DS NEWSLETTER CHINA
NEWSLETTER - LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

China's Cybersecurity Law is Changing. Ready or Not?

Cybersecurity Law("*CSL*") has undergone its first revision since its initial implementation in 2017. The amended CSL, published on October 28, 2025, is set to come into force on January 1, 2026. This newsletter provides a Q&A-style overview of the key revisions for your reference.

1. What prompted the revision of the *CSL*?

CSL, enacted in 2016 and effective from 2017, serves as the foundational statute in China's cybersecurity domain. In response to rapid technological advancements, evolving risks, and the introduction of subsequent regulations—such as *the Personal Information Protection Law and Data Security Law in 2021*—this revision focuses on strengthening legal accountability, specifying penalties in greater detail, and enhancing alignment with the broader legal framework.

2. Which revisions are most fundamental and important for most enterprises?

The most critical updates involve the cybersecurity protection obligations under Articles 23 and 27 of the amended *CSL,* which apply to all network operators. These provisions mandate the fulfillment of security duties to safeguard networks from disruption, destruction, or unauthorized access, and to prevent network data leaks, theft, or tampering. Key requirements include:

- Formulating internal security management systems and operating procedures, designating a cybersecurity responsible person, and implementing cybersecurity protection responsibilities;
- Adopting technical measures to prevent cyber threats such as computer viruses, network attacks, and intrusions;
- Implementing technical measures to monitor and record network operational status and cybersecurity incidents, retaining relevant network logs for no less than six months as required;
- Enforcing data classification, important data backup, encryption, and other necessary measures, etc.

Additionally, enterprises are required to formulate cybersecurity contingency plans, promptly address vulnerabilities, and upon occurrence of a cybersecurity incident, immediately activate the contingency plan, take remedial actions, and report to the relevant authorities as required.

While the obligations under Articles 23 and 27 remain unchanged, it is the consequence of non-compliance will become significantly more severe. Specifically, the potential fines for legal persons have substantially increased. Under the current *CSL*, minor violations only require rectification and a warning, which has led some enterprises to adopt a «wait and see» approach—delaying compliance until being inspected. However, under the amended *CSL*, general non-compliance can now result in fines ranging from RMB 10,000 to 50,000, in addition to rectification orders and warnings. This change will compel many enterprises to proactively review and enhance their compliance posture.

Moreover, the scope of penalties for responsible individuals has been expanded. Previously, liability for management personnel was triggered only if the legal person refused to rectify violations or caused harm, with fines ranging from RMB 5,000 to 50,000. The amended *CSL* not only doubles these individual fines to RMB 10,000 to 100,000, but also broadens the scope of punishable individuals to include «other directly responsible personnel.»

Finally, the amended *CSL* significantly raises the maximum fines for violations. For example,

- Critical Information Infrastructure (CII) Operators (CIIOs) that fail to comply with CII cybersecurity protection obligations now face baseline penalties that include fines of RMB 50,000 to 100,000, in addition to rectification orders and warnings.

- In severe cases, maximum fines can reach RMB 10 million for legal entities and RMB 1 million for directly responsible personnel and management, applicable to both general enterprises and CIIOs.

We recommend that enterprises begin by reviewing their cybersecurity compliance against the fundamental obligations outlined in this section and seek professional advice from qualified cybersecurity institutions. It is advisable to aim for completing necessary compliance upgrades—or at least initiating substantive compliance work—before the amended *CSL* takes effect.

For your reference, the legal consequences of violating the aforementioned Article 23 or Article 27 under the newly amended *CSL* are summarized as follows:

Severity of Violation Consequences	Penalties for Legal Persons	Penalties for Liable Individuals
General cases	Rectification order, warning, and may include a fine of RMB 10,000 to 50,000	Not applicable.
Refusal to rectify or causing harmful consequences	Rectification order, warning, and a fine of RMB 50,000 to 500,000	Fines of RMB 10,000 to 100,000 for responsible personnel in charge and directly responsible individuals, respectively
Causing severe consequences such as large-scale data leakage or partial loss of function of CII	Rectification order, warning, and a fine of RMB 500,000 to 2 million	Fines of RMB 50,000 to 200,000 for responsible personnel in charge and directly responsible individuals, respectively
Causing severe consequences such as major loss of function of CII	Rectification order, warning, and a fine of RMB 2 million to 10 million	Fines of RMB 200,000 to 1 million for responsible personnel in charge and directly responsible individuals, respectively

3. Any good news about the amended *CSL*?

While increased fines raise the cost of violations, the amended *CSL* also introduces opportunities for rectification. It emphasizes the principle of proportionality and refines the granularity of penalties, avoiding a one-size-fits-all punitive approach. For example, the newly added Article 73 specifies that if a case meets the circumstances for mitigated, reduced, or exempted penalties under the Administrative Penalty Law—such as voluntarily eliminating risks, promptly correcting issues, causing no harm, or being a minor first-time violation—it may be handled accordingly.

