Legal 500
Country Comparative Guides 2025

China

Data Protection & Cybersecurity

Contributor

Zhong Lun Law Firm
LLP

Jihong Chen

Partner | chenjihong@zhonglun.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in China.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

China: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The *Cybersecurity Law of the People's Republic of China* (the "CSL"), effective as of June 1, 2017, serves as the cornerstone of China's cybersecurity and data privacy protection legislation. On June 10, 2021, the *Data Security Law of the People's Republic of China* (the "DSL") was enacted, becoming effective as of 1 September 2021. The DSL is the fundamental law in data security landscape, outlining mechanisms for data security, obligations, and liabilities at both the State and data processor levels. Furthermore, the *Personal Information Protection Law of the People's Republic of China* (the "PIPL"), enacted on August 20, 2021, came effective as of November 1, 2021, which embraces the new era of personal information ("PI") protection as well as corporate data protection compliance. Together, the CSL, DSL, and PIPL form the foundation of China's data regulatory framework. Additionally, on December 1, 2022, *the Anti-Telecom and Online Fraud Law of the People's Republic of China* came into force, targeting the illegal use of PI in telecom and online fraud.

In addition to the foregoing fundamental laws, China's cybersecurity and data protection regime is further supported by various supplementary regulations, implementing measures, and standards. Key regulations and rules include:

- *The Cybersecurity Review Measures*
- *The Security Protection Regulations for Critical Information Infrastructure*
- *The Regulations for the Administration of Network Data Security*
- *The Administrative Regulation for Public Security Video Image Information Systems*
- *The Measures for Security Assessment of Data Outbound Transfer*
- *The Measures for the Standard Contract for Outbound Transfer of Personal Information*
- *The Measures for Certification of Personal Information Protection for Outbound Transfer of Personal Information (Draft)*
- *The Announcement on the Implementation of Certification for Personal Information Protection and the Implementing Rules*
- *The Announcement on Carrying out Certification for Data Security Management and the Implementation Rules*
- *The Guiding Opinions on Strengthening the Comprehensive Governance of Algorithms Related to Internet Information Services*
- *The Administrative Provisions on Algorithm Recommendation for Internet Information Services*
- *The Administrative Provisions on Deep Synthesis for Internet Information Services*
- *The Interim Measures for the Administration of Generative Artificial Intelligence Services*
- *The Measures for Labeling AI-Generated or Composed Content*
- *The Measures for Review of Scientific and Technological Ethics (for Trial Implementation)*
- *The Anti-monopoly Guidelines of the Anti-monopoly Commission of the State Council on Platform Economy*
- *The Administrative Measures for the Record-filing of Security Vulnerability Collection Platforms for Network Products*
- *The Regulations on the Protection of Minors Online*
- *The Notice of the Ministry of Industry and Information Technology on the Record-filing of Mobile Internet Apps*
- *The Interim Provisions on Accounting Treatment Related to Enterprise Data Resources*
- *The Provisions on Facilitating and Regulating Cross-border Data Flows*
- *The Administrative Measures for the Compliance Audit of Personal Information Protection*
- *The Administrative Provisions on the Application Security of Facial Recognition Technology*
- *The Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)*

Moreover, various industries are developing specific regulations addressing sectoral data management, such as the *Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation)*, the *Administrative Measures for Data Security of Banking and Insurance Institutions*, and *the Administrative Measures for Data Security in the Field of Natural Resources*, etc.

China's legislations on cybersecurity and data protection establish a number of supervisory mechanisms and impose significant obligations on companies. Non-compliance may lead to a range of legal consequences, including civil liability, administrative sanctions and even criminal liabilities.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Recent years have seen active legislative developments in China regarding the regulation of cross-border data transfer ("CBDT"). Following the official launch of the *Provisions on Facilitating and Regulating Cross-border Data Flows* (the "Cross-border Provisions"), which became effective on March 22, 2024, the Cyberspace Administration of China (the "CAC") published the *Measures for Certification of Personal Information Protection for Outbound Transfer of Personal Information (Draft)* on March 1, 2025. This draft aims to promote the enforcement of a certification mechanism for outbound transfers of PI. In addition, spurred by the *Cross-border Provisions*, several pilot free trade zones in China (such as Beijing and Shanghai) have launched their own negative lists of CBDT and additional facilitation measures. These efforts are expected to be further developed and refined by local administration in pilot free trade zones. (**Further discussed in Question 24**).

To adapt to the new legislations and establish a coherent legal liability system, China has initiated the first amendment procedure of CSL, originally enacted in 2017. On September 12, 2022, the first draft of the CSL amendment was published for public consultation. On 28 March 2025, the second draft amendment of the CSL was released for further public opinions, focusing primarily on the legal liabilities for violations related to general cybersecurity provisions, security protection of Critical Information Infrastructure ("CII"), supply of critical network equipment and specialized cybersecurity products, online information security and PI protection. This amendment is expected to be finalized and come into effect in 2025-2026.

Additionally, the *Regulations for the Administration of Network Data Security* (the "RANDS") were published on September 24, 2024 and become effective as of January 1, 2025. A key impact of RANDS is the clarification of protection measures and legal liabilities of Important Data, which is crucial to the data protection framework based on the data classification and grading mechanism outlined in the DSL and other enforcement of regulations based on data grading mechanism. In order to respond to the practical need, significant progress is anticipated in both the overall standard and sector-specific catalogs for Important Data.

To further regulate the application of facial recognition technology and enhance the protection of facial information, the CAC and the Ministry of Public Security promulgated the *Administrative Provisions on the Application Security of Facial Recognition Technology* (the "Facial Recognition Provisions") on March 13, 2025, with an effective date of June 1, 2025. The Facial Recognition Provisions emphasize the necessity for applying facial recognition technology and processing facial information, and organizations are expected to carefully screen and assess the business needs for processing facial information and ensure its security and compliance.

Besides, lawmakers have been closely monitoring the artificial intelligence ("AI") technology and application. The State Council included the draft AI Law in its legislative plans of both 2023 and 2024. In 2025, the Work Report of the Standing Committee of the National People's Congress indicated that it would enhance research on AI-related legislation. Additionally, the *Measures for Labeling AI-Generated or Composed Content* come into effective as of September 1, 2025, and are expected to have significant implications for service providers, Internet application distribution platforms, and users involved in AI-generated content.

Last but not the least, following the *Opinions of the CPC Central Committee and the State Council on Building a Basic Data System to Better Play the Role of Data Elements* issued in 2022, the National Development and Reform Commission and the National Data Bureau have accelerated the introduction of policies aimed at promoting the development and utilization of data resources. These policies include, but are not limited to, the *Guiding Opinions on Promoting the High-quality Development of the Data Industry*, the *Opinions on Accelerating the Development and Utilization of Public Data Resources*, and the *Opinions on Promoting the Development and Utilization of Corporate Data Resources*. Concurrently, the administration's efforts are underway to construct data infrastructures, establish trustworthy data spaces, and develop national data standards.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Art.34 of the DSL illustrates that "where laws and administrative regulations stipulate that the provision of services relating to data processing is subject to administrative licensing requirements, the service provider shall obtain license(s) in accordance with the law". For protection of Important Data, Article 30 of the DSL emphasizes the obligations of data processors to regularly assess the risks associated with the processing of Important Data and to submit the corresponding reports to the competent authorities.

Art.25 of the DSL also aligns with the export control laws in China, stipulating that "data relating to safeguarding national security and interests or the fulfillment of international obligations of the State which belongs to controlled items is subject to export control laws." According to the *List of Technologies Prohibited or Restricted from Export (2023)*, the export of restricted technologies including certain AI interface technologies, speech synthesis technologies and personalized recommendation technologies requires an export license from the Ministry of Commerce (the "MOFCOM"). Failure to obtain the export license may result in sanctions, including the order to stop illegal activities, confiscation of illegal earnings, fines, or even order to suspend business for rectification in severe cases.

Key registration and filing requirements under the PIPL primarily apply to entities engaged in CBDT activities, which include the filing for the CAC security assessment and registration of the Standard Contract along with the PI protection impact assessment ("PIA") report with the CAC (**further discussed in Question 24 below**). Non-compliance with the PIPL may lead to administrative penalties, civil actions, or even criminal prosecution. It is also noteworthy that, processors processing PI of natural persons in China from overseas for the purpose of offering products or services for natural persons in China, or analyzing or assessing their behaviors, are subject to the PIPL. These overseas entities are required to establish a special agency or appoint a representative within China and register it with the local cyberspace administration.

Certain other filing requirements apply to the Internet information service providers using algorithm recommendation and the AI-generated service providers. Additionally, under the Facial Recognition Provisions, PI processor who store facial information of more than 100,000 individuals is required to file with local cyberspace administration. Failure to comply with these requirements may result in administrative or even criminal liability.

In addition, the CSL sets out the network security multi-level protection scheme ("MLPS") applicable to network operators who build, operate, maintain and use networks within China. For networks with level 2 or above, network operators shall file for records with related public security authorities. Failure to fulfill this requirement can lead to administrative penalties or criminal liability.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

"Personal information" under the PIPL is defined as any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized.[1]
"Sensitive personal information" as defined in Art.28 of the PIPL means PI that, once leaked or illegally used, is likely to cause detriment to the dignity of a natural person or damage to one's personal or property safety, including biometric identification, religious beliefs, specific identities, medical health, financial accounts, whereabouts and tracks as well as the PI of minors under the age of 14. Additionally, the Facial Recognition Provisions provide a definition for "facial information" which refers to the biometric information of facial features, recorded in electronic or other forms, and is associated with an identified or identifiable natural person, excluding the anonymized information.

