COUNTRY
COMPARATIVE
GUIDES 2024

The Legal 500
Country Comparative Guides

China

DATA PROTECTION & CYBERSECURITY

Contributor

Zhong Lun Law Firm LLP

Mr. Chen Jihong

Senior Equity Partner and Head of IP Department | 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 by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Cybersecurity Law of the People's Republic of China (hereinafter as the "CSL") was enacted on June 1, 2017, which forms the backbone of cybersecurity and data privacy protection legislation in China. On 10 June 2021, *the Data Security Law of the People's Republic of China* (hereinafter as the "DSL") was adopted at the 29th session of the Standing Committee of the 13th National People's Congress, effective as of 1 September 2021. The DSL is the fundamental law in data security sphere which widely covers data security mechanisms, obligations, and liabilities at both State administration and data processor level. On 20 August 2021, *the Personal Information Protection Law of the People's Republic of China* (hereinafter as the "PIPL") was adopted at the 30th session of the Standing Committee of the 13th National People's Congress, effective as of 1 November 2021, which embraces the new era of personal information ("PI") protection as well as corporate data protection compliance. The DSL, the PIPL and the CSL altogether outline the data regulatory framework in China. In addition, *the Anti-Telecom and Online Fraud Law of the People's Republic of China* was adopted at the 36th session of the Standing Committee of the 13th National People's Congress, effective as of 1 December 2022, which is aimed to prevent the illegal use of the PI in telecom or online fraud.

The cybersecurity and data protection legislative framework in China, besides the foregoing fundamental laws, also covers multiple supplementary regulations, implementing measures, and standards. Key regulations and rules entail:

- *The Cybersecurity Review Measures*
- *The Security Protection Regulations for Critical Information Infrastructure*
- *The Regulations for the Administration of Network Data Security (Draft)*
- *The Measures for Security Assessment of Data Cross-border Transfer*
- *The Measures for the Standard Contract for Outbound Transfer of Personal Information*
- *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 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 Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation)*
- *The Regulations on the Protection of Minors Online*
- *Information Security Technology - Requirements for Classification and Grading of Network Data (Draft)*
- *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 (Draft)*
- *The Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)*

China's legislation on cybersecurity and data protection establishes a number of supervisory mechanisms and sets up numerous obligations for companies, non-compliance business operations in relation to cybersecurity, data security and related regulation could result in civil infringement, administrative sanctions and even criminal liabilities.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Legislations regulating the cross-border data transfer ("CBDT") in China has been active in recent years. For instance, the *Measures for the Standard Contract for Outbound Transfer of Personal Information* came into effect as of June 1 2023. For the purposes of facilitating data flow and promoting foreign investments, the *Provisions on Facilitating and Regulating Cross-border Data Flows ("Cross-border Provisions")* was officially launched and became effective on 22 March 2024. (**Further discussed in Question 32**).

To adapt to the new legislations and establish a coherent legal liability system, China has initiated the first amendment procedure of CSL which was enforced in 2017. On September 12, 2022, a drafted amendment of the CSL has been published for seeking public opinions. This amendment mainly focuses on the legal liabilities for violating general provisions on cybersecurity, security protection of Critical Information Infrastructure ("CII"), online information security and PI protection, and the amendment is expected to be completed and come into effect in 2024-2025.

In addition, the *Regulations for the Administration of Network Data Security (Draft) (*"RANDS"*)* was published for comments in 2021 by the Cyberspace Administration of China ("CAC"), which is attached with high importance and is also expected to make progress in 2024-2025. One of the essential impacts of the formal issuance of RANDS, according to the present drafted version, is to further clarify the identification and protection measures, as well as legal liabilities, of Important Data, which is critical in the establishment of data classification and grading mechanism provided by DSL and other enforcement of regulations based on data grading mechanism. In order to respond to the practical need, the legislative works relating to Important Data are expected to have great progress both in overall standard and Important Data catalogs in separate sectors.

Besides, with regard to the key legal developments on cybersecurity and PI protection, *the Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)* (**further discussed in Question 34 below**) and the *Administrative Measures for the Compliance Audit of Personal Information Protection (Draft)* were published for comments in 2023 and are most likely to be finalized in 2024.

Last but not the least, based on 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 Data Bureau and 17 other departments further jointly issued the *"Three-Year Action Plan for "Data Element x" (2024-2026)"* ("Action Plan") on January 4, 2024. The Action Plan explicitly provides supports from following three aspects, namely, enhancing the level of data supply, optimizing the data circulation environment, and strengthening data security. In addition, the Action Plan once again proposes to continuously optimize the regulatory measures for cross-border data flow.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

The DSL reiterates certain registration or licensing requirements which is greatly in line with the telecommunication and export control regulations. The DSL, Art.34 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 laws". Such provision is in great convergence with the existing telecommunication supervision regime in China, for example operators of cloud storage and computing services shall obtain related licenses including IDC/IRCS license. Qualification administration of data processing related services may become another regulatory focus.

Art.25 of the DSL also aligns with the export control laws in China, specifying 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”. In accordance with the *List of Technologies Prohibited or Restricted from Export (2023)*, export of restricted technologies including certain artificial intelligence (“AI”) interface technology, speech synthesis technology and personalized recommendation technology requires export licenses by the Ministry of Commerce (“MOFCOM”).

Key registration and filing requirements under the PIPL are mainly for entities conducting data cross-border transfer activities, i.e., the filing for the CAC security assessment and registration of the Standard Contract along with the personal information protection impact assessment (“PIA”) report with the CAC (**further discussed in Question 32 below**)

In addition, the CSL sets out the network security multi-level protection scheme (“MLPS”) applicable to network operators building, operating, maintaining and using networks within the territory of China. For networks with level 2 or above, network operators shall file for records with related public security organs.

