International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2022

Ninth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

China


Susan Ning


Han Wu

King & Wood Mallesons

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There are three major principal data protection laws, i.e., the Cybersecurity Law (the "**CSL**"), the Personal Information Protection Law (the "**PIPL**") and the Data Security Law (the "**DSL**").

1.2 Is there any other general legislation that impacts data protection?

Yes. Both the general civil and criminal legislation in China provide requirements on data protection.

In particular, the Civil Code, which took effect on 1 January 2021, establishes the right to privacy and the principles of personal information protection. It mainly provides a definition of personal information and sets out basic requirements for personal information processing, the obligations on the personal information processors and the rights of individuals to their personal information. Most of the provisions in the Civil Code are restatements of requirements contained in the CSL. National Standards such as the Information Security Technology – Personal Data Security Specification (the "**Standard**") also have an impact on the authorities' enforcement on data protection practices.

The Criminal Law also sets forth offences relating to infringing personal data and privacy, e.g., the offence of infringing citizens' personal information in Article 253-(1), the offence of refusing to fulfil information network security responsibilities in Article 286-(1), and the offence of stealing, purchasing or illegally disclosing other people's credit card information in Article 177-(1). The Interpretation of Several Issues Regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information Handled by the Supreme People's Court and the Supreme People's Procuratorate issued in 2017 provides further explanation regarding the offences relating to infringing personal data and privacy.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. There are various pieces of sector-specific legislation that impact data protection, including but not limited to medical and health, telecommunications, e-commerce and automobiles. For example, the Commercial Bank Law requires banks to keep confidential on depositors' personal savings deposit businesses. The People's Bank of China ("the **PBOC**") has released the Implementing Measures of the People's Bank of China for Protection of Financial Consumers' Rights and Interests, which provide basic requirements on protection of financial information (including personal information) of individual customers. The Biosecurity Law and the Administrative Regulations on Human Genetic Resources set out requirements on processing of human resource information. The E-commerce Law restates the principle of personal information protection in the field of e-commerce industry. There are also various legal requirements on protection of personal information and data in automobile industry, such as the Several Provisions on Automotive Data Security Management (for Trial Implementation). Furthermore, the Provisions on Protecting the Personal Information of Telecommunications and Internet Users set out obligations of telecommunication and Internet information service providers.

1.4 What authority(ies) are responsible for data protection?

As for personal information protection, China has no single authority responsible for enforcing provisions.

The Cyberspace Administration of China (the "**CAC**") is responsible for coordinating the protection of personal information and relevant supervision and administration work, while other departments of the State Council, such as the Ministry of Industry and Information Technology (the "**MIIT**"), the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.

For example, the Ministry of Public Security (the "**MPS**") and its local branches are entitled to impose administrative penalties and are also in charge of criminal investigations against the unlawful obtaining, sale or disclosure of personal information.

The MIIT and its local branches are responsible for the supervision and administration of personal information in the telecommunications and Internet sector.

Also, the State Administration for Market Regulation (the "**SAMR**") and its local counterparts are responsible for the supervision and administration of personal information of consumers, pursuant to the Law on Protection of the Rights and Interests of Consumers.