The PIPL also sets out the following key definitions:

"Processing": includes collection, storage, use, processing, transmission, provision, disclosure and deletion of PI.[2]

"Personal information processor": means any organization or individual that independently determines the purposes and methods of processing in their PI

processing activities, which is substantially equivalent to the concept of "controller" under the GDPR.[3] The PIPL also introduces the notion of "Processor of small-scale PI"[4]. It is expected that competent authorities, including the CAC, may issue specific PI protection rules soon for further clarification.

"De-identification": refers to the process in which PI is processed so that it is impossible to identify certain natural persons without the aid of additional information.[5]

"Anonymization" refers to the process by which PI is processed so that identification of certain natural person is impossible and that it cannot be recovered.[6] Anonymized information is not considered as PI under the PIPL.

In addition, "Personal information subject" is defined as the natural person identified by or associated with the PI according to the *Standard Contract for Outbound Transfer of Personal Information* issued by the CAC.

Footnote(s):

[1] Personal Information Protection Law of the People's Republic of China, Art.4.

[2] *Ibid.*

[3] Personal Information Protection Law of the People's Republic of China, Art.73.

[4] Personal Information Protection Law of the People's Republic of China, Art.62(2).

[5] Personal Information Protection Law of the People's Republic of China, Art.73.

[6] *Ibid.*

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

The PIPL outlines a set of comprehensive principles for PI processing, which shall be adhered to throughout the entire lifecycle of PI processing activities. The PIPL and GDPR are quite alike with respect to PI processing principles. Key principles include:

PIPL	GDPR (Art.5)
Lawfulness, legitimacy, necessity and good faith (Art.5)	Lawfulness, fairness and transparency
Purpose limitation (Art.6)	Purpose limitation
Data minimization (Art.6)	Data minimization
Transparency (Art.7)	Lawfulness, fairness and transparency
PI quality (Art.8)	Accuracy
Accountability (Art.9)	Accountability
Data security (Art.9)	Integrity and confidentiality
/[7]	Storage limitation

Chart 1. Principles (PIPL v. GDPR)

Under the PIPL, PI can only be processed when a valid legal basis is met. For the principle of privacy, the PIPL requires the PI processors to inform the individuals (PI subjects) of[8]: (1) the name and contact information for PI processors; (2) the purpose, method of processing, and the type of processed PI; (3) the retention period of PI and disposal method upon expiration; (4) the method and procedure of exercising rights by individuals in relation to their PI. If processing sensitive PI, providing PI to other PI processors, or providing PI overseas, additional information shall be provided to the PI subjects.

In line with data minimization principle, PI shall be kept for the minimum period necessary for achieving the purpose of processing, unless as otherwise required by laws or administrative regulations.

Footnote(s):

[7] Though the PIPL, as opposed to the GDPR, does not include storage limitation in the principles relating to PI processing, it specifies in its Art.19 that PI shall be kept for the minimum period necessary for achieving the purpose of processing, unless as otherwise stipulated by laws and administrative regulations.

[8] Personal Information Protection Law of the People's Republic of China, Art.17; Regulations for the Administration of Network Data Security, Art.21.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Under Art.13 of the PIPL, there are seven legal bases for PI processing[9], with "consent" and "necessity for the performance of a contract or for human resource

management" being the most commonly used in business contexts involving PI processing. In general, consent is typically required where the PI processing is not solely intended for providing services and products and no other legal bases apply. For example, consent is normally required for targeting advertising and promotional marketing purposes.

The PIPL also stipulates that "separate consent" is required for certain processing activities, including the provision of PI to other PI processors, provision of PI to an overseas party, disclosure of PI, and processing of sensitive PI, etc. Notably, the *Standard Contract for Outbound Transfer of Personal Information* further clarified that the "separate consent" requirement for provision of PI to an overseas party only applies to the PI processing activities taking "consent" as legal basis, shedding some light on the relationship between "separate consent" and other legal bases under PIPL.

Art. 14 and 15 of the PIPL set out the conditions for valid consent are fully informed, freely given, explicit and easy to withdraw. Where PI processing activities are based on consent, individuals have the right to withdraw their consent, and the PI processors shall provide a convenient channel for the withdrawal. The effectiveness of any PI processing activities prior the withdrawal will not be affected.[10] It's prohibited for mandatory tying of the consent of individuals to the provisions of services or products[11], for example an online shopping APPs shall not deny its basic services to consumers who refuse to grant its microphone permission which is not deemed as necessary for the provision of the online shopping services. Further, Art.22 of the RANDS also provides detailed requirements for consent. For instance, consent shall not be frequently asked for after an individual has explicitly rejected the processing of his/her PI.

To fulfill the obligation of obtaining the "separate consent", PI processors shall at least ensure that individuals are allowed to give consent to certain processing activities separately rather than to granting consent in a bundle.

Footnote(s):

[9] The seven legal bases are: Consent; Necessary for the performance of a contract or for human resource management; Necessary for the performance of statutory obligations; Vital interests under public health incidents or emergencies; Public interests; Utilization of public PI; Otherwise prescribed by laws and administrative regulations.

[10] Personal Information Protection Law of the People's Republic of China, Art.15.

[11] Personal Information Protection Law of the People's Republic of China, Art.16.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Under Art.28 of the PIPL, sensitive PI includes PI about biometric identification, religious beliefs, specific identities, medical health, financial accounts, whereabouts and tracks as well as PI of minors under the age of 14. Sensitive PI can only be processed with specific purpose(s) and necessity and strict protection measures shall be adopted. Processing sensitive PI necessitates enhanced transparency and the obtaining of separate consent.

PI processors shall, in addition to the disclosure matters stipulated in Art.17, inform individuals of the necessity of processing their sensitive PI and the impact on their personal rights and interests, unless otherwise provided by law.[12] separate consent requirement is required for processing sensitive PI[13], but only when the consent is the legal basis for processing (**discussed in Question 6 above**). Furthermore, PIA is required for processing sensitive PI, and the PIA report and related documentation shall be kept for at least three years.[14] Besides, specialized rules shall be formulated when processing the PI of minors under the age of 14. It is recommended that companies implement stringent technical and organizational safeguards for sensitive PI protection based on data classification and grading mechanism, and remain vigilant to any legislative developments, enforcement trends and industrial practices.

In China, certain types of data are subject to specific prohibitions or restrictions based on the processing activity or the entity involved. For example, human genetic resource information which refers to information materials such as data generated from human genetic resource materials, is subject to stringent controls. When it is provided or offered open access to foreign organizations, individuals and the institutions established or actually controlled thereby, it shall be filed for record with the administrative department of science and technology and submit such information for backup, in

accordance with the *Administrative Regulations on Human Genetic Resources*. Further details on the management of human genetic resources information are provided in the *Implementing Rules of the Regulations for the Management of Human Genetic Resources* promulgated in 2023. For another example, credit investigation organizations are prohibited from collecting PI related to religion, gene, fingerprints, blood type, diseases and medical history, etc. according to the Art.14 of the *Administrative Regulations on Credit Investigation Industry*.

Footnote(s):

[12] Personal Information Protection Law of the People's Republic of China, Art. 30.

[13] Personal Information Protection Law of the People's Republic of China, Art. 29.

[14] Personal Information Protection Law of the People's Republic of China, Art. 55, Art. 46.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The PIPL and RANDS do not apply to the processing of PI by a natural person for his or her personal or family affairs. Where there are legal provisions on the processing of PI in the statistical and archive administration organized and implemented by the people's governments at all levels and relevant departments thereof, such provisions shall prevail.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

1) PIA. Under Art.55 of the PIPL, PI processor shall conduct a PI protection impact assessment ("PIA") prior to the processing in the following circumstances:

- Processing sensitive PI;
- Use of PI for automatic decision-making;
- Entrusted processing, provision of PI to other PI processors, public disclosure of PI;
- PI cross-border transfer; or
- Other PI processing activities that have significant impact on rights and interests of individuals.

The PIA must address[15]:

- Whether the purpose and method of processing activities are lawful, legitimate, and necessary;
- Impact on rights and interests of individuals and security risks; and
- Whether the protection measures taken are lawful, effective and commensurate with the degree of risks.

If the PIA is triggered by processing facial information by applying facial recognition technology, the content of PIA shall additionally include the risks of breach, tampering, loss, damage, or illegal acquisition, sale or use of facial information and possible harm according to Art. 9 of the Facial Recognition Provisions.

PIA report and related documentation shall be kept for at least three years. In cross-border PI transfers applicable to Standard Contract, the PIA report shall be filed with cyberspace administration jointly with the effective Standard Contract.