4. What are the specific circumstances for "*mitigated, reduced, or exempted penalties*" under the newly amended CSL?

According to the *Administrative Penalty Law*, penalties may be mitigated, reduced, or exempted under the following circumstances:

- Mitigated or Reduced Penalties may apply where:
  - o The violator voluntarily eliminates or mitigates the harmful consequences of the violation;
  - o The violator assists the administrative authorities in investigating the violation with meritorious performance.
- Exempted Penalties may apply where:
  - o No administrative penalty shall be imposed if the violation is minor, promptly corrected, and has caused no harmful consequences;
  - o Penalties may (though are not guaranteed) be exempted for a first-time violation with minor harm that is promptly corrected;
  - o No penalty shall be imposed if the violator provides sufficient evidence to prove the absence of subjective fault.

In practice, if an enterprise identifies non-compliance during self-assessment, it is advisable to take prompt action to implement improvements.

5. What are the newly amended AI-related provisions in the *CSL*?

The amended *CSL* introduces a new Article 20, which emphasizes improving AI ethics standards, strengthening risk monitoring, assessment, and safety supervision for AI. At the same time, it encourages the use of new technologies such as AI to innovate cybersecurity management methods and enhance the level of cybersecurity protection.

In summary, while AI has seen breakthrough developments in recent years, it is still in its early stages from a long-term perspective. AI, built on data as its body and algorithms as its soul, is deeply embedded in cyberspace. Given that technological advancements are introducing new types of cybersecurity threats, the *CSL* must, at this stage, address the dual role of AI technology as both a "spear" and a "shield" in cybersecurity. On one hand, AI itself is regulated, requiring its development to adhere to the baseline of safety and compliance; on the other hand, AI is regarded as a powerful tool for safeguarding cybersecurity, encouraging all parties to leverage its intelligence to enhance cybersecurity capabilities.

Specifically, this newly added Article 20 marks the first time that China has established legal obligations for AI cybersecurity at law level. It underscores the need for AI systems to comply with cybersecurity requirements. Enterprises whose core business relies on AI should strengthen internal risk monitoring, assessment, and supervision. Relevant companies should prioritize reviewing whether their AI products and operations align with the published AI-related key regulations, such as:

- *Provisions on the Management of Algorithmic Recommendations for Internet Information Services* (effective March 1, 2022)
- *Provisions on the Management of Deep Synthesis for Internet Information Services* (effective January 10, 2023)
- *Interim Measures for the Management of Generative AI Services* (effective August 15, 2023)
- *Measures for the Identification of AI Generated and Synthetic Content* (effective September 1, 2025)

6. What should enterprises do?

At first glance, the amendments to the *CSL* may appear limited in length. However, a closer review reveals that the majority of the revisions focus on penalty provisions. Crucially, a single penalty clause can often correspond to multiple obligation clauses. With more scenarios triggering penalties, lower thresholds for fines, a broader range of accountable management personnel, and increased maximum fines for legal entities, the amended *CSL* ultimately becomes significantly less tolerant.

Consequently, enterprises must re-examine all relevant obligation clauses under the *CSL* – even those seemingly unchanged – as they are now backed by these strengthened penalties. A wait-and-see approach is likely no longer viable. We recommend that enterprises and their management heighten the priority and urgency of cybersecurity compliance, promptly adapting their organizational measures to meet the requirements of the amended *CSL*.

Ending remarks:

The newly amended *CSL* includes other amended provisions concerning areas such as cybersecurity services and product compliance, which are not detailed here due to space constraints. Enterprises are advised to consult professional experts for any specific questions.

For any additional information, please contact:

ZHANG Beibei
Senior associate - Shanghai Office
Zhangbeibei@dsavocats.com

Isabelle DOYON
Avocate - Paris Office
Doyon@dsavocats.com

13 November 2025