China: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection & cyber security laws and regulations that may occur in China.

For a full list of jurisdictional Q&As visit here
1. Please provide an overview of the legal and regulatory framework governing privacy 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)?

Coming into effect on 1 June 2017, the Cyber Security Law of the People’s Republic of China (the “CSL”) forms the backbone of cybersecurity and data privacy protection. Since the CSL does not stipulate comprehensive rules, China’s data and privacy framework appears to be a patchwork with textures of various laws, measures, and sector-specific regulations, as well as national standards. The CSL imposes different data privacy obligations on network operators and critical information infrastructure operators (CIIOs). Network operators encompass virtually all companies involved in any kind of Internet-based services (CSL. Art. 76. A Network Operator (NO) refers to the owner or manager of a network or the provider of a network service). Among them, CIIOs are the network operator of the critical information infrastructure in important industries that, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people’s livelihood and public interests (CSL. Art. 31. CIIO refers to the network operator of the critical information infrastructure in important industries and sectors such as public communications, information service, energy, transport, water conservancy, finance, public service and e-government, and other critical information infrastructure that, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people’s livelihood and public interests).

The non-binding national standard of Information Security Technology – Personal Information Security Specification (the “PI Specification”) (The first official version was GB/T 35273-2017 and the second version is GB/T 35273-2020, and the second version will become effective as of 1 October 2020 in replace of the first version. All citations here are made according to the GB/T 35273-2020) illustrates the obligations of privacy protection in detail. Drafted with reference to the European General Data Protection Regulations (GDPR), the PI Specification adopts some definitions in the GDPR, e.g., the definitions of personal information controller and personal information processor mirror the definitions of data controller and data processor under the GDPR. The PI Specification plays a key role in personal information protection and has been cited by courts and enforcement authority. An increasing number of companies in the market also tend to refer to the PI Specification as the standard when conducting self-auditing of their personal information protection.

For certain types of information in special sectors, the authorities have enacted special regulations or standards. Take the financial sector as an example, the People’s bank of China, the central bank of China responsible for regulation of financial institutions in mainland China, has issued rules to protect personal financial information even prior to the legislation of the CSL, such as the Notice from the People’s Bank of China on Further Proper Protection of Personal Financial Information of Customers by Financial Institutions in 2011.

The enforcement authorities in this field at least include the Cyberspace Administration of China (“CAC”), the Ministry of Industry and Information Technology (MIIT), the Ministry of
Public Security (MPS), State Administration for Market Regulation (SAMR) and industry regulators.

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

There is no binding law require data controller/processor to register privacy mechanism, while if they fall into the scope of Network Operator under the CSL, they shall comply with the Multi-Level Protection Scheme (“MLPS”) requirements.

China has issued a draft Administrative Measure on Data Security requiring network operators to make a filing with the local cyberspace administration when they collect important data or sensitive personal information for the purposes of business operations (Administrative Measures on Data Security (Draft) Art. 18). As a regional response, Tianjin has issued an interim measure with requiring the data operator to make a filing on its collection and use of personal information (Tianjin Interim Administrative Measures on Data Security. Art. 11).

3. **How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

Personal information under the CSL is defined as the information that is recorded in electronic or any other form and used alone or in combination with other information to recognize the identity of a natural person. The PI Specification expands the definition of “personal information” to include the information that reflects a person’s activities (PI Specification. 3.1.).

Sensitive personal information is defined in the PI Specification as information that, if leaked, illegally provided or used without authorization, will endanger human rights and property interest, or cause damages to reputation, physical and mental health, or lead to discriminatory treatment (PI Specification. 3.2.).

Another key concept is the “important data” that is defined as data closely related to national security, economic development, and social and public interests (Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft). Art. 17 (stipulating that specific scope of “important data” needs to refer to relevant national standards and important data identification guidelines for its specific scope. The official national standards and guidelines have not come out yet)).

4. **What are the principles related to, the general processing of personal data or PII?**

The CSL stipulates that Network operators shall abide by the “lawful, justifiable and necessary” principles to collect and use personal information. The PI Specification sets out
following seven basic principles for personal information controllers/processors to follow when carrying out personal information processing activities (PI Specification. 4.):

1. Accountability. A personal information controller shall adopt technology and other necessary measures to ensure the security of personal information and be accountable for any damages to the legal rights and interests of personal information subjects caused by its personal information processing activities.