2) PI protection compliance audits. According to Art.54 of the PIPL, PI processors shall regularly conduct compliance audits on their PI processing activities. Accordingly, the *Administrative Measures for the Compliance Audit of Personal Information Protection* (the "Audits Measures") launched by the CAC, effective as of May 1, 2025, further specify that, PI processors processing PI of more than 10 million individuals shall conduct the audit at least once every two years[16], while no compulsory frequency requirement is clearly imposed on other processors. PI processors may conduct the audit themselves or entrust a professional organization. In certain cases, such as significant security risk or harming the rights and interests of individuals in PI processing activities, the regulatory authorities may require the PI processor to entrust a professional organization to conduct the audit[17]. Audits shall refer to the audit guidance officially attached to the Audits Measures[18]. In addition, the draft national standard *Data security technology — Personal Information Protection Compliance Audit Requirements* is worthy to keep tuned to for conducting the audits.

3) CAC security assessment for CBDT[19]. The CSL, the DSL and the PIPL altogether outlined the comprehensive CBDT regulation framework in China. PI and Important Data[20] generated and collected within China during operation by Critical Information Infrastructure Operators ("CIIOs")[21] as well as PI generated and collected by PI processors within China reaching the threshold[22]

stipulated by the CAC shall be stored in China, and when truly necessary to be transferred outside the territory of China, it shall pass the CAC security assessment (**further discussed in Question 24**).

4) Filing of Standard Contract and PIA report for CBDT. PIA is required before providing PI to overseas party, and if the provision is subject to the Standard Contract, such PIA report shall be filing with the cyberspace administration together with the Standard Contract within 10 working days after the Standard Contract entering into effect.[23] PIA in such scenario shall focus on:

- The legality, legitimacy and necessity of the purpose, scope and method of the processing PI by the PI processor and the overseas recipient;
- The scale, scope, type, and sensitivity of PI to be transferred abroad, and the risks to the PI rights and interests that may be caused by the outbound transfer of PI;
- The obligations that the overseas recipient promises to undertake, and whether the management and technical measures and capabilities of the overseas recipient to perform the obligations can ensure the security of the PI to be transferred abroad;
- The risk of tampering, destruction, leakage, loss and illegal use after outbound transfer of PI, and whether the channels for individuals to exercise their PI rights and interests are accessible and smooth;
- The impact of policies and regulations for the protection of PI on the performance of the Standard Contract in the country or region where the overseas recipient is located;
- Other factors that may affect the security of outbound transfer of PI. [24]

5) Cybersecurity Review. *The Cybersecurity Review Measures (2021)*, released in accordance with the CSL and DSL, is of great importance to implementing the cybersecurity review mechanism. The triggering conditions include:

- Mandatory filing requirements:
  - Purchasing of network products or services by CIIOs which affects or may affect national security;[25]
  - Network platform operators with over 1 million user PI going public listing abroad;[26]
- Ex officio initiation by the CAC cybersecurity review office:
  - Network products or services or data processing activities which affects or may affect national security.

The key considerations of the cybersecurity review include "risks of influence, control or malicious use of CII, Core Data, Important Data or large amounts of PI by foreign governments after listing abroad", "risks of theft, disclosure, damage, illegal use or cross-border transfer of Core Data, Important Data or large amounts of PI", etc. The review progress could take one to six months.

Footnote(s):

[15] Personal Information Protection Law of the People's Republic of China, Art. 56.

[16] The Administrative Measures for the Compliance Audit of Personal Information Protection, Art.4.

[17] The Administrative Measures for the Compliance Audit of Personal Information Protection, Art.5.

[18] The Administrative Measures for the Compliance Audit of Personal Information Protection, Art.6.

[19] It shall be noted that regulation with respect to data cross-border transfer still requires further supplemental measures and clarification by the competent authorities, companies shall keep tuned to any legislative developments, enforcements trends and industrial practices.

[20] "Important Data" is a proper noun in China cybersecurity and data protection legal regime. With respect to the Regulations for the Administration of Network Data Security, "Important Data" means data in a specific field, group or area or with a certain precision and scale, which, once tampered with, destroyed, leaked, illegally obtained or illegally used, may directly endanger national security, economic operation, society stability, public health and security.

[21] The Security Protection Regulations for Critical Information Infrastructure, Art.2.

[22] With reference to the Measures for Security Assessment of Data Cross-border Transfer by the CAC effective as of September 1, 2022, "Where PI processors with over 1 million users transfers PII overseas; or where PI of more than 100,000 people or sensitive PI of more than 10,000 people are transferred overseas accumulatively since January 1 in the last year, PI processor will be subject to localization requirement and will need to go through the CAC security assessment."

[23] The Measures for the Standard Contract for Outbound Transfer of Personal Information, Art. 7

[24] The Measures for the Standard Contract for Outbound Transfer of Personal Information, Art. 5

[25] The Cybersecurity Review Measures (2021), Art. 5.

[26] Public listing at HK SAR does not trigger mandatory filing of the cybersecurity review under the Cybersecurity Review Measures (2021), though competent authorities may initiate the review process if it's deemed as would affect or may affect national security.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

In China, specific requirements for personal information processing are outlined in various supporting regulatory documents, including the *Regulations on the Protection of Minors Online*, the *Provisions on the Cyber Protection of Children's Personal Information*, and the *Provisions on Facial Recognition Technology Application*. Additionally, national standards, was well as cybersecurity standard guidelines issued by the National Technical Committee 260 on Cybersecurity of Standardization Administration of China ("TC260"), address particular data processing activities. Examples include the draft national standard *Information security technology — Security requirements for processing of sensitive personal information*, and the *TC260-PG-20251A Cybersecurity Standard Guideline – Requirements for the security protection of personal information in facial recognition payment scenarios*.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

The CSL requires that network operators shall maintain records of network operation statuses and any security incidents, with related worklogs being kept for at least six months.[27] Failure to comply with this requirement may lead to rectification order(s) and/or warning(s), administrative fines or even suspension, termination of related businesses or revocation of related business licenses.[28]

The PIPL stipulates that PI processors shall keep the PIA report and related documentation for at least three years (**PIA is further discussed in Question 9**). Art. 12 of RANDS further specifies that records of processing activities of PI and Important Data provided or entrusted to other processors shall be kept for at least three years.

GB/T 35273—2020 Information security technology — Personal information security specification (the "PI Security Specification") recommends PI processors to establish, maintain and update records of processing activities. Such records may include:

- Type, volume and source of the PI involved;
- Purpose(s), business scenarios for PI processing activities, whether involving any entrusted processing, joint processing, provision of PI to other third parties, PI cross-border transfer, etc.;
- information systems, organizations or personnel related to all aspects of PI processing activities.

Footnote(s):

[27] Cybersecurity Law of the People's Republic of China, Art.21 (3).

[28] Cybersecurity Law of the People's Republic of China, Art.64.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Art.19 of the PIPL states that the retention period of PI shall be the minimum period necessary to achieve the purpose of processing, unless otherwise stipulated by laws and administrative regulations.

Art.47 of the PIPL outlines the circumstances under which PI shall be deleted by the processor or upon request by the PI subject:

- Where the purpose of processing has been achieved or it is impossible to achieve such purpose, or it is no longer necessary to achieve such purpose;
- Where the PI processor ceases to provide products or services, or the retention period has expired;
- Where the individual withdraws his/her consent;
- Where the processing of PI is in violation of laws, administrative regulations or any agreements; or
- Other circumstances stipulated by laws and administrative regulations.

Art.47 also specifies that, in cases where it is technically impossible to delete PI, the PI processors shall stop any processing except for the purposes of storage and

necessary security protection measures. In such cases, companies shall ensure that the PI at question is effectively protected, for example, through data segregation or tagging, and shall refrain from further processing the PI.

Art.21 of the RANDS further requires that PI processors inform PI subjects of the method used to determine the retention period if it is difficult to specify a period. Additionally, Art.24 sets out that, where it is impossible to avoid collecting unnecessary PI or collecting an individual's PI without obtaining his/her consent according to the laws through automatic collection technology, or if an individual deregisters his/her account, the processors shall delete or anonymize the PI. Where the retention period provided by laws and administrative regulations has not expired or it is technically difficult to delete or anonymize the PI, the processors shall stop the processing except for storage and necessary security measures.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Unlike the GDPR, the PIPL sets no mandatory prior consultation requirement, neither the CSL, the DSL nor related administrative regulations. However, in practice, companies may carry out prior consultations or enquires with competent authorities as regards for example specifics concerning the cybersecurity review or licensing requirements for certain data processing activities. This is typically done to streamline compliance efforts and ensure alignment with regulatory expectations.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

The PIPL and the DSL set out various requirements for appointment of responsible persons in charge of PI protection and Important Data security.

1. **Responsible person for PI protection** (analogous to the role of "DPO" in the GDPR) is not required for all PI processors. However, according to Art.52 of the PIPL and Art.12 of Audits Measures, PI processors processing PI of more than 1 million individuals shall appoint a person in charge of PI protection to be responsible for overseeing PI processing activities, implementing protection measures, and compliance audits, etc. PI processors shall make public the contact details of this person and submit the name, contact information, etc. of this person to competent authorities.
2. **Responsible person for data security.** 27 of the DSL states that processors of Important Data shall specify the person(s) responsible for data security and the management body to implement the responsibilities of data security protection**.** According to the RANDS Art.30, the responsible person(s) shall possess professional knowledge of data security and relevant management experience, and shall be a member of the management team of the data processor, having the right to directly report the data security situation to the relevant competent authority.
3. **Responsible person for automotive data security management and a User Rights Affairs Contact.** In the field of automotive data regulation, Art. 13 of the *Several Provisions on Automotive Data Security Management (for Trial Implementation)* requires the automotive data processors processing Important Data to report the information regarding their automotive data security management annually to the local cyberspace administration. This annual report must include the name and contact details of the responsible person for automotive data security management and a User Rights Affairs Contact, which means that the automotive data processor processing Important Data shall appoint these two roles to comply with regulatory requirements.

