GT GreenbergTraurig

Advisory | Data Privacy & Cybersecurity

February 2026

China's Amended Cybersecurity Law Takes Effect

The amended Cybersecurity Law of China (CSL) entered into force on Jan. 1, 2026. These amendments, officially approved by China's top legislature in October 2025, mark the first major changes to the law since it took effect in 2017. Without altering obligations of cybernetwork operators under CSL, the amendments specify the penalties applicable to breaches of different obligations, expand the government's power to enforce against extra-territorial activities jeopardizing China's cybersecurity, and set forth certain policy and regulatory goals for the new governance regime on developing and applying AI.

What Remained Unchanged?

The Cybersecurity Administration of China (CAC) first proposed the amendments in September 2022, with the stated purpose of "modifying and improving the legal responsibilities" applicable to different breaches of the obligations under CSL. The final amendments reflected those goals.

In a nutshell, the obligations applicable to different cybernetwork operators (i.e., businesses using any form of public or private network) under CSL remain unchanged, and the jurisdiction of the law, as stated under Article 2 of CSL, remains limited to "construction, operation, maintenance, and use of cybernetworks, and supervision and administration of cybersecurity within the territory of the People's Republic of China."

What Has Changed?

Three areas of CSL have changed with the amendments.

- **Legal responsibilities applicable to different breaches under CSL:**
  - For the breach of any general obligation to protect cybersecurity, including to take organizational and technical measures, such as designating a person in charge of cybersecurity and retaining security logs for no less than six months, the original CSL empowered the enforcing authority to mandate rectification and to issue a warning to the breaching business. If the business failed to comply with the mandate or the breach caused damages upon cybersecurity, the breaching business may have been fined with an amount from RMB 10,000 to RMB 100,000, and the responsible person may have been fined with an amount from RMB 10,000 to RMB 50,000.

    Under the amendments, the enforcing authority may now impose a straight fine on the breaching business with an amount between RMB 10,000 and RMB 50,000 without proving "non-compliance with the mandate to rectify" or "damages upon cybersecurity." If the business fails to comply with the rectification mandate or cybersecurity is proven to be damaged, the range of the fine is increased to an amount between RMB 50,000 and RMB 500,000 for the breaching business and between RMB 10,000 to RMB 100,000 for the responsible person. The amendments also empower the authority to penalize, in certain aggravated circumstances including "leakage of massive data," the breaching business with an increased fine between RMB 500,000 to RMB 2 million, and the responsible person with a fine between RMB 50,000 to RMB 200,000.
  - For the breach of the obligation to stop dissemination of illegal information (including upon the authority's request), the original CSL allowed the enforcing authority to mandate rectification, issue a warning, and forfeit illegal earnings. Under the original law, only in the event that the business failed to comply with the mandate or the breach is with aggravated circumstances (e.g., repeated breaches), may the authority have fined the business with an amount from RMB 100,000 to RMB 500,000. The authority also could have shut down its related business, license, or website, and the person responsible may have been fined an amount from RMB 10,000 to RMB 100,000.

    With the amendments, the enforcing authority may now impose a straight fine on the breaching business with an amount between RMB 50,000 and RMB 500,000 without proving "non-compliance with the mandate to rectify" or "damages upon cybersecurity," and the authority may publish the breach. If the business fails to comply with the mandate or the breach is with aggravated circumstances, the amendments now allow the authority to impose an increased fine on the business from RMB 500,000 to RMB 2 million, and RMB 50,000 to RMB 200,000 for the responsible person. In certain further-aggravated circumstances with "particularly serious consequences," the authority may increase the fine it imposes on the breaching business to RMB 2 million to RMB 10 million, and the authority may increase the fine on the responsible person to RMB 200,000 to RMB 1 million.
  - CSL also obligates providers of cyber products and services to take immediate remedies and to notify users and government authorities if they identify any security defect. It also mandates that businesses not install malware in their product or service, nor cease providing security-related maintenance services without justification. If businesses breach any of the above obligations, the original CSL empowered the authority to mandate rectification and to issue a warning. If the breaching provider failed to comply with the mandate or the authority proved compromised cybersecurity, the provider may have received a fine with an amount between RMB 50,000 and RMB 500,000, and its responsible person may have received a fine with an amount between RMB 10,000 and RMB 100,000. The amendments now further empower the authority to impose an

increased fine — in certain aggravated circumstances including "leakage of massive data" or "partial dysfunction of critical information infrastructure (CII)" — upon the breaching provider with an amount between RMB 500,000 to RMB 2 million, and upon the responsible person with an amount between RMB 50,000 to RMB 200,000. The authority may levy a greater fine of up to RMB 10 million upon the business and up to RMB 1 million upon the responsible person if their conduct causes "extremely serious damages" to cybersecurity, including when the "primary function" of certain CII is disabled due to the provider's breach.

  - The penalties applicable to an operator of CII for similar breaches have also increased.

- **Enforcement against extra-territorial activities jeopardizing China's cybersecurity**

  The amended CSL grants the enforcing authority the ability to launch enforcement actions against any "foreign institution, organization[,] or individual" if they are carrying on activities jeopardizing China's cybersecurity, and to impose sanctions if such activities cause serious damage. Prior to the amendments, the permitted enforcement actions were limited to activities jeopardizing the "critical information infrastructure" within China. The amendments expand the possible actions that China's enforcing authority may launch against persons and entities located outside of China, as "cybersecurity" may be interpreted to cover security related to both infrastructure (e.g., IT systems) within China, and to personal and other sensitive data collected within China, even when parties transfer and store such data outside of China. To date, the authority has not announced any investigations or penalties launched against corporations outside of China.

- **Enshrining Policy and Regulatory Goals for AI Governance**

  The amended CSL for the first time lays down certain policy and regulatory goals for China's AI governance regime, including (a) the state will support the research and development of key AI technologies relating to basic theories and algorithms; (b) the state will push forward construction of infrastructure and facilities relating to data training and computing power; (c) the state will improve regulation of AI ethics, strengthen risk monitoring and assessment, and security supervision; and (d) the state will promote the application and healthy development of AI. With these goals in place, a spur of new AI-related policies and regulations may soon come, both from central and local governments.

Considerations for Stakeholders

The amendments have expanded the responsibilities and penalties for breaches under CSL, and immediate monetary fines may now be possible for even first-time breaches. Multinational companies may wish to review their compliance programs under CSL to confirm that they address any pending compliance actions before the enforcement authority identifies any non-compliance (leading to potential enforcement actions that may follow in 2026). Multinational companies servicing any IT systems of Chinese customers from outside of China may also wish to take a second look at their total exposure under CSL, considering the expanded enforcement power under the amended CSL.

Authors

This GT Advisory was prepared by:

- Philip Ruan | +86 (0) 21.6391.6633 | ruanp@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Andrea C. Maciejewski | +1 303.685.7458 | maciejewskia@gtlaw.com