2. Purpose Specification. A personal information controller shall have clear and specific purposes for processing personal information.

3. Solicitation for Consent. A personal information controller shall explicitly specify the purpose, methods, scope and rules in processing personal information, and seek the authorization of the personal information subject.

4. Proportionality (minimum necessary). A personal information controller shall only retain the minimum amount of personal information necessary to achieve the purpose(s) authorized by the personal information subject and shall delete the personal information once it fulfills the purpose(s).

5. Transparency. A personal information controller shall, unambiguously and in plain language and reasonable manner, disclose the scope, purpose(s), rules of its personal information processing to the public.

6. Security. A personal information controller shall be equipped with security capability in line with the security risk it faces and take adequate management and technological measures to safeguard the confidentiality, integrity and availability of the personal information.

7. Subject Participation. A personal information controller shall provide the personal information subject with means to access, correct and delete his or her personal information, the method to withdraw his or her consent, cancel the count and the complaint means.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there rules relating to the form, content and administration of such consent?

Overall, a noticeable difference from GDPR is that the legal basis under the CSL is entirely consent-based. The CSL requires the network operator to expressly notify and obtain consent of the users if the products or services collect user information and comply with relevant laws and regulations governing personal information protection if personal information of users are involved (CSL. Art. 41). With a few exceptions listed in the PI specification (PI Specification. 5.6.) (discussed under Question 8), a network operator is required to inform the personal information subject of the purposes, means and scope of the collection and use of his or her personal information, and consent must be obtained prior to such collection (CSL. Art. 41. PI Specification. 5.4 a)).

The PI Specification aims to guarantee the PI subject’s autonomy on personal information processing by requiring the controller to permit the subjects to make free choice when there’re multiple functions (PI Specification. 5.3). Annex C of the PI Specification provides
detailed means for realizing the autonomy of the personal information subjects. Particularly, before the extended business function is used for the first time, the personal information subject shall be informed of the extended business function and the circumstance of personal information collection via popups, text descriptions, checking boxes, prompts, etc., and allow the personal information subject to select and give consent to the extended business function one by one (PI Specification. Annex C. 4 a)).

In addition, before collecting biometric information (discussed under Question 19), the personal information controller should separately inform the personal information subject of the purpose, method and scope of collecting and using personal biometric information, as well as the retention period and other rules, and obtain the explicit consent of the personal information subject (PI Specification. 5.4 c)).

Any processing of personal information thereafter must be carried out within the scope of the consent. A renewed consent is required when the processing exceeds the original scope of consent (PI Specification. 7.3 a)).

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

Explicit consent from the personal information subject is required for processing sensitive personal information (PI Specification. 5.4 b)). “Explicit consent” is defined as express consent given in writing or orally or through other affirmative actions freely made by personal information subjects (PI Specification. 3.6). A personal information controller is required to ensure that the explicit consent of the personal information subject is his/her autonomous, specific and clear willingness given after being fully informed (PI Specification. 5.4 b)).

There might be requirements on data which are prohibited from collection in special industry sectors. For example, credit investigation organizations shall be prohibited from collecting personal information pertaining to religion, gene, fingerprint, blood type, diseases and medical history and other personal information for which collection is prohibited by laws and administrative regulations (Administrative Regulations on Credit Investigation Industry. Art.14).

7. How do the laws in your jurisdiction address children’s personal data or PII?

Personal information of person aged 14 or under are child’s personal information and is classified into sensitive personal information (PI Specification. 3.2). Before collecting personal information of minors (eighteen is the age of majority in China) aged 14 or older, it shall seek explicit consent from the minors or their guardians; where the minors are aged under 14, it shall seek explicit consent from their guardians (PI Specification. 5.5 c)). Activities related to children’s personal information are also subject to the special protection of the Provisions on the Cyber Protection of Children’s Personal Information.
8. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

The PI Specification elaborates following exceptions to obtaining consent of the personal information subject for the collection and use of personal information (PI Specification. 5):