There are also industrial-specific data protection requirements, which are mainly enforced by relevant industrial authorities. For example, the PBOC and the China Banking and Insurance Regulatory Commission promulgate and enforce legal requirements on the protection of personal financial information. The National Health Commission and Ministry of Science and Technology supervise the processing of medical and health data.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal data**"
  Pursuant to the PIPL, personal data/personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding information processed anonymously.
- "**Processing**"
  Pursuant to the PIPL, the processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.
- "**Controller**"
  The PIPL does not use the term "controller(s)" to refer to entities that hold or handle personal information. Instead, it names such entities as "personal information processors" considering their engagement in processing personal information. Pursuant to the PIPL, a personal information processor is defined as an organisation or individual that independently determines the purpose and method of the processing of personal information.
- "**Processor**"
  The PIPL does not define "processor" in the same way as under the General Data Protection Regulation ("the **GDPR**"). However, the PIPL sets out the scenario of entrusted processing of personal information, where a personal information processor may entrust an entity with such processing.
- "**Data subject**"
  The PIPL does not define "data subject". However, both the Civil Code and the PIPL provide that a natural person's personal information shall be protected by law. It is widely understood that a natural person/individual identified by the personal information shall be regarded as a data subject.
- "**Sensitive personal data**"
  Pursuant to the PIPL, sensitive personal data/sensitive personal information refers to personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts, as well as the personal information of minors under the age of 14.
- "**Data breach**"
  The CSL, PIPL and DSL do not define "data breach". The National Contingency Plan for Cyber Security Incidents issued by the CAC defines "Cybersecurity incidents", which refers to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. Cybersecurity incidents can be divided into hazardous programme incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents and other incidents.
- **Other key definitions**
  Under the PIPL:
  - "**De-identification**" refers to the process in which personal information is processed so that it is impossible to identify certain natural persons without the aid of additional information; and
  - "**Anonymisation**" refers to the process in which personal information is processed so that it is impossible to identify certain natural persons and cannot be recovered.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Under the CSL, relevant authorities are entitled to monitor, prevent and manage cybersecurity risks and threats from other jurisdictions. Pursuant to Article 50, if any information from other jurisdictions is found to be prohibited by law, the CAC and competent authorities may take measures to block the transmission of such information. Pursuant to Article 75, the law applies to an overseas institution, organisation or individual that engages in activity that also endangers Critical Information Infrastructure ("**CII**"). Further, companies operating under the offshore model but providing services to Chinese clients/users may also be subject to the personal data protection rules established by the CSL, especially those on the cross-border transfer of data. However, the law does not clearly specify how to realise the sanctions. As such, the extent to which these provisions will be enforced abroad against overseas companies remains unclear.

The PIPL provides similar rules to the GDPR regarding its jurisdiction over businesses located outside of China. Article 3 provides that the law shall apply to the processing of personal information of natural persons who are in China under any of the following circumstances, where the processing happens outside of China:

1) where the purpose is to provide domestic natural persons with products or services;
2) where the activities of domestic natural persons are analysed and evaluated; and
3) other circumstances as prescribed by laws and administrative regulations.

Furthermore, according to Article 42 of the PIPL, where an overseas organisation or individual engages in personal information processing activities that infringe upon the personal information rights and interests of citizens of the People's Republic of China or endanger the national security and public interests of the People's Republic of China, the CAC may include such organisation or individual in the list of subjects to whom provision of personal information is restricted or prohibited, announce the same, and take measures such as restricting or prohibiting provision of personal information to such organisation or individual.

The DSL also empowers relevant authorities with the power to investigate the liabilities of entities that process data outside of China that damages the national security, public interest or the legitimate rights and interests of citizens and organisations.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Article 41 of the CSL stipulates that network operators shall make public the rules for collecting and using personal data, and expressly notify the purpose, methods and scope of such collection and use. The same principle

has also been included in the PIPL. According to Article 7, the principles of openness and transparency shall be observed in the processing of personal information; the rules for the processing of personal information shall be publicly disclosed, and the purpose, manners and scope of processing shall be explicitly indicated.