In practice, it is common in practice for companies to appoint IT lead or person responsible for information security as the above responsible persons based on their governance/organization and considerations. Some companies may also opt to establish a committee rather than appointing a specific person to hold those roles. Person(s) in these positions may be subject to administrative liability or even criminal liability under the law. Failure to comply with the law and related data protection obligations could lead to administrative fines on the major responsible person directly in charge, which may refer to the responsible person(s) as illustrated above.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

Employee training on data protection is a general obligation under Chinese data protection laws. Art. 27 of the DSL stipulates that companies engaged in data processing activities are obliged to conduct data security education and training to ensure data security. Failure to meet this obligation could lead to rectification orders, warnings, administrative fines of up to 2 million RMB for company, and fines of up to 200,000 RMB for the responsible person directly in charge, even suspension or termination of related business operations, revocation of related business licenses and permits.[29] Art.30 of the RANDS also stipulates that the management body responsible for network data security shall regularly organize education activities about network data security.

Specifically, the PIPL stipulates the obligation of regular employee education and training for PI security and protection in its Art.51.[30] Companies are recommended to refer to Items 19 & 21 of the audit guidance attached to the Audits Measures, which suggest that PI processors establish and implement a security education and training program on PI protection tailored to their management personnel, technical personnel, operators and all employees, and an assessment of the awareness and skills of relevant personnel for PI protection is also recommended. Moreover, the training content, method, object and frequency are recommended be designed to meet the needs of PI Protection.

Footnote(s):

[29] Data Security Law of the People's Republic of China, Art.47.

[30] GB/T 35273—2020 Information security technology — Personal information security specification, Art.11.6 (f) recommends that PI training shall be carried out at least once a year or when there is any major change in the PI protection policy.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Art.7 and Art.17 (information to be provided) lay down the transparency fundamentals under the PIPL. Such requirements are generally implemented through companies' privacy policies. Art.17 stresses that, before processing any PI of an individual, the processors shall provide the individual with clear, accurate, and complete information about the processing activities. This means that companies shall avoid vague wordings of "etc." and "such as" in their privacy policy and relevant documents. The information provided shall cover all items required under Art.17.

Moreover, the PIPL sets forth additional disclosure requirements for specific scenarios, such as when PI is provided to third parties[31], when sensitive PI is processed[32] or when PI is cross-border transferred.[33] Furthermore, Art.21 of the RANDS further specifies that the rules for processing PI shall be displayed in centralized and public manner that is easily accessible and put in eye-catching position. The content shall be clear, specific and understandable. Privacy policy shall be delivered to each individual in a noticeable way, such as through a tick box or a pop-up window on the account registration page, before any PI is collected. Additionally, the privacy policy shall be easily accessible. Companies may consider placing their privacy policies on their website homepages, APPs user setting sections, etc.

Footnote(s):

[31] Personal Information Protection Law of the People's Republic of China, Art. 23.

[32] Personal Information Protection Law of the People's Republic of China, Art. 30.

[33] Personal Information Protection Law of the People's Republic of China, Art. 39.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

The PIPL defines "PI processor" (substantially equivalent to the concept of "controller" under the GDPR) as any organization or individual that independently determines the purpose and method of processing in their PI processing activities. On the other hand, entrusted parties are those conducting PI processing activities on behalf of a PI processors and strictly in accordance with the instructions provided by the PI processor.

According to the PIPL, PI processors are held accountable for their processing activities and shall ensure compliance with the law.[34] Yet Art.59 of the PIPL specifies that the entrusted parties are obliged to take necessary measures, in accordance with the laws and

relevant administrative regulations, to ensure the security of the processed PI and assist the PI processor in fulfilling its obligations under the PIPL.

Art.21 of the PIPL outlines the contractual requirement for PI processors and the entrusted parties. It mandates that where a PI processor entrusts another party with PI processing, it shall agree with the entrusted party on the purpose, duration and method of the entrusted processing, type of PI, protection measures, as well as respective rights and obligations of both parties.

The entrusted party shall process PI as agreed upon and shall not process it beyond the agreed purpose and method. If the entrustment contract becomes ineffective, invalid, revoked or terminated, the entrusted party shall return the PI to the PI processor or delete it, and shall not retain it. Additionally, the entrusted party shall not subcontract any processing without prior consent of the PI processor.

The PI processor is also obliged to conduct a PIA[35] and oversee the activities of the entrusted party to ensure that the entrusted party has the necessary data security capabilities and complies with legal requirements.

Footnote(s):

[34] Personal Information Protection Law of the People's Republic of China, Art. 10.

[35] Personal Information Protection Law of the People's Republic of China, Art. 55.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Under Art. 24 of the PIPL, automated decision making shall be transparent and fair. Data subjects are entitled to request an explanation and to refuse the decision having a significant impact on its rights and interests. In addition, when automated decision-making is used for commercial advertising or pushing notices, a non-personalized option or a convenient method to refuse such personalization shall be provided to data subjects.

Art. 42 of the RANDS further specifies that, for network platform service providers pushing notices to individuals by automated decision-making, the option to disable personalized recommendation shall be easy to understand, access and operate. The network platform service providers shall provide users with functions to refuse to receive pushed information and delete user tags targeted at their personal characteristics. Automated decision-making, including algorithm recommendation technologies, has become a focus of regulatory scrutiny in China.

Under the CSL and the PIPL regime, tracking technologies such as cookies are not prohibited. However, data collected through cookies (such as web browsing records, click records, and favorites) is considered as PI and is therefore subject to data protection laws. Combined with the legal requirements and good industrial practice, companies shall inform individuals of the use of cookies (particularly if third-party cookies are involved) for example through cookie policies, obtain prior consent, especially for the use of targeting or advertising cookies, and provide an opt-out mechanism that is as convenient as its way for granting consent.

It is also important to consider the governance of Software Development Kits ("SDKs"), which are widely used in APPs development. SDKs are also subject to data protection laws in China when they involve PI processing by embedding in APPs. The Ministry of Industry and Information Technology ("MIIT") has set forth requirements for SDK operators, including the obligation to provide rules for PI processing and to ensure that PI processing activities are carried out lawfully. APP operators are responsible to manage the use of SDKs within their APPs, including assessing the PI protection capability of the SDKs, displaying the names, functions, and PI processing rules of embedded SDKs in a centralized manner, and ensuring that this information is updated timely.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

Behavioral advertising, which is largely based on profiling and targeted analysis of PI collected from users, is subject to both PI protection laws and advertising regulations (**further discussed in Question 21 below**). PI shall not be collected or used for behavioral advertising unless the data subjects have provided explicit consent. Under Art. 24 of the PIPL, if business marketing or information push is conducted towards an individual through automated decision-making (**automated decision making is also discussed above in Question 18**), an option not targeting the characteristics of the individual, or an easy way to refuse to receive this, shall be provided to the individual. Also, with reference to the PI Security Specification, where targeted profiling is used for

behavioral advertising, such profiling shall avoid labels including obscene, violence, discrimination against nations, ethnic and religions, etc.[36]

With respect to any sharing of PI with business partners and third parties involved in cross-contextual behavioral advertising, companies shall adhere to the rules of the PIPL. This includes the requirements to conclude data processing agreements to determine the scope of the PI processing as well as respective rights and obligations of each party. The receiving parties shall ensure the legality of the PI transferred. If any PI collected and generated within China is being provided to individuals or organizations outside the territory of China, related cross-border transfer rules shall be followed. (**Regulation of PI cross-border transfer is further discussed in Question 24**).

Footnote(s):

[36] GB/T 35273—2020 Information security technology — Personal information security specification, Art.7.4.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

Art.44 of the CSL stipulates that no individual or organization shall unlawfully sell or provide any PI to others. The illegal sale of PI could lead to confiscation of illegal earnings by public security authorities and a concurrent fine equivalent to more than 1 but less than 10 times the illegal earnings, or a fine less than 1 million yuan if there are no illegal earnings. Such behaviors may also constitute a criminal offense.[37]

The Criminal Law of the People's Republic of China (2023), in its Art.253, stipulates the "Crime of Infringement upon Citizens' Personal Information", which includes the following circumstances[38]:

- 50 pieces or more of location information, communication information or property information;
- 500 pieces or more of accommodation information, health information or other information that may have an impact on citizens' health or property security;
- 5,000 pieces or more of other PI
- Illegal income is over 5,000 yuan.

Those convicted of the "Crime of Infringement upon Citizens' Personal Information" may face imprisonment for up to three years or criminal detention and may also be fined or only be fined. In particularly serious cases, offenders may be sentenced to imprisonment for more than three years but not more than seven years and may also be fined.