1. those related to the fulfillment of personal information controllers’ obligations imposed by laws and regulations;
2. those directly related national security and national defense;
3. those directly related to public safety, public health, and significant public interests;
4. those directly related to criminal investigation, prosecution, trial, and judgment enforcement, etc.;
5. when safeguarding the major lawful rights and interests such as life and property of personal information subjects or other persons, and it is difficult to obtain the authorized consent of the personal information subject;
6. when the personal information subject voluntarily opened the collected personal information to the general public;
7. when necessary to sign and perform a contract according to the personal information subject’s request (note however, the main function of the personal information protection policy is to disclose the scope and rules of the collection and use of personal information by the controller of personal information, which should not be treated as contract in this context);
8. when the personal information is collected from legitimate public information channels, such as the legitimate news reports and open government information;
9. when necessary to maintain the safe and stable operation of the provided products or services, such as to detect and handle product or service malfunctions;
10. when necessary for the personal information controller, as a news agency, to make legal news reports;
11. when necessary for the personal information controller, as an academic research institute, to conduct statistical or academic research in the public interest, which also has de-identified the personal information when providing academic research or results externally.

Exceptions of 1-4, and 8 above also constitute the exceptions to the general rule of no sharing, transfer or public disclosure (PI Specification. 9.5). Exceptions to the rights of personal information subjects are discussed under Question 27.

9. **Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.**

No provision in current binding data and privacy laws has imposed any requirements of privacy by design/default, albeit they are helpful for fulfilling the obligations imposed by the CSL. A similar system is indicated in the PI Specification where personal information controllers are recommended to comply with national standards (including Information...
10. **Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.**

Under the CSL, network operators are required to record network operation and cybersecurity events and maintain the cyber-related logs for no less than six months (CSL. Art. 21.3). Since the CSL is a binding law and the enforcement authorities have published sanctions on those who failed to maintain the logs, most business entities follow such requirement and keep log records for no less than six months.

Personal information controller is required to keep records in certain circumstances under the PI Specification. A personal information controller should correctly record and retain the arrangement for delegation of the personal information processing (PI Specification. 9.1 e)). In case of sharing and transferring personal information for reasons other than merger, acquisition and restructuring, it is required to correctly record and retain the circumstances of sharing and transfer of personal information, including the dates of sharing and transfer, the scale, the purposes, the basic information of the recipient, etc (PI Specification. 9.2 e)). In addition, internal records should be retained where it is truly necessary to allow specific personnel to exceed their privileges to process personal information (PI Specification. 7.1 d)).

The PI Specification also recommends controllers to establish, maintain and update records of personal information processing activities. Such records of the collection and use of personal information processing activities may include the following (PI Specification 11.3):

1. the type, quantity and source of the personal information involved.
2. the processing purpose and usage scenario.
3. information systems, organizations or personnel related to all aspects of personal information processing activities.

11. **When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?**

Current laws and regulations in China do not have prior consultation requirement like GDPR.

12. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

A CIO shall conduct security assessment where the personal information and important data
generated from its operation in China need to be provided abroad for business reasons (CSL. Art. 37). A CIIIO shall also by itself or entrust a cybersecurity service provider in conducting examination and assessment of its cybersecurity and potential risks at least once a year, and submit such results together with improvement measures to the competent authorities (CSL. Art. 38).

Personal information controllers are advised by the PI Specification to establish a personal information security impact assessment system to evaluate the security risk brought to personal information processing activities (PI Specification. 10.2 a)). The PI Specification requires personal information controllers to carry out risk assessments in some specific scenarios, such as when ensuring that the delegated processor has sufficient data security capabilities and provide sufficient security safeguards (PI Specification. 9.1 b)), when sharing and transferring personal information for reasons other than merger, acquisition and restructuring, where the personal information has to be publicly disclosed as authorized by the law or for reasonable cause (PI Specification. 9.2 a)). Prior to the release of a product or service, or when there are major changes in business functions, a personal information security impact assessment should also be performed (PI Specification. 11.4 c)). Additionally, when laws and regulations have new requirements, or when a major change occurs to the business model, information system, or operational environment, or when a major personal information security incident transpires, a new personal information security impact assessment should be conducted (PI Specification. 11.4 d)).

Personal information security impact assessment mainly aims at evaluating whether processing activities obey the basic principles of personal information security and assess the impact of personal information processing on the lawful rights and interests of PI subject (PI Specification. 11.4 b)). In carrying out the assessment, business find it helpful to refer to the non-binding draft guide named Information Security Technology – Security Impact Assessment Guide of Personal Information (the “PIA Guide”). The PIA Guide provides details to the assessment regarding who should initiate, how to prepare and what factors should be considered and how to balance the factors (PIA Guide. 4.4, 5.2, 5.4-5.6, 6.).