- **Lawful basis for processing**
  Article 41 of the CSL and Article 1035 of the Civil Code require network operators to abide by the "lawful, justifiable and necessary" principles when collecting and using personal information. The PIPL similarly requires that the processing of personal information shall follow the principles of lawfulness, legitimacy, necessity and good faith, and processing personal information by misleading, fraud, coercion or otherwise is not permitted.
  Furthermore, Article 13 of the PIPL provides various legal grounds for processing of personal information, including:
  1) the consent of the individual concerned is obtained;
  2) it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resource management in accordance with the labour rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;
  3) it is necessary for the performance of statutory duties or statutory obligations;
  4) it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;
  5) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest;
  6) processing within a reasonable scope of personal information that is publicly disclosed in accordance with the PIPL; or
  7) other circumstances prescribed by laws and administrative regulations.
- **Purpose limitation**
  Article 41 of the CSL requires that network operators shall not collect any personal information that is not related to the services it provides. PIPL similarly requires that the processing of personal information shall be for a definite and reasonable purpose and be directly related to the purpose of processing.
- **Data minimisation**
  Article 6 of the PIPL provides that the processing of personal information shall be conducted in a way that minimises the impact on personal rights and interests, and shall be limited to the minimum scope for achieving the purpose of processing. It is prohibited to excessively collect personal information.
- **Proportionality**
  There is no explicit rule providing for a "proportionality principle" under the CSL or the PIPL, but the data minimisation principle under the PIPL is similar in essence to the "proportionality principle", emphasising "processing of personal data only within a proper and necessary scope", and "shall be conducted in a way that minimises the impact on personal rights and interests".
- **Retention**
  Pursuant to Article 19 of the PIPL, unless otherwise stipulated by laws and administrative regulations, the retention period of personal information shall be the minimum period necessary for achieving the purpose of processing.
- **Other key principles**
  - **Data quality and accuracy –** Article 8 of the PIPL provides that the quality of personal information shall be ensured in the processing of personal information to avoid the adverse impact on personal rights and interests caused by inaccurate or incomplete personal information.
  - **Accountability –** Article 9 of the PIPL requires a personal information processor to be responsible for its processing of personal information and take necessary measures to ensure the security of the personal information processed.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Both the Civil Code and the PIPL entitle an individual to consult or copy his/her personal information from a personal information processor.
- **Right to rectification of errors**
  The PIPL provides that where an individual finds that his/her personal information is inaccurate or incomplete, he/she is entitled to request the personal information processor to make corrections or supplements. The Civil Code and the CSL provide similar rules.
- **Right to deletion/right to be forgotten**
  The PIPL requires a personal information processor to delete personal information actively or under the request of relevant individuals in any of the following circumstances:
  1) where the purpose of handling has been achieved, it is impossible to achieve such purpose, or it is no longer necessary to achieve such purpose;
  2) where the personal information processor ceases to provide products or services, or the storage period has expired;
  3) where the individual withdraws his/her consent;
  4) where the personal information processor processes personal information in violation of laws, administrative regulations or the agreement; or
  5) other circumstances stipulated by laws and administrative regulations.
- **Right to object to processing**
  Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.
- **Right to restrict processing**
  Under the PIPL, a data subject has the right to restrict or refuse others to process his/her personal information.
- **Right to data portability**
  Pursuant to Article 45 of the PIPL, where an individual requests to transfer his/her personal information to a personal information processor designated by him/her, which meets the conditions stipulated by the CAC, the personal information processor shall provide a way for the transfer.
- **Right to withdraw consent**
  Article 15 of the PIPL provides that where the processing of personal information is based on the consent of the individual concerned, the individual is entitled to withdraw his/her consent. The personal information processor shall provide a convenient method for the individual to withdraw his/her consent.

- **Right to object to marketing**
  Section 8.4 of the Standard stipulates that data subjects have the right not to receive commercial advertisements that are based on their personal data. Furthermore, regarding marketing by means of automated decision-making, the PIPL requires the processor to provide convenient rejection ways to relevant individuals.
- **Right protecting against solely automated decision-making and profiling**
  The PIPL provides that where a processor makes use of personal information to make an automatic decision, it shall ensure the transparency of the decision-making and the fairness and impartiality of the results, and shall not impose unreasonable discriminatory treatment on individuals in respect of the transaction price and transaction conditions. In a scenario in which there is information pushing and commercial marketing to an individual through automated decision-making, the processor shall in parallel provide options that do not target the individual's personal characteristics, and provide convenient means of rejection to relevant individuals. On the other hand, an individual shall have the right to require the personal information processor to make an explanation and to reject such explanation only through automatic decision-making where such decision has a significant impact on an individual's rights and interests.
- **Right to complain to the relevant data protection authority(ies)**
  The right for individuals to complain to data protection authorities has been recognised in a number of pieces of legislation. For example, Section IX of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection provides that any organisation or individual has the right to report to the relevant authorities regarding the illegal or criminal conduct of stealing or otherwise unlawfully acquiring, selling or providing to others a citizen's personal electronic information. Further, the CSL provides in Article 14 that one could report acts that endanger network security to the CAC, telecom and public security authorities.
  Under the PIPL, any organisation or individual shall have the right to complain or report illegal personal information processing activities to the authorities performing duties of personal information protection.
- **Other key rights**
  The PIPL protects the rights of close relatives of the deceased. Where a natural person dies, his/her close relatives may, for the purpose of their own lawful and legitimate interests, exercise such rights as consulting, copying, correcting and deleting the relevant personal information of the deceased as prescribed in this chapter, unless otherwise arranged by the deceased prior to his/her death.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There are similar rules under the PIPL. Article 70 of the PIPL provides that where any personal information processor processes personal information in violation of this Law, which infringes upon the rights and interests of a large number of individuals, the People's Procuratorate, the consumer organisations specified by law and the organisations determined by the CAC may bring a lawsuit to a people's court.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Under the PIPL, personal information of children under the age of 14 shall be regarded as sensitive personal information, the processing of which shall be subject to additional legal requirements. Pursuant to Article 31 of the PIPL, processing personal information of children under the age of 14 requires the consent of the children's parents or other guardians, and specialised rules shall be formulated for such processing.