Despite the emphasis on promoting the development and utilization of data resources in China, relevant authorities still emphasize the legality and security of PI transactions. For example, the *Implementation Plan for Improving Data Circulation Security Governance and Better Promoting the Market-oriented Valuation of Data Elements*, issued by the National Development and Reform Commission and other authorities, explicitly states that the circulation of PI shall be based on obtaining individual consent in accordance with laws and regulations, or through anonymization processes.

Footnote(s):

[37] Cybersecurity Law of the People's Republic of China, Art.64.

[38] Interpretation of Supreme People's Court and Supreme People's Procuratorate on Several Issues regarding Application of Law in Processing of Criminal Cases Involving Infringement of Citizen's Personal Information, Art.5.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

The Advertising Law of the People's Republic of China (2021) is the fundamental law that regulates advertising activities. Other key applicable laws and regulations include the *Measures for Administration of Internet Advertising* which came into effect on May 1, 2023 and the *Provisions on the Administration of Text Message and Voice Call Services (Draft for Comment)* released by the MIIT in August 2020.

"Internet Advertising" refers to commercial advertisements that directly or indirectly promote goods or services through websites, web pages, Internet applications and other Internet media, using formats such as texts, pictures, audios, videos, etc.[39]

Before sending any adverts, companies shall obtain the recipients' consent to, or request for, such advertisement, and shall also disclose their true identity, contact details and the opt-out method for receiving advertisements sent via electronic means.[40] Adverts publishing and posting through the Internet shall not affect users' normal use of network. Advertisements published in the form of pop-up

window on the Internet shall prominently indicate the close sign and ensure one-click closing of the window.[41] The PI Security Specification also recommends avoiding using direct profiling that can identify specific individuals for direct marketing purposes,[42] and that PI processors shall ensure that the data subjects have the right to refuse receiving commercial advertisements based on his/her PI.[43]

Footnote(s):

[39] Measures for Administration of Internet Advertising, Art.2.

[40] Advertising Law of the People's Republic of China (2021), Art.43.

[41] Advertising Law of the People's Republic of China (2021), Art.44.

[42] GB/T 35273—2020 Information security technology — Personal information security specification, Art.7.4 (c).

[43] GB/T 35273—2020 Information security technology — Personal information security specification, Art. 8.4(b).

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

Biometric information includes personal genes, fingerprints, voice prints, palm prints, auricles, iris, facial recognition features, etc.[44] Biometric information is classified as sensitive PI and is subject stringent protection measures, including special transparency and separate consent requirements (**special requirements for sensitive PI discussed under Question 6**). Great reference can be made to the PI Security Specification and the *GB/T 40660-2021 Information security technology–Basic requirements of biometric data* for further guidance for biometric information protection.

With respect to the facial recognition technology application, the judicial interpretation issued by the Supreme People's Court in August 2021 clarifies that processing of facial recognition information shall be sufficiently necessary; PI processors shall obtain the consent of an individual for processing his/her facial recognition information, unless such processing is necessary for providing products or services.[45]

At the administrative regulation level, the Facial Recognition Provisions impose further limitations on the processing of facial information. The Facial Recognition Provisions specify that facial recognition technology shall not be used as the sole verification method if there are alternative non-facial recognition methods that can achieve the same purpose or meet the same business needs. When an individual refuses to verify their identity via facial recognition, other reasonable and convenient alternatives shall be provided.[46] Additionally, unless stipulated by laws or administrative regulations or with the individual's separate consent, facial information shall be stored locally on facial recognition equipment and shall not be externally transmitted over the Internet.[47] The *F*acial Recognition Provisions also impose a filing obligation on processors storing facial information of more than 100,000 individuals.[48] Furthermore, TC260 has released specific guidelines (TC260-PG-20251A) addressing the protection of facial information in facial recognition payment scenario.

Footnote(s):

[44] GB/T 35273—2020 Information security technology — Personal information security specification, Annex B.

[45] Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information, Art.4.

[46] The Administrative Provisions on the Application Security of Facial Recognition Technology, Art. 10.

[47] The Administrative Provisions on the Application Security of Facial Recognition Technology, Art. 8.

[48] The Administrative Provisions on the Application Security of Facial Recognition Technology, Art. 15.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

In 2023, a regulatory framework for AI has been systematically established and implemented, which mainly includes the *Interim Measures for the Administration of Generative Artificial Intelligence Services* (the "AIGC Measures"), which came into effect on August 15, 2023, and the *Circular on Releasing the Measures for Review of Scientific and Technological Ethics (for Trial Implementation)*, which took effect on December 1, 2023.

The AIGC Measures expressly outline the regulatory framework for generative AI, covering various stages such as application deployment, model training and

optimization, as well as the roles of content producers, service providers and service users. On February 29, 2024, TC260 released *TC260-0003 Basic Security Requirements for Generative Artificial Intelligence Services*, providing basic requirements and guidelines for assessing the security of AI generated content. Additional rules addressing various aspects of AI governance have been successively developed, including:

- **Content labeling requirement:** In line with the AIGC Measures and other provisions, the CAC and other authorities launched the *Measures for Labeling AI-Generated or Composed Content* (the "Labeling Measures") on March 7, 2025, effective as of 1 September 2025. The Labeling Measures clarify the obligations of generation or synthesis services providers, users, Internet application distribution platforms, internet information content dissemination service providers to ensure effective content security management through labeling. The Labeling Measures require both explicit labels to be added to the content and implicit labels embedded in the file metadata. The Labeling Measures are also equipped with a compulsory national standard *GB 45438—2025 Cybersecurity technology—Labeling method for content generated by artificial intelligence*, specifying the labeling methods various types of AI-generated content, such as text, image, and video, etc.
- **Training data management:** A national standard titled *Cybersecurity technology—Security specification for generative artificial intelligence pre-training and fine-tuning data* was drafted and opened for public comments on April 3, 2024.
- **AIGC services security risk management:** TC260 released a draft cybersecurity standard guideline, *Guidelines for Emergency Response to Security Incidents in Generative Artificial Intelligence Services* on December 18, 2024, to seek for public comments.

Furthermore, the *Circular on Releasing the Measures for Review of Scientific and Technological Ethics (for Trial Implementation)* reflects China's significant focus on the ethical challenges posed by emerging AI technologies.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

PI cross-border transfer is under stringer supervision under Chinese cybersecurity and data protection laws. The PIPL, the CSL and the DSL altogether outline the overall regulation of CBDT in China, along with multiple supplemental regulations, measures, and standards. Chapter III of the PIPL sets the conditions under which PI can be transferred overseas.

- **General requirements:** Companies involved in cross-border transfer of PI shall take necessary measures to ensure that PI processing activities by overseas recipients meet the PI protection standards set out in the PIPL. In practice, such substantial requirement can be fulfilled through contractual arrangements, regular reviews and audits and technical monitoring. Additionally, PI processors shall meet the transparency requirement, providing adequate information about such cross-border transfer activities (e.g., name of the overseas recipient, contact information, purpose and method of processing, type of PI, etc. as required in Art.39 of the PIPL) and conduct PIA before initiating any PI cross-border transfer. The separate consent requirement applies only when the PI was originally processed based on consent (e.g., for targeted advertising purpose).[49]
- **CBDT Mechanisms:** PI processors that outbound transfer PI shall implement one of three CBDT mechanisms outlined in Art. 38 of the PIPL. Specifically:
- **CAC Security Assessment:** The *Measures for Security Assessment of Data Cross-border Transfer* by the CAC, formulated in accordance with the CSL, DSL and the PIPL, took effect as of September 1, 2022, and some of its contents were modified by the Cross-border Provisions. Art. 7 of the Cross-border Provisions explicitly stipulates the mandatory triggering conditions for the CAC security assessment , i.e. where a CIIO provides PI or Important Data (regardless of quantity) overseas; where a non-CIIO data processor provides Important Data overseas; or where a non-CIIO data processor provides PI of more than 1 million individuals (excluding sensitive PI) or sensitive PI of more than 10,000 individuals to overseas since January 1 of the current year. The CAC security assessment normally takes 45 working days or longer in complicated cases or when materials should be corrected and supplemented, and its validity lasts for 3 years.
- **CN Standard Contract:** Where the CAC security assessment is not triggered, Art.38 of the PIPL allows PI processors to enter into contracts with the overseas recipients in accordance with the Standard Contract to be formulated by the CAC (substantially equivalent to SCCs under the GDPR) and filling with the local cyberspace administration. The CN Standard

Contract ("Chinese SCCs") were officially released and became effective on June 1, 2023. It is noteworthy that the Chinese SCCs shall be concluded strictly according to the version published by the CAC, and the CAC may also adjust the Chinese SCCs in light of actual circumstances.