After the assessment, the personal information controller is required to formulate a personal information security impact assessment report, and take measures to protect the personal information subject to reduce the risk to an acceptable level (PI Specification. 11.4 e)). The personal information controller is also required to retain the personal information security impact assessment report properly to ensure that it can be consulted by relevant parties and disclosed to the public in an appropriate form (PI Specification. 11.4 f)).

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

The CSL requires network operators to appoint personnel responsible for cybersecurity (CSL. Art. 21). Provisions on the Cyber Protection of Children’s Personal Information also requires
the network operator to designate persons to take charge of the protection of children’s personal information (Provisions on the Cyber Protection of Children’s Personal Information. Art.).

Organizational measures in the PI Specification also advise a personal information controller to appoint a head in charge of personal information protection and an agency in charge of personal information protection (PI Specification. 11.1 b)). If an organization (1) has more than 200 personnel and its main business involves processing personal information; or (2) processes or is expected to process the personal information of more than 1 million people within 12 months; or (3) processes sensitive personal information of more than 100,000 people, it should establish a department with designated staff in charge of personal information security (PI Specification. 11.1 c)). Distinguished from the DPO under the GDPR, the person in charge of personal information protection is less independent as he or she would be directly responsible for personal information security (PI Specification. 11.1 d) 1).

14. **Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

The CSL stipulates that Network operators shall abide by the “lawful, justifiable and necessary” principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected (CSL. Art. 4). The PI specification requires personal information controllers to inform the personal information subject of the rules regarding the purpose, method and scope of collecting and using personal information and obtain the authorized consent of the personal information subject (PI Specification. 5.4 a).

Personal information protection policy (aka “privacy policy”) is the common form of privacy notice. The PI Specification requires personal information controllers to establish personal information protection policy (PI Specification. 5.5 a)) and promptly send notification to the information if the personal information protection policy is updated (PI Specification. 5.5 f)).

15. **Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)**

The CSL does not specify the distinction between the controllers and the processors. However, obligations are placed on controllers as well as processors yet with different weight by the PI Specification.

Personal information controllers themselves face heavier burden in taking organizational measures and technical measures for delegated processing. The PI Specification also lays out
a number of requirements for the processors to follow (PI Specification. 9.1 c)): (1) process the personal information strictly in accordance with the instructions of the personal information controller. If the delegated processor cannot process the personal information according to the requirements of the personal information controller due to special reasons, the delegated processor shall promptly inform the personal information controller; (2) obtain the authorization of the personal information controller in advance if the delegated processor needs to redelegate the processing; (3) assist the personal information controller in responding to the requests from the personal information subject; (4) promptly inform the personal information controller if the delegated processor cannot guarantee a sufficient level of data security protection or encounters a safety incident during the processing of personal information; (5) no longer retain the personal information once the delegation relationship terminates (PI Specification. 9.1 c)).

16. **Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?**

The PI Specification requires the personal information controller to supervise the processor in the manners including but not limited to establish the processor’s responsibilities and duties through contract and carry out an audit of the processor (PI Specification. 9.1 d)). It also requires the personal information controller to carry out a personal information security impact assessment, ensuring that the processor has met data security capabilities requirement and provides sufficient security safeguards (PI Specification. 9.1 b)). If the controller learns or finds that the processor has not handled the personal information in accordance with the instructions of the controller or failed to effectively fulfil the personal information security protection responsibility, the controller shall immediately request the processor to cease the relevant activity, and take or require the processor to remediate. Measures (such as changing passwords, revoking permissions, disconnecting network connections, etc.) should be adopted to control or eliminate security risks to personal information. If necessary, the controller of personal information shall terminate the business relationship with the processor and require the processor to delete the personal information obtained from the controller of the personal information in a timely manner (PI Specification. 9.1 f)).

Besides, there might be stricter requirements in special sectors. Processing of personal financial information with higher sensitivity like user’s authentication information(C3) and supplementary information for authentication in C2, could not be delegated to third party (Personal Financial Information Protection Technical Specification. 6.1.4.4).

17. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms**
defined and what restrictions are imposed, if any?

Under CSL regime, tracking technologies like cookies are not prohibited, while cookies are usually regarded as personal information and the collection of which shall comply with personal information requirements.

