criminal case transfer becomes two-way.

Key Takeaways for Stakeholders

Stakeholders impacted by the 2026 Revisions should consider the following:

- **Audit portfolios in 2026:** Stakeholders may wish to assess whether unused or defensive registrations could be vulnerable to ex officio cancellation or refusal and should consider documenting the commercial rationale and genuine use of retained marks — e-commerce and social-media use counts.
- **Move faster on oppositions:** The two-month window may call for continuous watching services, pre-built evidence files, and rapid internal sign-off.
- **Reassess anti-squatting strategy:** The shift from an "improper means" test to an "intentional" preemption test should make it easier to challenge filings that copy a mark already in use, and with a certain influence, but not yet registered in China — provided the brand owner can show the applicant knew or should have known of that use.
- **Review prior-interest and well-known-mark filings**: Broader protection of "prior legitimate rights and interests" (including influential trade names, packaging and similar identifiers) and cross-class protection for unregistered well-known marks may give foreign brands additional grounds beyond classic squatting claims.
- **Mindful use:** Misleading or altered use of an individual or entity's own registered marks may attract fines — and even cost the registration itself — once the 2026 Revisions take effect.
- **Review licensing and agency arrangements:** Stakeholders should consider using the statutory termination right in license drafting and conducting due diligence on local agents, whose filing conduct may carry higher exposure.
- **Enforce with evidence:** With damages ceilings unchanged but bad-faith litigation to become sanctionable, stakeholders should consider compiling strong evidence on both use and loss for enforcement actions.

International Trade

New PRC Regulations on Supply Chain Security and Anti-Foreign Extraterritorial Jurisdiction

中国出台产业链供应链安全领域与反不当域外管辖相关法规

On 7 April 2026, China's State Council promulgated Decrees No. 834 and No. 835, respectively issuing the *Regulations of the State Council on Industrial and Supply Chain Security* (Regulation 834) and the *Regulations of the People's Republic of China on Counteracting Foreign Improper Extraterritorial Jurisdiction* (Anti-Extraterritorial Jurisdiction Regulations). Both regulations took effect immediately upon publication, with no transition period. On 22 June 2026, MOFCOM issued Announcement No. 24 of

2026, publishing the *Measures for Industrial and Supply Chain Security Investigations* (Investigation Measures) as the implementing rules for Regulation 834, which also became effective upon publication.

Together, these three instruments establish a comprehensive legal framework in China covering supply chain security from top-level design to enforcement, and from domestic regulation to countermeasures against foreign extraterritorial jurisdiction, with direct implications for multinational enterprises operating in China and participants in cross-border supply chains.

Anti-Extraterritorial Jurisdiction Regulations

The Anti-Extraterritorial Jurisdiction Regulations govern acts, measures, directives, or policies issued by foreign governments that seek to restrict how certain non-PRC actors or entities engage with the PRC and PRC entities.

This Regulation, consisting of 20 articles, is China's second major legislative instrument in the field of counteracting foreign extraterritorial jurisdiction, following the *Anti-Foreign Sanctions Law* (2021).

Key mechanisms include:

Identification and Announcement of Improper Measures

The State Council's legal affairs department, together with relevant agencies, identifies foreign extraterritorial jurisdiction measures based on four factors: (i) violation of international law and basic norms of international relations; (ii) appropriateness of the connection between the conduct and the foreign jurisdiction; (iii) harm to China's sovereignty, security, or development interests, or infringement of rights of Chinese citizens/organizations; and (iv) other relevant considerations. Measures identified as improper may be publicly announced, and the Regulations restrict organizations and individuals from complying with the improper measure or assisting with its execution.

Malicious Entity List and Nine Countermeasures

Foreign organizations or individuals that promote or participate in implementing improper extraterritorial jurisdiction measures may be added to the malicious entity list. Countermeasures include visa denial or entry ban; cancellation or restriction of work/residence permits; seizure or freezing of assets in China; restrictions on data, personal information, and transactions; prohibitions on import/export activities; investment bans; restrictions on products/transport entering China; fines; and other necessary measures. These may extend to entities controlled or operated by listed parties.