Besides, the CAC has promulgated a special regulation regarding the protection of children's personal information, i.e., the Provisions on the Cyber Protection of Children's Personal Information. Network operators that process children's personal information shall formulate special data protection rules and user agreements and designate persons as responsible for the protection of such information.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Under the CSL, PIPL and DSL, transferring personal information or important data abroad may trigger such obligation in certain circumstances. As for operators of CII ("**CIIOs**"), a security assessment shall be conducted pursuant to the measures developed by the CAC and/or competent departments of the State Council, if the personal information or important data generated or collected by them within the territory of China needs to be transferred abroad for business purposes. Personal information processors whose quantity of processing reaches that as prescribed by the CAC will also be subject to such obligation according to the PIPL. As for other personal information processors, there are some other ways provided by the PIPL to compliantly transfer personal information outside China, among which the processors can choose to pass the security assessment organised by the CAC.

According to the DSL, processors of important data shall, in accordance with the relevant provisions, carry out risk assessments on their data processing activities on a regular basis and submit a risk assessment report to the relevant competent authority. On an industrial-specific basis, the CAC has issued a regulation on the security protection of automotive data, in which the CAC requires that an automotive data processor shall conduct risk assessments and submit an assessment report to the cyberspace administration at provincial level and other relevant authorities for its processing of important data. Such processor is further required to submit its annual automotive data security management report to these authorities by December 15 of each year. Furthermore, the international transfer of important data by the processor shall also be subject to the assessment organised by the CAC and relevant authorities.

The CAC also sets out legal requirements on the application of algorithm recommendation technologies for provision of Internet information services, where an algorithm recommendation service provider with public opinion attribute or social mobilisation ability shall, within 10 working days from the date of provision of services, go through record-filing formalities.

Additionally, where the processing of data raises national security issues, such activities may further trigger a cybersecurity review. According to the Cybersecurity Review Measures released by the CAC and a number of other national departments, the purchase of network products and services by CIIOs and the data processing activities carried out by online platform operators, which affect or may affect national security, shall be notified to the relevant authorities for cybersecurity review. Online platform operator holding personal information of more than 1 million users shall also declare for cybersecurity review when they enter into an initial public offering ("**IPO**") in other countries.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

For the security assessment of international transfer of personal information and important data, according to relevant draft regulations, the notification is designed to be specific, covering various aspects such as legitimacy, fairness, necessity of the transfer, categories, quantity, sensitivity of the data, security risk, etc.

The report by automotive data processors is also required to be specific. Processors are requested to provide details of the processing activities, such as the type, scale, purpose, and necessity of the processing of automotive data, the measures for security protection and management of automotive data, provision of automotive data to third parties, data security incidents and the handling thereof, etc.

The filing of algorithms needs to be conducted via the Internet information service algorithm record-filing system operated by the relevant authorities, where detailed information such as the service provider's name, service form, application field, algorithm type, algorithm self-assessment report and content shall be provided.