The PI Specification recommends limited personalized display (PI Specification. 7.2) and user profiling (PI Specification. 7.4). It is “direct user profiling” when the personal information of a specific natural person is directly used to create a unique model of the natural person’s characteristics (PI Specification. 3.8). Except for realizing the purpose authorized by the personal information subject, clear personal identity should be avoided when using personal information to avoid pinpointing specific individuals. For example, in order to accurately evaluate personal credit status, direct user profiling could be used, and indirect user portraits should be used for commercial advertising purposes (PI Specification. 7.4 c)). Where personalized display is used in the process of providing business functions to personal information subjects, the content of personalized display and non-personalized display shall be distinguished significantly (PI Specification. 7.5 a)). Where personalized display is used in the process of providing business functions to personal information subjects, it is advisable to establish an independent control mechanism of the personal information subject on the personal information (such as labels, image dimensions, etc.) on which the personalized display relies, to ensure that the personal information subject is able to adjust the relevancy of the personalized display (PI Specification. 7.5 d)).

In the E-commerce context, when displaying search results of commodities or services to consumers according to their interests, preferences, consumption habits and other personal characteristics, an e-commerce operator shall also provide consumers with options irrelevant to their personal characteristics, and respect and equally safeguard the lawful rights and interests of consumers (E-commerce Law. Art. 18.; PI Specification. 7.5 b)).

Where personalized display is used in the process of pushing news information services to personal information subjects, they should (PI Specification. 7.5 c)):

1. Provide simple and intuitive options for the personal information subject to deactivate or close the personalized display mode;
2. When the personal information subject chooses to deactivate or close the personalized display mode, the personal information subject is provided with the option to delete or anonymize the personal information based on the targeted pushing activity.

Please describe any laws in your jurisdiction addressing 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 (the “Advertising Law”) is the fundamental law that regulates advertising. Depending on the direct marketing means –
email, telephone call, SMS, or pop-up ad on websites – statutes and regulations on particular means, such as the Interim Measures for Administration of Internet Advertising, Administrative Provisions on Short Message Services, may apply. In terms of email marketing, the sender shall obtain consent or request of the recipient and the sender shall also disclose its true identity, contact details and the opt-out method in such advertisements distributed via electronic means (Advertising Law. Arts. 43 & 44). The PI Specification also requires the personal information controller to ensure that the personal information subject have the right to refuse to receive commercial advertisements based on his/her personal information (PI Specification. 8.4 b)).

19. **Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these 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. Biometric information falls into the category of sensitive personal information. Before collecting biometric information, the personal information controller should separately inform the personal information subject of the purpose, method and scope of collecting and using personal biometric information, as well as the retention period and other rules, and obtain the explicit consent of the personal information subject (PI Specification. 5.4 c))

Generally, original biometric information (such as samples, images, etc.) should not be stored. Measures that can be taken include, but are not limited to: (1) Only summarized information of biometric information is stored. (2) Use biometric information directly in the collection terminal to implement functions such as identity recognition and authentication. (3) After using face recognition features, fingerprints, palm prints, iris, etc., to implement identity recognition, authentication and other functions, delete the original image that can extract biometric information (PI Specification. 6.3 c)). Where biometric information is necessary to be stored, it should be stored separately from personally identifiable information (PI Specification. 6.3 b).

Similarly, biometric information should not be shared or transferred in general. If it is necessary to share or transfer due to business needs, the individual information subject should be informed of the purpose, the type of personal biometric information involved, the specific identity of the recipient, and the data security capabilities, etc., and obtain the explicit consent of the personal information subject (PI Specification. 9.2 i)).

In Addition, the draft of the national standard for Biometric Information Protection also provides guidance for the processing of biometric information.

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

Under the CSL, CIIOs shall store within the territory of the People’s Republic of China personal information and important data collected and generated during its operation within the territory of the People’s Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail (CSL. Art. 37).

Under the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps, a valuable reference released by the authorized enforcement agency, the storage territory (domestic or foreign) of personal information shall be clearly indicated in privacy policies (Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps. Assessment Key 10). If provision of personal information overseas is involved, the types of personal information provided overseas shall be listed item by item and clearly marked (such as in bold fonts, star asterisks, underlines, italics, colors, etc.) in private policies (Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps. Assessment Key 12).

Legislation or regulations on the transfer of personal information outside the People’s Republic of China has not been officially published. The Measures on Security Assessment for Cross-border Transfer of Personal Information and Important Data (Exposure Draft) were first released in April 2017 (the “Former Measures”). On 13 June 2019, the CAC released the new draft of Measures on Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft) (the “New Measures”).