Prohibition Orders and Judicial Remedies

The State Council's legal affairs department may issue prohibition orders against organizations or individuals for complying with or assisting in the implementation of improper measures. Victims may bring civil actions in Chinese courts for cessation and damages. Non-compliance with countermeasures or prohibition orders may result in corrective orders, restrictions on government procurement, bidding, import/export, cross-border data transfer, exit/entry, fines, and criminal liability where applicable.

Exemption Application Mechanism

Chinese citizens or organizations that, due to special circumstances, must execute or assist in executing foreign measures, or must engage in otherwise prohibited activities with listed parties, must apply to the

State Council's legal affairs department or relevant agency for approval, providing facts and reasons. Only upon approval may such activities proceed within a defined scope.

Regulation 834 and Investigation Measures

Regulation 834 (18 articles) establishes the top-level framework for supply chain security. The Investigation Measures (22 articles), issued by MOFCOM, implement Regulation 834's investigative authority.

Two Triggering Scenarios for Investigation

The following scenarios may trigger an investigation under Regulation 834 and its Investigation Measures:

- **State/Regional/International Level:** Foreign states, regions, or international organizations violate international law/norms and impose discriminatory prohibitions or restrictions affecting China's supply chain security.
- **Foreign Organization/Individual Level:** Foreign organizations or individuals violate market principles, disrupt normal transactions with Chinese parties, or impose discriminatory measures causing or threatening substantial harm to China's supply chain security.

Damage Assessment and Investigation Procedures

MOFCOM assesses harm based on: (i) security of domestic/foreign elements (materials, technology, capital, data, personnel, enterprises, projects); (ii) smoothness of flows (logistics, commerce, personnel, capital, data, information); and (iii) impact on international competitiveness and development potential. Investigations may be initiated upon applications by domestic entities or provincial commerce departments. Methods include inquiries, document review, public solicitation, questionnaires, sampling, technical appraisal, hearings, on-site inspections (including abroad unless objected to). Respondents may present defenses; refusal to cooperate may lead to determinations based on available facts. Investigations may be terminated if measures are withdrawn or settlements reached.

Three Levels of Countermeasures

- **Against States/Regions/International Organizations:** Prohibitions/restrictions on goods, technology, services; special fees; inclusion in countermeasure lists; measures under the Anti-Foreign Sanctions Law.
- **Against Foreign Organizations/Individuals**: Import/export bans; investment bans; transaction prohibitions; entry bans; cancellation/restriction of work/residence permits; measures extendable to controlled/affiliated entities.
- **Against Domestic Non-Compliance:** Corrective orders; restrictions on government procurement, bidding, import/export, services; restrictions on cross-border data/personal information transfer; exit/entry bans. Measures may be dynamically adjusted.

Considerations for Enterprises

Given the lack of transition period for the Regulations and their Implementing Measures, companies operating in China or engaged in cross-border supply chains may wish to assess:

1. **Supply Chain Risk Review**: Stakeholders should consider mapping reliance on foreign raw materials, technology, equipment; identifying single-country/region risks; and diversifying supply channels.

2. **List and Counterparty Monitoring**: Impacted entities and individuals should track MOFCOM countermeasure lists, State Council malicious entity lists, and announcements of improper measures; using that information, they should consider conducting thorough due diligence on counterparties.

3. **Compliance Priority**: When facing foreign sanctions, export controls, or court orders, stakeholders may wish to assess whether they constitute announced improper measures.

4. **Domestic Information Collection Compliance**: Foreign enterprises conducting supply chain audits, ESG reviews, or supplier checks in China must comply with PRC law to avoid penalties under Regulation 834.

5. **Cross-Border Data Controls**: Impacted entities and individuals may wish to review all scenarios of data/personal information transfer abroad; assess whether recipients are listed entities; and adjust transmission arrangements accordingly.

6. **Internal Response Mechanism**: Stakeholders should consider establishing standard operating procedures for receiving, evaluating, and reporting foreign extraterritorial jurisdiction demands; preserving evidence; and pursuing claims in Chinese courts if necessary.

** 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