- **Certification:** Conduct PI protection certification by designated institutions is another CDBT mechanism provided by the Art.38 of PIPL, which is voluntary for PI processors to apply if the CAC security assessment is not triggered. The CAC has clarified that, when applying for a certification, PI processors that carry out CBDT activities shall confirm to the *TC260-PG-20222A – Security Certification Specifications for Cross-border Personal Information Processing Activities* to identify the applicable type of certification. In addition, on March 16, 2023, the national standard *Information security technology-Certification requirements for cross-border transfer of personal information (Draft)* (the "Certification Requirements") were published for public comments. As a recommended national standard, the Certification Requirements is not mandatory but may serve as an important reference for enterprises to carry out the Certification. On January 3, 2025, the CAC launched the *Measures for Certification of Personal Information Protection for Outbound Transfer of Personal Information (Draft)*. This draft clarifies that processors processing PI of natural persons in China from overseas under Art.3(2) of the PIPL, may carry out CBDT after obtaining the relevant certification. The certification process shall be assisted and applied for by its specialized agency or designated representative established within China, who will be subject to supervision by the relevant authorities and certification agency.
- **Exempted scenarios:** The *Cross-border Provisions* issued by CAC on March 22, 2024, introduce several exempted scenarios from the CBDT application procedures, which are, CBDT that does not contain PI or Important Data, where data processors transfer PI collected and generated overseas after being processed domestically without involving domestic PI or important data in the process, where CBDT is necessary for the establishment or performance of contracts to which individuals are parties, where CBDT is necessary for implementing cross-border HR management based on legally formulated labor rules and collective contracts, where CBDT is necessary in emergency situations to protect the life, health, and property safety of natural persons, where a non-CIIO data processor provides PI of less than 100,000 individuals (excluding sensitive PI) to overseas since January 1 of the current year. In general, the Cross-border Provisions reflect the trend of stabilizing foreign-investments and promoting economic development, providing positive signals for multinational companies.
- **Local facilitation measures:** 6 of the Cross-border Provisions allows the pilot free trade zones ("FTZs") to independently develop negative lists for CBDT that require regulation within the zone, while those outside the negative lists can be exempted. In this context, FTZs such as those in Shanghai, Beijing, and Zhejiang Province have successively introduced negative lists which are mainly formulated for specific scenarios in specific industries within the FTZs. Beyond delineating the restricted data fields or features, these negative lists have also seen breakthroughs in the thresholds for outbound data volumes generally provided in CBDT mechanisms, thereby further facilitating cross-border data flows. Additionally, for CBDT activities within Guangdong-Hong Kong-Macao Greater Bay Area, there have been great efforts to facilitate the application of CBDT mechanism by applicable processors, including issuing guidance to simplify the Chinese SCCs filing, collaboratively establishing common protection requirements for CBDT with the Office of the Privacy Commissioner for Personal Data of Hong Kong, etc. Companies are recommended to keep tune of these local facilitation measures to seek for a compliant and convenient way of conducting CBDT activities.

Footnote(s):

[49] Companies shall keep tuned to further legislative developments, enforcements trends and industrial practices.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Art.42 of the CSL stresses that network operators shall take technical and other necessary measures to ensure the security of PI they collect, and to protect it from leakage, damage or loss. The DSL elaborates that entities engaged in data processing activities shall establish a data security management system covering entire lifecycle of data processing, and take corresponding technical measures and other necessary measures.[50] Data processors shall also strengthen risk monitoring and take immediate remedies upon any discovery of data security vulnerabilities, bugs or any data incidents.[51]

Art.51 to Art.57 of the PIPL describe the comprehensive obligations of PI processors, requiring companies to set

up internal PI protection management based on PI security. Particularly, Art.51 stipulates that PI processors shall, considering the purpose, method of PI processing, PI categories, impacts on personal rights and interests and possible security risks, take the following measures to ensure PI security:

- Formulating internal management policies and operating procedures;
- Implementing categorized management of PI;
- Taking corresponding technical security measures such as encryption and de-identification;
- Reasonably determining access to PI processing activities, conducting security education and training for relevant employees on a regular basis;
- Formulating and organizing the implementation of emergency plans for PI security incidents; and
- Other measures stipulated by laws and administrative regulations.

Art.9 of the RANDS imposes additional security requirements, obligating network data processors to establish and improve security management system and take technical measures such as encryption, backup, access control and security authentication. These measures shall also include disposal of network data security incidents, preventing illegal and criminal activities aiming at and using network data, and taking primary responsibility for the security of network data they process. Focusing on Important Data protection, Art. 31 of the RANDS requires Important Data processors to conduct risk assessments before providing Important Data to others, entrusting others to process or jointly processing Important Data. These processors shall also conduct annual risk assessment for its network data processing activities and submit the reports to competent authorities.

With reference to the *Guidance on Application of Cross-border Data Transfer Security Assessment (Second version)*, data processors subject to CAC security assessment shall evaluate its data security safeguard capability including both management and technological aspects. The management capability shall cover organization structure, internal policies (including full process management, data classification and grading, emergency response, risk assessment, protection of PI rights and interests), while technological capability shall cover the security measures adopted in the entire data processing lifecycle, including data collection, storage, use, process, transfer, provision, disclosure and deletion, etc. In practice, if a data processor applying for CAC security assessment has not been equipped with the above items, it shall introduce its improvement plan in application materials to CAC. This indicates that such data processors shall fulfill these security obligations to demonstrate their data security capability.

Footnote(s):

[50] Data Security Law of the People's Republic of China, Art.27.

[51] Data Security Law of the People's Republic of China, Art.29.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Art.57 of the PIPL provides that remedial measures shall be taken immediately by PI processors when PI has been or may be leaked, tampered with or loss. These situations are generally referred to as PI security incidents. The Chinese SCCs further categorize several types of PI security incidents, including tampering, destruction, leakage, loss, unauthorized use, unauthorized provision, and unauthorized access. Art.57 of the PIPL further requires that, when PI has been or may be leaked, tampered with or loss, PI processors shall notify the competent authorities and data subjects concerned. The notification shall include the following information:

- Types of PI involved or potentially involved in the leakage, tampering with or loss, the reasons and possible harm from the leakage, tampering with or loss of information;
- Remedial measures taken by the PI processor and measures that data subjects themselves can take to mitigate harms; and
- The contact information of the PI processor.

If the PI processor has taken measures to effectively avoid damages caused by leakage, tampering with or loss of information, it may opt not to notify the individuals concerned; However, if competent authorities believe that damages may be caused, they may require the PI processor to notify data subjects concerned.

27. Do the data protection laws in your jurisdiction establish specific rights for

individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

The PIPL in its Chapter IV grants ten specific rights to data subjects as shown in the chart below. The PIPL incorporates the right to data portability which requires that PI of data subjects to be transferred to other designated PI processors. Art.50 requires PI processors to establish a convenient response mechanism for request of data subjects to exercise his or her rights. If the PI processor refuses such request, it shall explain the reasons and data subjects may file a lawsuit with the People's Court in accordance with laws.

PIPL	GDPR
right to know (Art.44)	information to be provided
right to decide (Art.44)	/
right to restrict (Art.44)	right to restriction of processing
right to refuse (Art.44)	right to object
right to access (Art.45)	right of access
right to copy (Art.45)	right of access
right to data portability (Art.45)	right to data portability
right to rectify (Art.46)	right to rectification
right to delete (Art.47)	right to erasure ('right to be forgotten')
related rights in automated decision making (Art.24)	related rights in automated decision making

Chart 2. Individual privacy rights (PIPL v. GDPR)

Art.49 specifies that, upon the death of a natural person, his or her close relatives may exercise data subject rights such as access, copying, rectification and deletion of the deceased's PI for the purpose of his or her own lawful and legitimate interests as prescribed in the PIPL, unless otherwise arranged by the deceased prior to death.

PI processors shall response to request by data subjects to exercise their rights unless otherwise prescribed by laws and administrative regulations. With reference to the PI Security Specification, related exceptions include[52]:

- In connection with the fulfilment of obligations under laws and regulations by the PI processors;
- Directly related to national security or national defense;
- Directly related to public security, public health or major public interests;
- Directly related to criminal investigations, prosecutions, trials or execution of court decisions;
- For the purpose of safeguarding the life, property or other significant lawful rights and interests of data subjects or other individuals, and it is hard to obtain consent from data subjects;
- PI is proactively disclosed to the public by data subjects;
- PI is collected from legally and publicly disclosed information, such as legal news reports and government information disclosure.

Art. 25 of the RANDS further outlines the conditions for exercising right to data portability. If the request of the individual to transfer its PI meets the following conditions, the network data processor shall provide channels for the processor designated by the individual to access or obtain relevant PI:

- True identity of the person making the request can be verified;
- PI requested for transfer is the PI that the PI subject has agreed to provide or has been collected based on a contract;
- Transfer of PI is technically feasible; and
- Transfer of PI does not damage the legitimate rights and interests of others.

Footnote(s):

[52] GB/T 35273—2020 Information security technology — Personal information security specification, Art. 8.7(e).

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

The Civil Code (effective as of January 2021) specifies that "The personal information of a natural person shall be protected by the law."[53] laying the foundation for PI protection through a dedicated chapter entitled "Privacy Rights and Personal Information Protection". Pursuant to *the Notice of the Supreme People's Court on Issuing the Decision on Amending the Provisions on the Cause of Action on Civil Cases* (December 2020), "dispute relating to personal information protection" has been added as an independent cause of action. Further the PIPL states that "where the PI processor refuses an individual's request for exercising his/her rights, the individual can file a lawsuit with a People's Court in accordance with the law".[54] *The Provisions of Supreme People's Court on Several Issues Concerning the Application of Law to Cases Involving Civil Disputes over Infringement upon Personal Rights and Interests by Using Information Networks (2020 amendment),* effective as of the January

2021, also provides the major legal accordance for private right of action concerning PI protection. The path of private right action over infringements upon personal rights and interests has been actively activated.