The New Measures center on personal information and remove the rules on transferring “important data” overseas set out in the Former Measures. The New Measures require all network operators to apply to the local cyberspace administrations at the provincial level for security assessment before the cross-border transfer of personal information. Meanwhile, network operators shall provide an application form, the contracts signed between network operators and data receivers; an analysis report on the security risks for the cross-border transfer of personal information and security measures; and other materials required (if any) for security assessment (New Measures. Art. 3). Besides, network operators shall file the related record regarding the cross-border transfer of personal information and contract performance of that year with the Cyberspace Administration Agency of the local province (New Measures. Art. 9). Network operators are also required to report to the Cyberspace Administration Agency of the local province upon comparatively significant data security incident (New Measures. Art. 9).

21. **What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?**
Under the CSL, China adopts the MLPS, under which network operators are required to perform the following obligations of security protection to ensure that the network is free from interference, disruption or unauthorized access, and prevent network data from being disclosed, stolen or tampered with (CSL. Art. 21).

In particular, for personal information, network operators shall keep the user information that they have collected in strict confidence and shall establish and improve their user information protection system (CSL. Art. 40). Network operators shall take technical and other necessary measures to ensure the security of personal information it collects, and to protect such information from disclosure, damage or loss (CSL. Art. 42).

Under the PI Specification, personal information controllers should establish appropriate data security capabilities, implement necessary managerial and technical measures, and prevent personal information from leakage, damage and loss (PI Specification. 11.5). Security measures such as encryption should be taken for transferring and storing sensitive personal information (PI Specification. 6.3 a)).

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?

“Cybersecurity incidents” is defined by the National Cybersecurity Incident Response Plan, one of the corresponding regulations of the CSL, as the incidents that (1) are caused by man-made reasons, defects or malfunctions of hardware and software, or natural disasters, (2) cause damage to networks, information systems or the data involved therein, and (3) cause negative effects to the society (National Cybersecurity Incident Response Plan. Art. 1.3). Cybersecurity incidents can be categorized into harmful program incidents, cyber-attack incidents, information or data breach incidents, information or content security incidents, device and equipment malfunctions, disaster incidents and other incidents. Cybersecurity incidents are divided into four levels, i.e., extraordinarily significant, significant, relatively significant and general. The factors deciding the level of a cybersecurity incident include (1) severity of the damage 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 (National Cybersecurity Incident Response Plan. Art. 1.4).

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

The CSL imposes higher obligations on CIIOs, and provides a special protection scheme in China on critical information infrastructure and the corresponding protection principles. However, no regulation on the identification standards, scopes or implementing rules of administration has been officially published yet. Information infrastructure – in important
industries and sectors such as public communications, information service, energy, transport, water conservancy, finance, public service and e-government – might fall within the scope of such regulation. A critical information infrastructure 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 (CSL. Art. 33). In addition to those security obligation imposed on network operators, CIIOs shall also fulfil stricter obligations of security protection (CSL. Art. 34):

In certain special sectors, there are specific security requirements. For example, in the financial sector, the Administrative Regulations on Financial Information Services issued by the CAC regulate the financial information service (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) providers and require them to take affirmative organizational measures (Administrative Regulations on Financial Information Services. Arts. 5 & 7) and appropriate technical measures (Administrative Regulations on Financial Information Services. Arts. 6 & 9). 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 Articles 13 to 15, covering both organizational and technical (Provisions on Protecting the Personal Information of Telecommunications and Internet Users. Arts. 13-15).

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

Network operators are required by the CSL to report the incident that threatens cybersecurity to competent authority in accordance with regulations and build up incident response plan (CSL. Art.25). In case of disclosure, damage or loss of, or possible disclosure, damage or loss of personal information, the network operator shall take immediate remedies, notify the users in accordance with the relevant provisions, and report to competent authority (CSL. Art.42).