4. How do these data protection laws define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”) versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

“Personal information” under the PIPL refers to 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 personal information that is likely to cause detriment to the dignity of a natural person or damage to one’s personal or property safety once leaked or illegally used, including biometric identification, religious belief, specific identity, medical health, financial account, whereabouts and tracks as well as personal information of minors under the age of 14.

The PIPL also sets out the following key definitions relating to PI processing:

“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 purpose and method of processing in their activities of processing of personal information, which is substantially equivalent to the concept of “controller” under the GDPR.[3] It is worth noticing that the PIPL introduces the notion of “Processor of small-scale PI”[4], it’s 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 in which personal information is processed so that it is impossible to identify certain natural persons and that it cannot be recovered[6]. Anonymized information is not deemed as personal information.

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 are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline

any such principles or “fair information practice principles” in detail.

The PIPL sets out comprehensive PI processing principles which shall be implemented throughout the full lifecycle of PI processing activities. The principles are illustrated as below:

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)

The PIPL and GDPR are quite alike with respect to PI processing principles. PI processing can only be conducted where one of the legal bases under the PIPL is fulfilled, and PI shall be kept for the minimum period necessary for achieving the purpose of processing, unless as otherwise stipulated by laws and 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.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

The PIPL in Art.13 provides seven legal bases for PI processing[8], among which “consent” and “necessary for the performance of a contract or for human resource management” are mostly used by companies conducting businesses related to PI processing. In general, consent is required where the PI processing at issue is not exclusively intended for the provision of services and products and other legal bases such as legal obligations are lacking as well, for example consent is normally required for targeting advertising and promotional marketing purposes. For the determination of “necessity” with respect to the performance of contract, reference can be made to the *Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (“Rules”)* issued by the CAC and relevant authorities on May 2021, which sets out the basic functional services and corresponding necessary PI[9] for thirty-nine types of service applications (“APPs”), for example for online ride-hailing apps, the basic functional service would be online car booking and calling related services and necessary PI includes registration mobile number, location of departure, destination, etc., payment information.

The PIPL also stipulates “separate consent” for specific PI 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. It is noteworthy that 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, which sheds some light on the relationship between “separate consent” and other legal bases provided by PIPL.

Footnote(s):

[8] 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.

[9] Necessary PI under the Rules refers to the personal information necessary for ensuring the normal operation of an App’s basic functional services, without which the App cannot achieve its basic functional services.

7. 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)?

Art. 14 and 15 of the PIPL set out the conditions of valid consent are fully informed, freely given, explicit and easy to withdraw. Where PI processing activities are conducted 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.

To fulfill the aforementioned 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):

[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.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

In accordance with Art.28 of the PIPL, sensitive PI can only be processed with specific purpose(s) and sufficient necessity and strict protection measures shall be adopted. Processing of sensitive PI is subject to special transparency and separate consent requirement. PI processors shall, in addition to the disclosure matters stipulated in Art. 17, inform individuals of the necessity of processing his/her sensitive PI and the impact on his/her personal rights and interests, unless otherwise prescribed by laws.[12] Processing of sensitive PI is subject to separate consent requirement[13], but it is only required where the processing is originally based on consent (**discussed in Question 6 above**). PIA is required for processing of sensitive PI, and the PIA report and related documentation shall be kept for at least three years.[14] It's recommended that companies implement stringent technical and organizational measures for sensitive PI protection on the basis of data classification and grading mechanism, and keep tuned to any legislative developments, enforcement trends and industrial practices.

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.

9. How do the data protection laws in your jurisdiction address health data?

Firstly, if the health data can be related to an identified or identifiable natural person, and can be considered as PI, it will be protected by PIPL, and personal health information is also included in the listed categories of sensitive PI, applying the protection measures **discussed in Question 8 above**.

Secondly, in a national standard of *GB/T 39725-2020 Information Security Technology-Guide for Health Data Security*, the definition of "health data" covers both personal health data and other electronic health data generated by processing of personal health data. According to this national standard, health data is graded to 5 levels according to the data importance and possible damage or impact it will exert to data subjects, equipped with various scope of permitted disclosure, and key points of security measures such as de-identification, close over and access control. There are also management requirements regarding health data including the establishment of health data security committee and office, management in the full process (such as planning, execution, inspection, improvement and emergency response) and record keeping.

In China, human genetic resource information refers to information materials such as data generated from human genetic resource materials. Those that provide or offer open access of the human genetic resource information to foreign organizations, individuals and the institutions established or actually controlled thereby shall file for record with the administrative department of science and technology under the State Council and submit such information for backup, as provided in the *Administrative Regulations on Human Genetic Resources*. In addition, the *Implementing Rules of the Regulations for the Management of Human Genetic Resources* promulgated in 2023 provide more details on the management of human genetic resources information.