Footnote(s):

[53] PRC Civil Code, Art. 1034.

[54] Personal Information Protection Law of the People's Republic of China, Art. 50.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

The liability for damages compensation upon infringements of PI rights and interests shall be determined based on the losses suffered by the individual concerned or the benefits obtained by the PI processor. If the losses suffered by the individual concerned or the benefits obtained by the PI processor are difficult to be determined, the amount of damages shall be determined in accordance with the actual circumstances.[55] If infringement of PI rights and interests causes serious injury of mental health to an individual, such individual is entitled to request compensations for such mental damage.[56]

Footnote(s):

[55] Personal Information Protection Law of the People's Republic of China, Art. 69.

[56] PRC Civil Code, Art. 1183.1.

30. How are data protection laws in your jurisdiction typically enforced?

1) Administrative regulation. Privacy and data protection regulatory enforcement has been tightening.

- **Comprehensive supervision for PI protection.** Various regulatory bodies, including cyberspace, public security, communications and market regulation authorities, have been conducting supervision and enforcement activities from different aspects. These activities typically include receiving complaints, conducting routine inspection, having interviews, providing ongoing guidance and supervision for rectification, and imposing administrative penalties, etc. Penalties are often imposed for issues such as unauthorized collection or misuse of PI and insufficient security measures. Additionally, regulators often launch special enforcement actions focusing on key issues. For example, a local cyberspace administration once launched a special action to address PI protection issues in the consumption sector. On March 28, 2025, the CAC, MIIT, Ministry of Public Security, and State Administration for Market Regulation jointly announced a series of special actions for PI Protection to be carried out in 2025.
- **Cybersecurity review.** The Cybersecurity Review Office of CAC is responsible for organizing cybersecurity review for purchase of network products or services by CIIOs or data processing activities conducted by network platform operators that affects or may affect national security. Several large network platforms in China have undergone cybersecurity reviews and were imposed severe penalties. Besides, network platform operators with over 1 million user PI going public listing abroad shall proactively apply for cybersecurity review, during which the authorities will inspect the compliance and security of their data processing activities.
- **APPs supervision.** Regarding unlawful collection and use of PI by APPs, the CAC, MIIT and competent authorities have conducted continuous inspections, focusing on issues including PI collection and processing beyond the agreed purposes or without prior valid consent, as well as the failure to provide users with an option to withdraw consent. The CAC and other authorities have issued implementing measures including the *Rules*, which are of great reference to regulatory supervision as well as compliance check by
- **Algorithm supervision.** In March 2023, the CAC issued the *Notice on Carrying out the Special Action of QINGLANG- Rectification of Poor Orientation of Short Video Content* and will take the lead in related regulatory work. The CAC requires optimization of algorithm recommendation mechanism of the platform and focus on solving the problem of value orientation deviation of the short video platform's algorithm mechanism. The special action also focuses on correcting the AI generated content short videos, such as using AI to illegally use other people's portraits and voices for face replacement or human voice synthesis. For algorithm filing, the CAC has successively published batches of domestic deep synthesis service algorithm filing information.

2) Public interest litigation. 70 of the PIPL stipulates that "where any PI processor processes PI in violation of this Law, which infringe upon the rights and interests of a large number of individuals, the People's Procuratorate, the consumer organizations specified by law and the organizations determined by the CAC may bring a lawsuit to a people's court in accordance with the law." In August 2021, the Supreme People's Procuratorate issued the *Notice on Implementing the Personal Information Protection Law and Promoting the Procuratorial Work of Public Interest Litigation for Personal Information Protection*, requiring the procuratorate organs to effectively increase case processing and promote the implementation of public interest litigation provisions of the PIPL.

3) Private right of action. The PIPL establishes the principle of presumption of liability, placing the burden of proof on the PI processors.[57] The local courts over the last year have received a number of civil cases concerning the protection of PI rights and interests. (**further discussed above in Question 28**)

4) Criminal charges. The "*Criminal Law Amendment (IX)*" integrates the "Crime of Selling and Illegally Providing Citizens' Personal Information" and "Crime of Illegally Obtaining Citizens' Personal Information" into "Crime of Infringement upon Citizens' Personal Information", expanding the scope of criminal subjects and acts of infringing PI. According to statistics from the Supreme People's Procuratorate of the People's Republic of China, procuratorial organs have prosecuted 2,458 people for infringing the PI of citizens through network in 2024.

Footnote(s):

[57] Personal Information Protection Law of the People's Republic of China, Art. 69.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Data protection laws in China impose a range of sanctions for violations, which includes warnings, rectification orders from competent authorities, confiscation of illegal earnings, administrative penalties, suspension or termination of related businesses, revocation of relevant business permits or licenses, and even criminal liabilities.

Administrative penalties under the PIPL could reach up to 50 million RMB or 5% of the turnover of the previous year on companies and up to 1 million RMB on the responsible person directly in charge and other directly liable persons.[58] Non-compliance with the DSL for example failing to comply with the data cross-border transfer regulation could lead to fines up to 10 million RMB on companies and 1 million RMB on the responsible person directly in charge and other directly liable persons.[59]

Footnote(s):

[58] Personal Information Protection Law of the People's Republic of China, Art. 66.

[59] Data Security Law of the People's Republic of China, Chapter 6.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Competent authorities and judicial departments in China have the discretion in determining the amount of fines on a case-by-case basis, considering factors such as the severity of the violation, the infringement of individuals' legitimate rights and interests, adverse impact on the society, etc. In March 23, 2023, the CAC issued the *Provisions on Administrative Law Enforcement Procedure of Cyberspace Administration*, which set forth the rules that: (1) a same illegal act must not be punished with more than two fines, and where the act violates multiple legal provisions and should be sanctioned with fines, punishment shall be given in accordance with the provision on the high amount of fines; (2) administrative punishments may not be imposed if the violation was first, the harmful consequence was minor, and the illegal act was promptly corrected; administrative punishments may also not be imposed if the violation was minor and corrected in a timely manner, with no harmful consequence caused.[60]

Footnote(s):

[60] Provisions on Administrative Law Enforcement Procedure of Cyberspace Administration, Art.16 & 33.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

A citizen, a legal person or any other organization may first apply to the relevant administrative organ for reconsideration and, if refusing to accept the reconsideration decision, may initiate an action to the people's court. The action may be initiated to the people's

court directly, unless it is required by any relevant laws to exhaust administrative reconsideration before seeking judicial review.[61]

Footnote(s):

[61] Administrative Procedure Law of the People's Republic of China (Amended in 2017), Art.44.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

According to the *Announcement on Launching a Series of Special Actions for Personal Information Protection in 2025* jointly issued by the CAC, MIIT, Ministry of Public Security, and State Administration for Market Regulation on March 28, 2025, the special enforcement actions will focus on 6 issues, focusing on the compliant collection and use of PI by APPs (including mini-programs, official accounts and fast apps), SDKs and smart terminals (including wearable products, home products and learning terminals), the compliant collection and use of facial recognition information in public places, and the compliant collection and use of PI in offline consumption sector, as well as the criminal crimes related to citizens' PI.

The CBDT mechanisms have been equipped with enforcement measures or standards. In view of the elimination of uncertainty in the CBDT regulatory policy with the release of the Cross-border Provisions, the enforcement actions or penalties to be imposed by the cyberspace administration will be closely observed. In addition to administration regulation, private civil action for torts against PI processor involved in illegal outbound transfers of PI have already been seen in judicial practice in China.

AIGC governance is expected to accelerate, especially the implementation of the AIGC Measures and the newly released Labeling Measures. The AIGC service filing mechanism is now operating steadily, with local cyberspace administration actively publishing and updating information on filed AIGC services. Administrative penalties against illegal behaviors of AIGC service providers have already been seen in local inspection.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

In accordance with Art.21 of the CSL, network operators are obliged to protect network and data security based on MLPS to ensure that their networks are free from interference, disruption or unauthorized access. They shall also prevent network data from being disclosed, stolen or tampered with:

- Formulating internal security management policies and operational procedures, and determining the person in charge of cybersecurity to implement accountabilities for cybersecurity;
- Taking technical measures to prevent computer virus, network attacks, network intrusions and other activities that endanger cybersecurity;
- Taking technical measures to monitor and record network operation and cybersecurity events, and maintaining related network logs for no less than six months as required;
- Adopting measures such as data classification, backup and encryption of Important Data, etc.; and
- Performing other obligations required by relevant laws and administrative regulations.

Under CSL, the CIIOs shall take additional measures including regular cybersecurity education, technical training and skill assessment for practitioners, disaster recovery backup of important systems and databases, etc.[62] CIIOs are also required to conduct assessment of its cybersecurity and potential risks at least once a year and submit the results and improvement measures to competent authorities.[63]

The CSL also places responsibility on network operators for network information security management. If a network operator discovers that information released by users is prohibited by laws and regulations, they shall immediately cease transmission of such information and take measures such as deletion to prevent further dissemination.[64] Additionally, network information security complaint and reporting mechanism shall be established by network operators, and the method for complaint and reporting shall be published.[65]

Footnote(s):

[62] Cybersecurity Law of the People's Republic of China, Art.34.