The PI Specification further illustrates the circumstances and content of such reporting. After a personal information security incident occurs, the personal information controller should, among other things, report in a timely manner according to provisions in the National Cybersecurity Incident Response Plan. The content of the report should include but not be limited to: type, quantity, content, and nature of PI subject; possible impact of the incident; measures that have been or will be adopted; and contact information of relevant personnel handling the incident (PI Specification. 10.1 c) 3)). Where the personal information breach may cause serious harm to the legitimate rights and interests of the personal information subject, such as the leakage of sensitive personal information, the personal information
controller should inform that personal information subject (PI Specification. 10.1 c) 4). The affected individuals should be informed of the incident in a timely manner by mail, letter, phone, push notification, etc. When it is difficult to inform the subjects of personal information one by one, a reasonable and effective way should be adopted to issue warning information related to the public (PI Specification. 10.2 a). The content of the notification shall include, but is not limited to: 1) the content and impact of security incidents; 2) disposal measures taken or to be taken; 3) suggestions for the personal information subject to autonomously prevent and reduce risks; 4) remedial measures provided for personal information subjects; 5) contact information of the person in charge of personal information protection and the personal information protection agency (PI Specification. 10.2 b)).

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

Under the CSL, the State shall take necessary measures to impose punishments on unlawful and criminal network activities according to the laws, and to maintain the security and order of cyberspace (CSL. Art. 5). The Criminal Law of the People’s Republic of China has criminalized the ‘rejection to perform security management obligations for information network’, the ‘unlawful use of information network’, the ‘assistance in criminal activities committed through information networks’ and the ‘fabrication and intentional spread of false information (including via the information networks)’ (Criminal Law. Arts. 286.1, 287.1, 287.2, and 291.1). For the purpose of punishing crimes such as refusing to fulfil the obligation of managing the security of information networks, illegally using information networks and assisting in criminal activities committed through information networks and maintain the normal network order, the Supreme People’s Court and the Supreme People’s Procuratorate jointly issued the Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Illegal Use of Information Networks and Assistance in Criminal Activities Committed through Information Networks.

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

The enforcement authorities in this field at least include the CAC, the MIIT, the MPS and industry regulators. According to Article 8 of the CSL, the CAC is in charge of overall planning with regard to data protection and privacy, and co-ordinates the competent authorities. The MIIT, MPS, SAMR, and industrial regulators are in charge of law enforcement in their respective sectors.

27. Do the 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 the rights, how they are exercised, what exceptions exist and any other relevant details.

Article 43 of the CSL entitles the individuals to require a network operator to delete his or
her personal information if he or she founds that collection and use of such information by
such operator violate the laws, administrative regulations or the agreement by and between
such operator and him or her; and is entitled to require any network operator to make
corrections if he or she founds errors in such information collected and stored by such
operator. Such operator shall take measures to delete the information or correct the error.

Laws and regulations in different sectors also contain provisions in protecting data subjects’
rights. The E-commerce Law of the People’s Republic of China (the “E-commerce Law”)
requires E-commerce business operators to clearly state the methods and procedures for
access, correction and deletion of user information as well as account cancellation (E-
commerce Law. Art. 24.). Article 26 of the Law on the Protection of Rights and Interests of
Consumers (Revised in 2013) (the “Consumer Protection Law”) also provides that business
operators shall not impose unfair and unreasonable provisions on consumers such as
elimination or restriction of consumer rights.

The PI Specification provides and describes in detail the personal information subjects’ rights
of access, rectification, deletion, withdrawal of consent, account cancellation, obtaining
copies of personal information, limitation on automated decision-making (PI Specification.
8.1-8.6). In addition, after accepting the request to cancel the account, if manual processing
is required, the verification and processing shall be completed within the promised time limit
(not exceeding 15 working days). A note to the right to access is that when a personal
information subject requests access to personal information that he or she did not voluntarily
provided, personal information controllers can evaluate the request, taking into account the
risk or harm to the subject’s lawful rights and interests that could arise from not responding
to the request, technical feasibility, cost, and other factors in carrying out the request (PI
Specification. 8.1). As for the right to withdrawal, the withdrawal of consent does not affect
the lawfulness of processing based on consent before its withdrawal (PI Specification. 8.4).

In addition, the right to PI copies under the Chinese data protection regime is not the same
as the portability rights under the GDPR where the latter among others includes the right to
request data transfer from one data controller to the other. The right to deletion under the
CSL regime is different from the right to be forgotten under the GDPR. The legal basis for
exercising the right to deletion includes illegal acts or violation of the agreement. Yet the
right to be forgotten provides for a wider range of legal bases for data subjects to demand
deletion.