10. Do the data protection laws in your

jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The PIPL does 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.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Protection of PI of minors under the age of 14 is subject to stringent regulation in China. *The Law of the People's Republic of China on the Protection of Minors (2020)* sets a separate chapter "Network Protection" to emphasize the protection of legitimate rights and interests of minors in cyberspace and to effectively prevent addiction to network products and services.[15]

In accordance with Art. 31 of the PIPL, PI processors shall obtain parental consent prior to any processing of PI of minors under the age of 14 and shall formulate specialized rules for processing such PI. PI of minors under the age of 14 also belongs to sensitive personal information, therefore is subject to stringent requirements of security protection, specific disclosure, PIA, etc. (**discussed in Question 8 above**). Where minors, their parents or guardians require PI processors to correct or delete the PI of minors, the PI processors shall promptly take measures to do so, unless otherwise provided by laws and administrative regulations.[16]

The *Regulations on the Protection of Minors Online* that was promulgated on 16 October 2023 and took effect on January 1 2024, further specifies the detailed requirements for minor protection on various subjects including manufacturers and sellers of smart terminal products, major internet platform service providers and internet service and product providers, for example, service providers of online games shall develop minor mode of its services, sets time and purchase limitation with respect to the use the game by minors and shall require identity authentication at registration and log-in. Failing to comply with the *Regulations on the Protection of Minors Online* could lead to fines up to 50 million RMB or 5% of the previous year's turnover, administrative fines up to 1 million RMB on responsible person(s) directly in charge, shutting down of related websites, revocation of relevant business licenses. Network product and service providers shall not re-apply for relevant licenses within 5 years, and their directly responsible supervisors and other directly responsible personnel shall not engage in similar network products and services within 5 years.[17]

Footnote(s):

[15] The Law of the People's Republic of China on the Protection of Minors (2020), Chapter V.

[16] The Law of the People's Republic of China on the Protection of Minors (2020), Art.72.

[17] Regulations on the Protection of Minors Online, Chapter VI.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

Online safety is a key area of regulation in China. In this regard, Article 15 of the *Administrative Measures on Internet-Based Information Services* has expressly stipulated certain contents that are banned to be produced, copied, published or distributed by network service providers, such as information that may endanger national security, incite ethnic hatred and ethnic discrimination, disseminate obscene materials, advocate gambling, violence, killing and terrorism, instigate others to commit crimes, humiliate or defame other persons, infringe the legitimate rights and interests of the others, etc. If the aforesaid information appears, network service providers shall immediately stop the information dissemination, keep record and report to relevant authorities. *Provisions on the Ecological Governance of Network Information Contents* released by CAC also stipulates similar content, that network information content producers should take measures to prevent and resist the production, reproduction, publication of content that may cause minors to imitate unsafe behavior and induce minors to bad habits, or bloody, scary, cruel or otherwise causing physical and mental discomfort. The network information content service platform is also required to strengthen the management of information content, improve user registration and account management rules, and conduct content review of user-published information. The *Regulations on the Protection of Minors Online* prohibits sending or pushing online information that may endanger minors' physical and mental health, and prohibits insulting, defaming, threatening and other cyberbullying behaviors against minors through the Internet[18].

With regard to law enforcement, according to the CSL and the *Administrative Measures on Internet-Based Information Services*, the network service provider will be liable for any erroneous, illegal or prohibited information published on a website or other medium it provides, whether intentionally or negligently. If the provider immediately takes action to stop the wrongdoing or blocks access to such inaccurate information after receipt of notice from the affected party, its liability might be limited. The *Regulations on the Protection of Minors Online* also provide for penalties for endangering the online safety of minors.

Footnote(s):

[18] Regulations on the Protection of Minors Online, Art.25, Art.26.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

There is currently no centralized regulatory body for children's and teenagers' personal information or online safety. Since it is a topic that impinges upon multiple industries, there are a wide range of law enforcement departments related to it and their duties and authorities intersect with each other. Pursuant to Article 3 of *Provisions on the Ecological Governance of Network Information Contents and* Article 18 of *Administrative Measures on Internet-Based Information Services,* the CAC is responsible for coordinating and supervising the governance of the network information content ecology and relevant regulatory work[19]. Relevant competent authorities such as those in charge of press, education, health, drug supervision, public security and national security shall, within their respective areas of responsibility, lawfully supervise and manage network information contents[20].

Regarding law enforcement activities, in June 2023, the CAC initiated a two-month special action titled "QINGLANG 2023 Summer – Improving the Online Environment for Minors", focusing on harmful content, cyberbullying, online fraud and other relevant issues. Such action further strengthens online safety and effectively enhance the healthy and safe network environment for minors.

Footnote(s):

[19] Provisions on the Ecological Governance of Network Information Contents, Art 3

[20] Administration Regulations on the Internet Information Services, Art 18

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

Legislations related to online safety have always been active in China. For instance, the CAC released a revised draft version for the *Administrative Measures on Internet-Based Information Services* in 2021. Additionally, in recent years, central CAC and many provincial CACs have been conducting series of special actions such as "*QINGLANG*" and "*JINGWANG*" to strengthen the governance of relevant issues such as false information, pornography, and misguided values on the Internet. It can be expected that the future online safety landscape will be further improved.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

The PIPL does not specially outline the requirement of "data protection by design and by default" like the GDPR, yet the essence of such requirement is incorporated throughout the law itself.

Art.51 of the PIPL stipulates that PI processors shall, taking into account the purpose, method of PI processing activities, PI categories, impacts on personal rights and interests and possible security risks, take the following measures to ensure compliance with the laws as well as 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.

Such rules would require that PI processors at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures to protect the rights of data subjects and to meet the requirements of the PIPL in particular PI protection principles of purpose limitation, data minimization, limited storage periods, data quality.

Companies are well recommended to sort out their data assets, spot and rectify outstanding compliance issues in accordance with the law, formulate and implement PI protection mechanism at both organizational and technical level, internal PI protection policies and procedures include PI identification and classification, determination of legal basis, PI retention and destruction, third-party management, response to requests of data subjects, etc.

16. Are controllers and/or processors of personal data required to maintain any internal 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 keep records of networks operation status and any security incidents, related worklogs shall be kept for at least six months.[21] Violation of such recording 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.[22]

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 19**). Despite the PIPL does not set out a specific clause requiring a PI processor to maintain a record of processing activities under its responsibility like the GDPR, companies are still well recommended to keep records of processing activities as they bear the responsibility to ensure and demonstrate compliance with the PIPL.