[63] Cybersecurity Law of the People's Republic of China, Art.38.

[64] Cybersecurity Law of the People's Republic of China, Art.47.

[65] Cybersecurity Law of the People's Republic of China, Art.49.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

The CSL imposes requirements regarding supply chain management, particularly for CIIOs. Under Art.36, when purchasing network products and services, CIIOs shall enter into agreements with the suppliers to clarify the security and confidentiality obligations. If there is any potential risk to national security associated with CIIOs' purchase of network products and services, CIIOs shall apply for cybersecurity review. This review may also be initiated by the authorities. It is noteworthy that critical network equipment and specialized cybersecurity products sold or supplied within China shall pass security certification or examination by qualified organizations.[66] Companies are recommended to verify the qualifications when purchasing such products.

Footnote(s):

[66] Cybersecurity Law of the People's Republic of China, Art.23.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

According to Art.29 of the CSL, cooperation among network operators in collection, analysis and notification of cybersecurity information and emergency response is supported. The MIIT promulgated the *Measures for Monitoring and Handling Threats to the Cybersecurity of Public Internet* in 2017. Art.6 of these measures requires that, if a discovered cybersecurity threat involves other entities, related information shall be promptly submitted to the MIIT and provincial communications administration. Furthermore, Art.7 of the *Administrative Provisions on Security Vulnerabilities of Network Products* requires that, if security vulnerability is identified in network products, providers shall report the vulnerability information to the sharing platform established by the MIIT in two days. Art.8 further requires that the release of security vulnerabilities information shall ensure necessity, authenticity, objectivity and being conducive to preventing cybersecurity risks.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

The CSL requires network operators to appoint a **person responsible for cybersecurity** to ensure the implementation of cybersecurity responsibilities.[67] With reference to Art.15 of the *Security Protection Regulations for Critical Information Infrastructure*, responsibilities of the cybersecurity responsible person may generally include, but are not limited to, the followings:

- Formulate internal cybersecurity administration policies and procedures;
- Promote cybersecurity protection, monitoring and risk assessment work;
- Develop emergency plan with respect to security incidents and conduct regular emergency drills;
- Organize cybersecurity review and assessment work, put forward related reward and punishment advice;
- Organize cybersecurity education and training;
- Conduct security management to related networks design, construction, operation, maintenance, etc.;
- Report security incidents and important matters as required by the law.

Footnote(s):

[67] Cybersecurity Law of the People's Republic of China, Art.21.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

Several competent authorities in China have developed industry-specific regulations for cybersecurity management. For examples, the National Health Commission and other authorities released the *Administrative Measures for the Cybersecurity of Medical and Healthcare Institutions* in 2022; the National Energy Administration amended the *Administrative Measures of Cybersecurity in Electric Power Industry* in 2022; the China Securities Regulatory Commission released the *Administrative Measures for Cybersecurity and Information Security in the Securities and Futures Industry* in 2023; and in January 2025, the *Administrative*

Measures of Reporting Cybersecurity Incidents in Business Areas of the People's Bank of China (Draft) has been published for public comments.

40. What impact do international cybersecurity standards have on local laws and regulations?

National standards of cybersecurity play an important role in guiding cybersecurity practices in China, and part of such national standards are based on international standards. For instance, the national standard *GB/T 31497-2024 Cybersecurity technology—Information security management — Monitoring, measurement, analysis and evaluation* is identically based on the international standard ISO/IEC 27004:2016.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

"Cybersecurity incidents", in accordance with the *Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)* (the "Cybersecurity Incident Measures") released by the CAC, refer to incidents that cause harm to networks and information systems or the data therein and result in adverse impacts on society due to human factors, software and hardware defects or failures, natural disasters, etc.

Pursuant to the *Guidance on Grading of Cybersecurity Incidents (Draft)*, which is an attachment of the Cybersecurity Incident Measures, cybersecurity incidents are divided into four levels, i.e., extraordinarily significant, significant, relatively significant and general. The factors determining the level of a cybersecurity incident include: (1) severity of the damages done to critical networks and information systems (e.g., if the damage paralyzes the systems or results in the loss of business processing capabilities); (2) severity of threats to national security and social stability posed by the loss, theft or tampering of national secrets, important and sensitive information, and critical data; and (3) severity of other impacts on national security, social order, economic development and public interests.[68]

Where any cybersecurity incident occurs, network operators shall immediately initiate emergency response plans to manage the incidents. Additionally, cybersecurity incidents classified as extraordinarily significant, significant and relatively significant, should be reported within 1 hour to competent authority.

Besides, Art.10 of the RANDS provides that, any security defect or vulnerability discovered in network products or services shall be notified to users and reported to competent authority in a timely manner. If such risks may harm the national security or public interest, the network data processors shall report to competent authority within 24 hours.

Footnote(s):

[68] Guidance on Grading of Cybersecurity Incidents (Draft). Art.1, Art.2, Art.3, Art.4.

42. How are cybersecurity laws in your jurisdiction typically enforced?

1) Administrative regulation.

- **Cybersecurity supervision**. The administrations of cyberspace, communications and public security and other industry regulators take supervision and enforcement measures from different aspects. Among them, the administration of public security keeps active in supervising and addressing violations of network operators affecting public or national security according to the CSL such as the failure to take effective management or technical measures regarding cybersecurity, etc. Enforcement actions may be initiated by compliant, routine monitoring and identification of cybersecurity threats, or in the investigation process into cybercrimes.
- **Cybersecurity and Internet content supervision.** The CAC in accordance with the CSL has also fined violating entities including major domestic online forum operator, social media, online retailing operator for repetitive dissemination of information and content prohibited by laws, failure to fulfill cybersecurity obligations about MLPS, system vulnerabilities, etc.
- **Cybersecurity review.** For substantial cybersecurity risks occurred in the purchase of network products and services by CIIOs or in the data processing activities by the network platform operators, which affect or may affect national security, the CAC may launch the cybersecurity review to inspect, take enforcement actions and impose penalties against illegal behaviors.

2) Criminal charges. *The Criminal Law of the People's Republic of China (2023)* stipulates several crimes related

to cybersecurity, which mainly includes the “Crime of Illegally Invading Computer Information System”(Art.285), “Crime of Illegally Obtaining Data of Computer Information System or Illegally Controlling Computer Information System”(Art.285), “Crime of Sabotaging Computer Information System”(Art.286), and “Crime of Refusal to Fulfill the Obligation of Security Administration on Information Networks” (Art.286).

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Comprehensively, Chapter 5 of the CSL describes the establishment of cybersecurity monitoring and early warning mechanism, which empowers authorities to oversee and take measures responding cybersecurity risks. For example, Art. 55 of the CSL provides that, where a material security risk is discovered or security event occurs in a network, authorities assuming oversight duties can interview with the legal representative or responsible person of operator of such network. Additionally, the Ministry of Public Security released the *Regulations for Internet Security Supervision and Inspection by Public Security Organs* in 2018, specifying the objects, content and procedures for cybersecurity inspection.

According to the RANDS, competent authorities assume the responsibility to regularly organizing the assessment of network data security risks of their respective industries and fields.[69] During supervision and inspection, regulators can take measures such as requiring the data processor to explain, consulting and copying relevant documents and records, inspecting the operation of security measures, etc.[70]

Footnote(s):

[69] The Regulations for the Administration of Network Data Security, Art.48.

[70] The Regulations for the Administration of Network Data Security, Art.50.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

Administrative penalties under the CSL can reach up to 1 million RMB or 10 times of illegal earning of violating company and up to 100,000 RMB on the responsible person directly in charge and other directly liable persons.[71] For crimes related to cybersecurity, penalties vary and may include fines, public surveillance, criminal detention, and fixed-term imprisonment.

Footnote(s):

[71] Cybersecurity Law of the People's Republic of China, Chapter 6.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Competent authorities and judicial departments in China have the discretion in determining the amount of fines on a case-by-case basis, taking into consideration of severeness of the violating acts, adverse consequence, etc. **(discussed in Question 32)**

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

A citizen, a legal person or any other organization may first apply to the relevant administrative organ for reconsideration and, if refusing to accept the reconsideration decision, may initiate an action to the people's court. The action may be initiated to the people's court directly, unless it is required by any relevant laws to exhaust administrative reconsideration before seeking judicial review.[72]

Footnote(s):

[72] Administrative Procedure Law of the People's Republic of China (Amended in 2017), Art.44.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

Enforcement activities in cybersecurity regulation are expected to continue focusing on the violations and crimes affecting national security. This includes the launch of cybersecurity review, priority investigation significant cybersecurity threats originating overseas and whether relevant entities have fulfilled the protection obligations or taken effective risk prevention measures, etc. Additionally, normalized inspection and enforcement by local regulators will also continue.

Information security governance is expected to be

tightened, particularly in response to information services driven by AI technology. The rectification of the misuse of AI is one of the key priorities in the "QINGLANG" series of special actions for 2025 as announced by the CAC on February 21, 2025. The CAC is focusing on managing information content security involving AI technology and will combat the generation and dissemination of false information through AI.

Contributors

Jihong Chen
Partner
chenjihong@zhonglun.com