Exceptions under the PI Specification that the personal information controller may not
respond to the rights of personal subjects include (PI Specification. 8.7 e)):

1. those related to the fulfilment of personal information controllers’ obligations imposed by
laws and regulations;
2. those directly related national security and national defense;
3. those directly related to public safety, public health, and significant public interests;
4. those directly related to criminal investigation, prosecution, trial, and judgment
enforcement, etc.;
5. where the personal information controller has sufficient evidence to show that the personal information subject is subjectively malicious or abuses his/her rights;
6. when safeguarding the major lawful rights and interests such as life and property of personal information subjects or other persons, and it is difficult to obtain the authorized consent of the personal information subject;
7. where responding to the request of the personal information subject will cause serious damage to the legitimate rights and interests of the personal information subject or other individuals and organizations;
8. where trade secrets are involved;

Even under such exceptions, however, the personal information controller should inform the personal information subject of the reason for the decision and provide the personal information subject with a channel for making complaints (PI Specification. 8.7 f)).

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

Affected individuals may also bring tort claims before courts. Legal bases for an individual to initiate private litigation include the General Rules of the Civil Law, Tort Liability Law, Consumer Protection Law, the CSL and the PI Specification. At the same time, individuals could make complaints to the authorities, which might initiate an investigation against the business.

29. **Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?**

Since it is a tort claim, the rules of actual damages and injury of feelings in the General Rules of the Civil law the People’s Republic of China (General Rules of the Civil Law of the People’s Republic of China. Art. 111. The personal information of a natural person shall be protected by the law. Any organization or individual shall legally obtain the personal information of others when necessary and ensure the safety of such personal information, and shall not illegally collect, use, process or transmit the personal information of others, or illegally buy or sell, provide or make public the personal information of others) of and the Tort Law of the People’s Republic of China may apply (As the CSL has been implemented since 1 June 2017, it is hard to ascertain the awarded damages from limited private civil lawsuits).

30. **How are the laws governing privacy and data protection enforced?**

China witnessed tightening law enforcement in privacy and data protection in recent years. In general, most cases or proceedings in privacy and data protection field are administrative investigation and punishment initiated and imposed by government authorities. Meanwhile, the CSL and the Consumer Protection Law are the two fundamental legal basis the authorities refer to in regulating and issuing punishment. Mobile Applications, the most
popular way for business to collect personal information, has been put spotlight on by the enforcement authorities throughout these years. In January 2019, the Office of CAC, MIIT, MPS, and SAMR jointly issued the Announcement of Launching Special Crackdown Against Illegal Collection and Use of Personal Information by Apps. To implement the Announcement, a series of standards have been issued, including the Self-assessment Guide for Illegal Collection and Use of Personal Information through Apps, Notice on Promulgation of the Method for Identifying the Illegal Collection and Use of Personal Information by Apps. These guidance and methods have been used as tools for App operators to conduct self-inspection as well as for law enforcement department to determine unlawful privacy and data protection activities. Besides, the criminal enforcement has been tightened up as well.

31. **What is the range of fines and penalties for violation of these laws?**

Depending on the violation, different sanctions and penalties may be imposed by the CSL (CSL. Arts. 59-75). For example, none-compliance with the personal information protection related provisions in the CSL may result in order to take rectification measures, warning, confiscation of illegal earnings, fines, or a combination thereof. The fine is more than the illegal earnings but less than ten times of the illegal earnings. In the event that there are no illegal earnings, the fine is no more than 1 million Chinese Yuan. The directly responsible person may face a fine ranging from 10,000 to 100,000 Chinese Yuan. In case of severe violation, the competent authority may order suspension of related business, winding up for rectification, shutdown of website, and revocation of business license of such operator or provider (CSL. Art. 6).

As for the criminal liability, the basic requirement is that, when persons sell or provide personal information of citizens to others in violation of relevant national provisions, and the circumstances are serious, the sentence can be fixed-term imprisonment of no more than 3 years or criminal detention, in combination of fines, or the sentence can be fines alone; if the circumstances are particularly serious, the sentence shall be fixed-term imprisonment from 3 to 7 years, in combination of fines (Criminal Law. Art. 253).

32. **Can personal data or PII owners/controller 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. Unless it is required by any relevant laws to exhaust administrative reconsideration before seeking judicial review, it/he may also initiate an action to the people’s court directly (Administrative Procedure Law of the People’s Republic of China (Amended in 2017). Art. 4).