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

- 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):

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

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

17. 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 for achieving the purpose of processing, unless otherwise stipulated by laws and administrative regulations.

Art.47 of the PIPL sets out the circumstances for PI deletion by PI processors or upon request by data subjects:

- 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 storage 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 clearly specifies that when technically impossible to delete PI, PI processors shall stop any processing thereof except for storage and necessary security protection measures. Companies under such circumstances shall ensure the PI at question is under effective protection for example through data segregation or tagging and shall not be further processed.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

The PIPL unlike the GDPR sets no mandatory prior consultation requirement, neither the CSL, the DSL nor related administrative regulations. Though in practice, companies may carry out prior consultations or enquires with competent authorities as regards for example specifics concerning the cybersecurity review or related licensing requirements for certain data processing activities to expedite related compliance work.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

1) PIA. According to Art.55 of the PIPL, PI processor shall conduct a PI protection impact assessment (“PIA”) prior to the processing under 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.

A PIA shall include the following contents[23]:

- 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.

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

For conducting the PIA, great reference can be made to the *Information Security Technology- Guideline for Personal Information Cross-Border Transfer Security Assessment (Draft)*, the non-binding guideline outlines the methodology, process, key points, etc.

2) CAC security assessment for data cross-border transfer[24]. The CSL, the DSL and the PIPL altogether outlined the comprehensive data cross-border transfer regulation framework in China. PI and Important Data[25] generated and collected within the territory of China during operation by Critical Information Infrastructure Operators (“CIIOs”)[26] as well as PI generated and collected by PI processors within the territory of China reaching the threshold[27] 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 32**).

3) CAC filing of Standard Contract and PIA report for data cross-border transfer. PIA is required before providing PI to overseas party according to the 55 of PIPL, and if the provision is to be restricted by concluding the Standard Contract, such PIA report shall be filing to the CAC together with the Standard Contract within 10 working days after the Standard Contract entering into effect.[28] This is required in the *Measures for the Standard Contract for Outbound Transfer of Personal Information*, according to which, PIA in such scenario shall focus on the following matters:

- 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.[29]

4) Cybersecurity Review. *The Cybersecurity Review Measures (2021)* released in accordance with fundamental laws including the CSL and DSL is of great importance to the implementation of the cybersecurity review mechanism. The triggering conditions are:

- Mandatory filing requirements:
- Purchasing of network products or services by CIIOs which would affect or may affect national security;[30]
- Online platform operators with over 1 million user PI going public listing abroad;[31]
- Ex officio initiation by the CAC cybersecurity review office:
- Data processing activities by online platform operators, which affects or may affect national security.

The key considerations of the cybersecurity review by competent authorities 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. Thy review progress could take around six months.

Footnote(s):

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

[24] 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.

[25] "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 (Draft) released by the CAC in November 2021, "Important Data" means data that once being tampered with, or sabotaged, leaked, illegal acquired or illegal used, may cause harm to national security or the public interest.

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

[27] 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."

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

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

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

[31] 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.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

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

1) The CSL requires that a **person responsible for cybersecurity** shall be appointed to ensure the implementation of cybersecurity responsibilities of the network operator.[32] With reference to *the Security Protection Regulations for Critical Information Infrastructure* (Art. 15. Responsibilities), responsibilities of the cybersecurity responsible person may generally include but 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.

2) **A responsible person for PI protection** (equivalent to the concept of "DPO" in the GDPR) is not required for all PI processors. Art.52 of the PIPL stipulates that PI processors processing PI over the volume stipulated by the CAC[33] shall designate a person in charge of PI protection to be responsible for supervising the activities of processing of PI, adopted protection measures, etc. PI processors shall make public the contact information of the person in charge of PI protection and submit the name, contact information, etc. of the person to competent authorities.

3) **A 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 and implement the responsibilities of data security protection**.** With reference to the RANDS Art.28, the person (s) responsible for data security shall perform the following responsibilities:

- Study and make recommendations for major decisions related to data security;
- Develop and implement data security protection plans and data security incident emergency response plans;
- Conduct data security risk monitoring, and disposing of data security risks and incidents in a timely manner;
- Organize activities such as data security awareness, education and training, risk assessment, and emergency drills to be conducted on a regular basis;
- Handle and respond to data security-related complaints and reports; and
- Report data security situations to cyberspace administrations and other competent authorities in a timely manner as required.

4) **A 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 processor processing important data to report the information on automotive data security management annually to the local cyberspace administration. One of the mandatory report matters is the name and contact information 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 positions to fulfill the regulatory requirements.

In practice, it is commonly seen in practice that IT lead or person responsible for information security is appointed as the above responsible persons by companies based on their own corporation governance/organization and considerations. Also, some companies choose to establish a committee instead of appointing a specific person to hold the roles. Such person(s) may be subject to administrative liability or even criminal liability under the laws. Failure to comply with the law and related cybersecurity and data protection obligations could lead to administrative monetary penalties on the major responsible person directly in charge, which may refer to the responsible person(s) of cybersecurity and data protection as illustrated above.

Footnote(s):

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

[33] Such threshold for PI volume with respect to the appointment of "DPO" are to be further ascertained by the CAC.

21. 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).