The cybersecurity review is also conducted in a detailed manner. Relevant data processors need to file (including but not limited to) an assessment report analysing in detail the risk factors concerning national security.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

For international data transfer, according to relevant draft regulations, the assessment has a two-year period of validity. When such period expires, the assessment shall be renewed. Furthermore, during the two-year period, the assessment will need to be renewed if: (i) any change occurs to the purpose, method, scope, or type of the data to be transferred, or the use or method of data processing by the overseas recipient, or the period for overseas storage of personal information and important data is extended; (ii) there is any change in the legal environment of the country or region where the overseas recipient is located, any change in the actual control of the data processor or the overseas recipient, or any change in the contract between the data processor and the overseas recipient that may affect the security of the outbound data, or other circumstances affecting the security of outbound data; or (iii) there are other circumstances that have an impact on the security of data transfer.

For automotive data, each processor (who conducts important data processing) is required to file a report of its overall automotive data processing activities. Similarly, the filing of algorithms shall be conducted by each relevant service provider, and if any change occurs to the information filed, the service providers shall make modifications within 10 working days.

As for cybersecurity review, as mentioned above, the review process is initiated when a CIIO purchases network products and services that affect or may affect national security, or when an online platform operator's certain data processing activity affects or may affect national security, or when an online platform operator holding personal information of more than 1 million users enter into an IPO in other countries.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please refer to questions 7.1 and 7.3.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please refer to question 7.2.

7.6 What are the sanctions for failure to register/notify where required?

CIIOs that fail to notify their cross-border transfer of personal information and important data, according to the CSL, shall be warned and ordered by the competent authority to make rectifications, and shall be subject to confiscation of illegal earnings and a fine ranging from RMB 50,000 to RMB 500,000, and may be subject to a suspension of related business, winding up for rectification, shutdown of website, and revocation of business licence, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000. As for personal information processors, pursuant to the PIPL, the authorities may order them to make corrections, give a warning to them and confiscate their illegal gains. If they refuse to make corrections, a fine of not more than RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data processor failing to report may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes serious consequences

such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

With respect to any algorithm recommendation service provider with the attribute of public opinions or the ability to mobilise the public, who has obtained record-filing by concealing relevant information, providing false materials or other improper means, its record filing shall be revoked, a warning given, or a notice of criticism circulated; if the circumstances are serious, it shall be ordered to suspend information updating and impose a fine of not less than RMB 10,000 but not more than RMB 100,000.

CIIOs using products and/or services that have not undergone or have failed in the security review shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than one but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB 10,000 to RMB 100,000.

7.7 What is the fee per registration/notification (if applicable)?

Currently, it remains unclear. Normally, such notifications are free of charge.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please refer to questions 7.1 and 7.3.

7.9 Is any prior approval required from the data protection regulator?

For the international data transfers mentioned in question 7.1, it is widely recognised that prior approval is required, where applicable. As for important data processing, there is no requirement of prior approval in the DSL. The same goes with the filing of algorithms.

For cybersecurity review, it is understood that prior approval is needed.

7.10 Can the registration/notification be completed online?

The filing of algorithms is conducted online. It remains unclear whether other notifications can be completed online.

7.11 Is there a publicly available list of completed registrations/notifications?

Since the laws and regulations are newly issued, currently there is no public channel established to list completed notifications.

7.12 How long does a typical registration/notification process take?

For the security assessment of international data transfers, the draft regulations provide that the CAC shall complete a security assessment of outbound data within 45 working days commencing from the date of issuing the written notice of acceptance; if the circumstance is complex or supplementary materials are required, the said time limit may be extended appropriately, but generally shall not exceed 60 working days.

For the filing of algorithms, relevant authorities shall, within 30 working days upon receipt of the record filing materials submitted by the record-filing applicants, grant record-filing, issue record filing numbers and make public the record filing; if the materials are incomplete, record-filing shall not be granted, and the record filing applicant shall be notified, with reasons stated, within 30 working days.

The cybersecurity review follows a period of "30+15+15" working days for an ordinary review procedure. Where a special procedure is needed, the review shall generally be completed within 90 working days, and the time limit may be extended for complicated cases.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Under the PIPL, where the quantity of personal information processed reaches that specified by the CAC, the personal information processor shall designate a person in charge of personal information protection to be responsible for supervising the activities of processing of personal information and the adopted protection measures. Currently, the threshold is yet to be made public.