Employee training for cybersecurity and data protection is a general obligation required. Art. 27 of the DSL stipulates that companies carrying out data processing activities are obliged to conduct data security education and training to ensure data security as required by the laws. In violation of such obligation could lead to orders for rectification, warnings by competent authorities, administrative fines up to 2 million RMB on company and fines up to 200,000 RMB on the responsible person directly in charge, even suspension or termination of related business operations, revocation of related business licenses and permits.[34]

Specifically, the PIPL stipulates the obligation of regular employee education and training for PI security and protection in its Art.51.[35] Art.34 of the CSL stresses such obligations to be implemented by CIIOs. It shall be noted that the RANDS in its Art.30 puts out more detailed requirements that data processors of any Important Data shall develop a data security training plan, organize whole-employee data security education and training to be conducted on a yearly basis, and the yearly education and training hours for data security-related technical and managerial personnel shall not be less than twenty (20) hours.

Footnote(s):

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

[35] 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.

22. 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 policy making. Art.17 stresses that, before processing any PI of an individual, the processor shall fully inform the individuals of information relating to PI processing in an explicit, accurate and complete manner, which indicates that companies should avoid using wordings of "etc." and "such as" in their privacy policy and relevant documents. In terms of content, companies shall include all items required under Art.17 in their privacy policy. Moreover, the PIPL puts out additional disclosure requirements for specific scenarios such as providing PI to third parties[36], processing of sensitive PI[37] and PI cross-border transfer.[38] Privacy policy shall be delivered to each individual in a notable manner for example on the account registration page via a tick box or pop-up window before any collection of PI. Besides, the privacy policy shall be easily accessible. Companies may consider placing their privacy policy on their website homepages, Apps user setting sections, etc.

Footnote(s):

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

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

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

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

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 activities of processing of PI. Parties conducting PI processing activities on behalf of PI processors strictly in accordance with the instruction of PI processors are described as the entrusted parties (**further discussed in Question 24**).

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

According to the PIPL, PI processors shall take accountability with respect to its PI processing activities and ensure the compliance with the law.[39] 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 PI processed and assist PI processors to perform the obligations stipulated under the PIPL.

Art.21 of the PIPL lays down the contractual requirement between PI processors and the entrusted parties of entrusted PI processing activities, the law specifies that where a PI processor entrusts others with the processing of PI, it shall agree with the entrusted party on the purpose, period and method of the entrusted processing, type of PI, protection measures, as well as respective rights and obligations.

The entrusted party shall process PI as agreed and shall not process PI beyond the agreed purpose and method of processing; where the entrustment contract is not effective, invalid, revoked or terminated, the entrusted party shall return PI to the PI processor or delete it, and shall not retain it. The entrusted party shall not carry out any sub-processing without prior consent of the PI processor.

Footnote(s):

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

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

The PI processor is required to conduct PIA[40] and monitor the entrusted PI processing activities by the entrusted party to ensure data security capability of the entrusted party as well as the complicate with the law. It is well recommended that companies keep accurate records of any entrusted PI processing activities.[41]

Footnote(s):

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

[41] GB/T 35273—2020 Information security technology — Personal information security specification, Art.9.1 (e).

26. 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 terms defined, and what restrictions on their use are imposed, if any?

According to Art. 24 of the PIPL, automated decision making shall be transparent and fair. Data subjects are entitled to request explanation and to refuse the decision if the automated decision has 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. Automated decision-making, including algorithm recommendation technologies have become one of the focuses of the regulatory departments.

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

27. Please describe any restrictions on targeted advertising and/or cross-contextual 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 the users, is subject to relevant PI protection laws, in addition to advertising regulations (**further discussed in Question 29 below**). PI shall not be collected or used for behavioral advertising if the data subjects have not agreed to this. Pursuant to Art. 24 of the PIPL, if business marketing or push of information is conducted towards an individual by means of automated decision making (**automated decision making is also discussed above in Question 26**), 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 not contain labels including obscene, violence, discrimination against nations, ethnic and religions, etc.[42]

With respect to any sharing of PI with business partners and third parties involved in cross-contextual behavioral advertising activities, companies shall follow the rules of the PIPL for example to conclude data processing agreements to determine the scope of the processing of PI involved as well as respective rights and obligations. The receiving parties shall ensure the legality of the PI transferred. Related cross-border transfer rules shall be abided by if any PI collected and generated within the territory of China is being provided to individuals or organizations outside the territory of China (**Regulation of PI cross-border transfer is further discussed in Question 32**).

Footnote(s):

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

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

Art.44 of the CSL stipulates that no individual or organization shall unlawfully sell or provide any PI to others. 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 crime.[43]

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[44]:

- 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.

Footnote(s):

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

[44] 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.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

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

"Internet Advertising" refers to commercial advertisements which directly or indirectly promote goods or services through websites, web pages, Internet applications and other Internet media in the forms of texts, pictures, audios, videos, etc.[45]

Companies before sending any adverts shall obtain from the recipients their consent to, or request for, advertising and shall also disclose their true identity, contact details and the opt-out method for receiving advertisements distributed via electronic means.[46] Adverts publishing and posting through the Internet shall not affect the normal use of network by users. Advertisements published in the form of pop-up window on the Internet shall indicate the close sign prominently and ensure one-click closing of the window.[47] The PI Security Specification also recommends avoiding using direct profiling identifiable to specific individuals for direct marketing purposes,[48] and that PI processors shall ensure that the data subjects have the right to refuse to receive commercial advertisements based on his/her PI.[49]

Footnote(s):

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

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

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

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

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

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

Biometric information includes personal genes, fingerprints, voice prints, palm prints, auricles, iris, facial recognition features, etc.[50] Biometric information falls into the category of sensitive PI, thus is subject stringent protection measures, special transparency and separate consent requirements (**special requirements for sensitive PI discussed under Question 8**). 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 hotly debated issue of application of face recognition technology, the judicial interpretation issued by the Supreme People's Court on August 2021 further clarifies that processing of facial recognition information shall be sufficient necessary; PI processor shall obtain the consent of an individual for processing its facial recognition, unless such processing is necessary for the provision of products or services.[51] Property service companies or any other building administrators shall not use facial recognition as the only means of identity authentication, reasonable alternatives should be provided to property owners or users as requested.[52]

Footnote(s):

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

[51] 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.

[52] 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.10.

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

In 2023, the regulatory framework on AI has been systematically built and implemented. Such framework mainly includes the *Interim Measures for the Administration of Generative Artificial Intelligence Services* ("AIGC Measures") that took effect on 15 August 2023 and the *Circular on Releasing the Measures for Review of Scientific and Technological Ethics (for Trial Implementation)* that took effect on 1 December 2023. The AIGC Measures expressly outline the regulatory framework for generative AI technology and encompass various stages such as application deployment, model training and optimization, and multiple subjects such as 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 guidance for assessing the AI generated content service security.

Furthermore, the *Circular on Releasing the Measures for Review of Scientific and Technological Ethics (for Trial Implementation)* demonstrate China's significant attentions to technology development as well as the problems and concerns brought about by emerging AI technologies.

32. 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 data cross-border transfer in China, along with multiple supplemental regulations, measures, and standards. Chapter III of the PIPL sets the conditions under which PII can be transferred overseas.

1) **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 standards for PI protection as prescribed by the PIPL. In practice, such substantial requirement can be fulfilled through contractual arrangements, regular reviews and audits and technical monitoring. In addition, PI processors shall meet the transparency requirement and provide adequate information with respect to 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 carrying out any PI cross-border transfer activities. With respect to the separate consent requirement, it's clarified that such requirement should only be met when the processing is originally conducted based on consent (e.g., for targeted advertising purpose).[53]

2) **CBDT Mechanisms:** PI processors that outbound transfer PI to abroad shall implement the three CBDT mechanisms in accordance with 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, has come into 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; 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 same year. The CAC security assessment normally would take 45 working days or longer in complicated situation or when materials should be corrected and supplemented, and its validity lasts for 3 years.

- **CN Standard Contract.** In addition to the CAC security assessment illustrated above, the PIPL Art.38 states that, PI processors can also 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). The CN Standard Contract ("Chinese SCCs") has been officially released and become effective on 1 June 2023. It is noteworthy that the Chinese SCCs shall be concluded in strict accordance with the version published by CAC and the CAC may also adjust the Chinese SCCs in light of actual circumstances.
- Conduct PI protection certification by designated institutions is another CDBT mechanism provided by the PIPL Art.38. The CAC clarifies 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* in order to identify the applicable type of certification. In addition, on 16 March 2023, the *Information Security Technology-Certification Requirements for Cross-border Transfer of Personal Information (Draft)* (the "Certification Requirements"), was published for public comments by the National Information Security Standardization Technical Committee. 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.
- Exempted scenarios: The Cross-border Provisions issued by CAC on 22 March 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, for the establishment or performance of contracts to which individuals are parties, in implementing cross-border HR management based on legally formulated labor rules and collective contracts, 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 same year. In general, the Cross-border Provisions show the trend of stabilizing foreign-investments and promoting economic development and shall be deemed as positive sign for multinational companies.

Footnote(s):

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

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

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

- Formulating internal security management policies and operation procedures to determine the person in charge of cybersecurity and 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.

In particular, Art.42 of the CSL stresses that network operators shall take technical and other necessary measures to ensure the security of PI it collects, and to protect such information from any leakage, damage or loss.

The DSL, in great convergence with the CSL, illustrates that entities carrying out data processing activities shall on the basis of the MLPS establish a data security management system throughout full lifecycle of data processing activities and take corresponding technical measures and other necessary measures to ensure data security.[54] Data processors when carrying out data processing activities shall strengthen risk monitoring and take immediate remedies upon any discovery of any data security vulnerabilities, bugs or any data incidents.[55]

Art. 51 to Art. 57 of the PIPL describe the comprehensive obligations of PI processors and require companies to set up internal PI protection management based on PI security. Particularly, Art.51 of the PIPL stipulates that PI processors shall, taking into account the purpose, method of PI processing activities, 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.

With reference to the *Guidance on Application of Cross-border Data Transfer Security Assessment (first version)*, data processor that meets the threshold of CAC security assessment shall evaluate its data security safeguard capability including security management capability and security technological capability. The data security management capability shall cover management organization and structure, and internal policies including full process management, data classification and grading, emergency response, risk assessment, protection of PI rights and interests, while data security technological capability shall cover the technological measures adopted in the full process of 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 prepare its improvement plan and introduce it in application materials to CAC, thus it can be deduced that such data processor shall fulfill these security obligations to prove its security safeguard capability on data processing.

Footnote(s):

[54] Data Security Law of the People’s Republic of China, Art.27.

[55] Data Security Law of the People’s Republic of China, Art.29.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a “security breach”?

“Cybersecurity incidents”, in accordance with the *Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)* (“*Cybersecurity Incident Measures*”) released by the CAC as one of the supplementary measures of the CSL, 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 on national security and stability of society posed by the loss, theft or tampering with 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[56].

Where any cybersecurity incident occurs, network operators shall immediately initiate emergency response plans to handle such incidents. In addition, cybersecurity incidents that are classified as extraordinarily significant, significant and relatively significant, should be reported within 1 hour.