Under the DSL, processors of important data shall specify the person(s) responsible for data security and the management body, and implement the responsibility of data security protection.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Under the PIPL, the authorities may order the processor to make corrections, give a warning to it and confiscate its illegal gains. If it refuses to make corrections, a fine of not more than RMB 1 million shall be imposed; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the person directly in charge and other directly liable persons. Where the circumstances are serious, such processor may face a higher fine of not more than RMB 50 million or not more than 5% of its turnover of the previous year; the authorities may also order it to suspend relevant business or suspend business for rectification, and revoke the relevant business permit or business licence. Furthermore, a fine of not less than RMB 100,000 but not more than RMB 1 million shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives and persons-in-charge of personal information protection of relevant enterprises within a certain period of time.

According to the DSL, an important data processor failing to appoint a data security officer may face an order to make rectifications and a warning, and may be concurrently fined not less than RMB 50,000 but not more than RMB 500,000, and the person directly in charge and other directly liable persons may be fined not less than RMB 10,000 but not more than RMB 100,000; if the processor refuses to make rectifications or causes

serious consequences such as massive data leakage, it will be fined not less than RMB 500,000 but not more than RMB 2 million, and may be ordered to suspend the relevant business or stop the business for rectification, and the relevant business permit or business licence will be revoked. The person directly in charge and other directly liable persons will be fined not less than RMB 50,000 but not more than RMB 200,000.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

If a Data Protection Officer ("**DPO**") fails to perform his or her duty with due diligence, then he or she may be accused of administrative or even criminal liabilities in respect of his or her role as a DPO.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The law and relevant rules do not specify whether a business can appoint a single DPO to cover multiple entities.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Section 11.1 of the Standard specifies that the DPO shall be a person with relevant management experience and professional knowledge of personal information protection.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please refer to the response to question 8.1. Furthermore, Section 11.1 of the Standard provides that the DPO's responsibilities include but are not limited to:

1) direct responsibility for, and comprehensive and overall implementation of, the organisation's personal data security;
2) organising the formulation of a personal information protection work plan and supervising its implementation;
3) drafting, issuing, implementing and regularly updating the privacy policy and related regulations;
4) establishing, maintaining, and updating the list of personal data held by the organisation (including the type, amount, origin, recipient, etc. of the personal data) and authorised access policies;
5) conducting a personal data security impact assessment, proposing countermeasures and suggestions for personal information protection, and urging the rectification regarding security risks;
6) organising personal data security training;
7) conducting product or service testing before its release in case of unknown collection, use, sharing and other processing activities of personal data;
8) announcing information such as complaint or reporting methods and promptly accepting the complaint and report;
9) conducting safety audits; and
10) communicating with supervisory authorities, and reporting on personal information protection and incident handling, etc.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Under the PIPL, yes. The personal information processor shall make public the contact information of the person in charge of personal information protection and submit their name and contact information to the authorities.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Yes. Please refer to question 8.7.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. Under the PIPL, where a personal information processor entrusts others with the processing of personal information, it shall agree with the agent on the purpose, time limit and method of entrusted processing, type of personal information and protection measures, as well as the rights and obligations of both parties, and supervise the personal information processing activities of the agent.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Please refer to question 9.1.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Pursuant to Article 43 of the Advertisement Law, no organisation or individual shall, without obtaining the consent or request of the parties concerned, distribute advertisements to them via electronic means. Advertisements distributed via electronic means shall state the true identity and contact details of the senders, and the method for the recipients to refuse acceptance of future advertisements. Article 44 further provides that advertisements published in the form of pop-up windows on the website shall show the "close" sign prominently.

Article 13 of the Administration of Internet Electronic Mail Services provides that the word "advertisement" or "AD" must be indicated in the email subject, and it is prohibited to send emails containing commercial advertisement without the express consent of the receivers. Article 14 provides that if an email recipient who has expressly consented to receive electronic direct marketing subsequently refuses to continue receiving such emails, the sender shall stop sending such emails, unless otherwise agreed by the parties. The receivers shall be provided with the contact details for the discontinuation of the receipt of such emails, including the email address of the sender, and shall ensure that such contact details are valid within 30 days.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The Advertisement Law as well as the Administration of Internet Electronic Mail Services Procedures do not specify whether they are only applicable to business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Section VII of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection provides that any organisation or individual shall not send commercial electronic messages to the fixed-line, mobile telephone or email inbox of an electronic message receiver without the prior consent or request of the receivers or if the receivers explicitly express rejection.