Footnote(s):

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

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

CIIOs under the cybersecurity and data protection laws in China bear stringent data security obligations. On July 30, 2021, the *Security Protection Regulations for Critical Information Infrastructure* was promogulated in the form of Decree No. 745 of the State Council, effective as of September 1, 2021. In accordance with the *Security Protection Regulations for Critical Information Infrastructure*, CII refers to the important network facilities and information systems in important industries and fields such as public telecommunication and information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damages to national security, the national economy and the people's livelihood and public interests.[57] CIIOs shall be developed with the capacity to support the steady and continuous business operation, and technical security measures shall be planned, established and put into use simultaneously . In addition to those security obligations imposed on network operators, CIIOs shall also fulfill stricter obligations of security protection.[58]

In certain special sectors, there are specific security requirements. For example, the CAC together with the National Development and Reform Commission (NDRC), MIIT, Ministry of Public Security ("MPS") and the Ministry of Transport released the Several Provisions on Automotive Data Security Management (for Trial Implementation) effective as of 1 October 2021, which sets of stringent data security obligations on the basis of MLPS, including regular risk assessment and annual filing requirements. In the financial sector, the *Administrative Regulations on Financial Information Services* issued by the CAC regulate the financial information service[59] providers and require them to take affirmative organizational measures[60] and appropriate technical measures.[61] In the telecom sector, the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users* issued by MIIT contain one chapter regarding security measures. Telecommunications business operators and Internet information service providers are required to adopt security measures specified in Art. 13 to 15, covering both organizational and technical.[62]

In the industry and information technology sector, the *Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation)* has been effective as of January 1, 2023, which regulates the processing of industrial data, telecommunications data and radio data, etc. if relevant data processor involves processing of Important Data and Core Data, it shall file the catalogs to the local sectoral regulatory authority. Such data processors shall also carry out risk assessment at least once a year and file the risk assessment report to the local sectoral regulatory authority.[63]

In algorithmic recommendation on Internet information service, service providers shall establish and improve the management systems and technical measures for algorithm mechanism and principle review, scientific and technological ethics review, user registration, information release review, data security and PI protection, anti-telecommunications and Internet fraud, CAC security assessment and monitoring, and security incident emergency response, formulate and disclose the relevant rules for algorithm recommendation services, and be equipped with professional staff and technical support appropriate to the scale of the algorithm recommendation service.[64] Algorithm recommendation service providers with public opinion attributes or social mobilization ability shall, within 10 working days from the date of providing services, go through the filing procedures. (**AI governance is further discussed in Question 31 above**.)

Footnote(s):

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

[58] Cybersecurity Law of the People's Republic of China, Art.34, Art.35.

[59] Financial information services were defined by the Regulations as the provision of information or data that may affect the financial market to users involved in financial analysis, financial trading and financial decision-making, or other financial activities.

[60] Administrative Regulations on Financial Information Services. Arts. 5 & 7.

[61] Administrative Regulations on Financial Information Services. Art.6, Art. 9.

[62] Provisions on Protecting the Personal Information of Telecommunications and Internet Users. Art. 13-15.

[63] Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation), Art. 12 & 31.

[64] Administrative Provisions on Algorithm Recommendation for Internet Information Services, Art.7

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

Notification of PI breach to the supervisory authority and communication of such breach to data subjects are generally required in the CSL and the DSL. The PIPL in its Art. 57 particularly specifies that where PI has been or may be divulged, tampered with or lost, the PI processor shall immediately take remedial measures and notify the competent authorities and data subjects concerned. The notice shall include the following matters:

- Types of PI that has been involved or may be involved in the divulgence, tampering with or loss, reasons and possible harm for the breach;
- 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.

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

- In addition to the PI breach above, Art.25 of the CSL stipulates that for security breach endangering cybersecurity, network operators shall immediately initiate emergency plans as developed, take corresponding remedial action and report to competent authorities in accordance with the law. For further implementation details of such reporting obligations, the *Cybersecurity Incident Measures* was published for comments on 8 December 2023, with the draft of *Guidance on Grading of Cybersecurity Incidents* and the *Cybersecurity Incident Information Report Form* being attached.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

The State shall in accordance with the laws impose sanctions towards cyber-crimes and maintain the security and order of cyberspace.[65] *The Criminal Procedure Law of the People's Republic of China* stipulates that any entity or individual, upon discovering facts of a crime or a criminal suspect, shall have the right and duty to report the case or provide information to a public security organ, a people's procuratorate or a people's court.[66] Yet no specific legal requirements are set out for dealing with cyber-crimes including ransoms payment.

Footnote(s):

[65] Cybersecurity Law of the People's Republic of China, Art.5.

[66] Criminal Procedure Law of the People's Republic of China, Art.110.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The CAC is the key regulator with respect to cybersecurity and data protection administration in China. The CSL, the DSL and the PIPL altogether specify that the CAC is in charge of the overall planning and supervision of cybersecurity and data protection, for example with respect to the CAC security assessment of PI cross-border transfer (PIPL, Art.40), the Cybersecurity Review as well as the formulation of the Chinese SCCs. There are multi-regulators in addition to the CAC taking charge of their respective duties supervising and administering cybersecurity and data protection in accordance with the laws, which include the MPS (MLPS, CII supervision, etc.), MIIT, State Administration for Market Regulation (SAMR) and industrial regulators are in charge of law enforcement in their respective sectors. **(For regulation of specific cybersecurity issues, see further discussion in Question 43 below.)**

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

The PIPL in its Chapter IV prescribes ten data subject rights 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 that a PI processor shall 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

Art.49 specifies that where a natural person dies, his or her close relatives may for the purpose of their own lawful and legitimate interests, exercise data subject rights such as accessing, copying, rectifying and deleting the relevant PI of the deceased as prescribed in the PIPL, unless otherwise arranged by the deceased prior to his or her 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[67]:

- 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.

Footnote(s):

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

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Individual data privacy rights are both enforceable through judicial system and administration regulators.

1) **Administrative enforcement**. Art.61 of the PIPL states that the CAC and related competent authorities are obliged to investigate unlawful PI processing activities and handle complaints related to PI protection.

2) **Civil litigation**. Art.50 of 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." (**further discussed in Question 41**)

41. 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."[68] and lays the foundation of PI protection in the form of a special 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* issued in 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"[69]. *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):

[68] PRC Civil Code, Art. 1034.

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

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is 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 thus suffered by the individual concerned or the benefits thus obtained by the PI processor; if the losses thus suffered by the individual concerned or the benefits thus obtained by the PI processor are difficult to be determined, the amount of damages shall be determined in accordance with the actual circumstances.[70] 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[71].

Footnote(s):

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

[71] PRC Civil Code, Art. 1183.1.

43. How are data protection laws in your jurisdiction enforced?

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

- **APPs supervision.** With respect to specific governance action towards unlawfully collection and use of PI by Apps, the CAC, MIIT and competent authorities have been carrying on continuous inspection, focusing on issues including PI collection and processing beyond the agreed purposes or without prior valid consent and failure to provide users with an option to withdraw consent. The CAC together with relevant authorities have issued implementing measures including the *Rules*, which is of great reference to regulatory supervision as well as compliance check of companies.
- **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' algorithm mechanism. The special action will also focus 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 publicly has issued four batches of domestic deep synthesis service algorithm filing information respectively in June 2023, September 2023, January 2024 and February 2024 including algorithms from technology companies such as Baidu, Alibaba, Tencent, etc.
- **Cybersecurity and Internet content supervision.** In addition, 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 comply with cybersecurity obligations in relation to MLPS, system

vulnerabilities, etc.

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.” The Supreme People’s Procuratorate in August 2021 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. Over the last year, procuratorial organs have handled more than 6,600 public interest litigation cases in the field of PI protection and anti-telecom and online fraud.

3) Private right of action. The PIPL establishes the principle of presumption of liability, thus the burden of proof is with the PI processors,[72] 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 41**)

4) Criminal charges. The “*Criminal Law Amendment (IX)*” integrates “crimes of selling and illegally providing citizens’ personal information” and “crimes of illegally obtaining citizens’ personal information” into “crimes of infringing 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, from January to November 2023, procuratorial organs have prosecuted 280,000 people in total for various types of cybercrimes, accounting for 18.8 percent of all criminal offenses. Among them, nearly 7,300 people were prosecuted due to the infringement of citizens’ PI and 42,000 people were prosecuted due to the telecom fraud.

Footnote(s):

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

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

Cybersecurity and data protection laws in China impose various sanctions on violating behaviors which could entail warnings, rectification orders by 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 be 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.[73] Administrative penalties under the CSL can be up to 1 million RMB or ten times of illegal earning of violating companies and up to 100,000 RMB on the responsible person directly in charge and other directly liable persons.[74] 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.[75]

Footnote(s):

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

[74] Cybersecurity Law of the People’s Republic of China, Chapter 6.

[75] Data Security 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 enjoy the discretion in determining the amount of fines on a case-by-case basis, taking into consideration of severeness of the violating acts, infringements upon legitimate rights and interests on individuals, adverse impact on the society, etc. In March 23, 2023, the CAC in China issued the *Provisions on Administrative Law Enforcement Procedure of Cyberspace Administration*, which sets 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 given if the violation was first and minor, the harmful consequence was minor, and the illegal act was promptly corrected; administrative punishments may also not be given if the circumstance of the violation was minor and corrected in a timely manner, without causing harmful consequence.[76]

Footnote(s):

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

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

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; it/he may also initiate an action to the people's court directly, unless it is required by any relevant laws to exhaust administrative reconsideration before seeking judicial review.[77]

Footnote(s):

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

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

The CBDT mechanisms have been equipped with enforcement measures or standards. The grace period for rectification stipulated in *the Measures for Security Assessment of Data Cross-border Transfer* and *the Measures for the Standard Contract for Outbound Transfer of Personal Information* for cross-border data transfer has expired. In view of the elimination of uncertainty in the CBDT regulatory policy with the release of the Cross-border Provisions, what kind of enforcement or punishment measures will be taken by the CAC needs to be further observed.

APPs supervision regarding unlawfully collection and use of PI is expected to continue by the CAC, MIIT and competent authorities and the examined Apps may also confront with examination back again. And the supervision content may expand to pop-ups information and other matters influencing user experience in Apps.

Algorithm governance is expected to accelerate, especially to implement the requirements of the *Administrative Provisions on Algorithm Recommendation for Internet Information Services* and *the Administrative Provisions on Deep Synthesis for Internet Information Services*. The Algorithm filing system has been opened and four batches of filing information has been published.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

The CSL, the DSL and the PIPL altogether have established the fundamentals for cybersecurity and data protection regulation in China. China has initiated the first amendment procedure of CSL which was enforced in 2017, in order to adapt to the new legislations and establish a coherent legal liability system. And it is well expected that key supplemental implementing measures such as the RANDS to be officially released. Based on the three fundamental laws, the RANDS on one hand further refines the regulatory mechanism regarding Important Data protection, and the other hand it adds some new requirements which to some extent proposes some legislative changes.

In addition, it's also expected that the CAC and relevant authorities to intensively launch implementing rules and measures, particularly pertaining to supervision of internet platform services, algorithmic governance, financial data, automotive data, etc.

Contributors

Mr. Chen Jihong
Senior Equity Partner and Head of IP Department

chenjihong@zhonglun.com