The operators of an e-commerce platform, when displaying search results of goods or services, shall mark "advertisement" for bid-ranked products or services, pursuant to Article 40 of the E-commerce Law. Furthermore, Article 18 provides that e-commerce business operators who provide search results based on consumers' preference or consumption habits shall in the meantime provide options not targeting consumers' personal characteristics.

As for marketing by means of automated decision-making, the PIPL requires the relevant processor to provide options not specific to individuals' characteristics simultaneously, or provide methods for individuals to refuse such marketing or push.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Advertisement Law and the E-commerce Law apply to operators providing products and services within the territory of China, while for foreign operators providing products or services to China on an offshore model, the law does not further elaborate whether it will apply or not. However, according to Article 3.2 of the Draft Security Assessment Guidelines on Cross-border Data Transfer, business operators not registered in China but providing products or services to China using the Chinese language, making settlement by the RMB, and delivering products to China are considered to be "providing products or services to China", in which case it is possible that the relevant provisions will apply.

The PIPL applies to the processing of personal information of natural persons within China for the purpose of providing products or services to them or analysing or assessing their conduct. Therefore, marketing sent by a personal information processor from other jurisdictions could be subject to the PIPL if it falls into the cases above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The Administration for Market Regulation is mainly responsible for the enforcement of marketing restrictions. There are recent cases where authorities such as the Administration for Market Regulation are taking action. For example, in 2017, Shanghai Paipaidai Financial Information Service Co., Ltd. was fined RMB 800,000 for its infringement of the Advertisement Law, the breaches including, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

If the source of the marketing lists is legitimate and lawful and the data subject has consented, then it is not prohibited. Otherwise, it is illegal to do so, as network service providers and other enterprises, public institutions and their employees are obligated to keep strictly confidential a citizen's personal electronic information collected during their business activities, and may not disclose, falsify, damage, sell or illegally provide such information to others, as provided in the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Article 63 of the Advertisement Law provides that sending direct marketing communications without obtaining the consent of the target may result in a fine of up to RMB 30,000.

E-commerce platforms that do not clearly mark "advertisement" for bid-ranked products may face a fine of up to RMB 100,000, pursuant to Article 81 of the E-commerce Law and Article 59 of the Advertisement Law.

In addition, Article 77 of the E-commerce Law provides that e-commerce business operators who provide search results in violation of Article 18 as described in question 10.3 shall be ordered to make the correction within a stipulated period, their illegal income shall be confiscated, and a fine ranging from RMB 50,000 to RMB 200,000 may be imposed. In serious cases, a fine ranging from RMB 200,000 to RMB 500,000 should be imposed concurrently.

As for the penalties under the PIPL, please refer to question 8.2.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no legislation addressing the use of cookies explicitly. Given that cookies may fall within the definition of personal information, it is understood that the general regulations on personal data apply to the use of cookies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The law does not distinguish between different types of cookies at this stage.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

There are no administrative actions on the use of cookies. Nonetheless, in 2015, the search engine Baidu's use of cookies to personalise advertisements aimed at consumers when they enter certain third-party websites was found by the court not to infringe an individual's right to privacy.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Please refer to the maximum penalties for other general breaches.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The CSL, PIPL and DSL have set out requirements on international data transfer. For restrictions on international transfer of personal information and important data, please refer to questions 7.1–7.12.

In October 2021, the CAC issued an updated draft regulation, i.e., the Draft Measures for the Security Assessment of Cross-border Data Transfer, according to which data processors are required to conduct security assessment when they provide important data collected and generated overseas during their operation within the territory of the People's Republic of China and personal information that shall be subject to security assessments according to law. The draft regulation is still under review by the relevant authorities and may be subject to further revision.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The PIPL provides several methods that a business can adopt to compliantly transfer personal information abroad, including the following:

1) passing the security evaluation organised by the CAC (for CIIOs and processors whose quantity of processing of personal information reaches that as prescribed by the CAC);
2) obtaining certification by a specialised agency for protection of personal information in accordance with the provisions of the CAC;
3) entering into a contract with the overseas recipient under the standard contract formulated by the CAC, specifying the rights and obligations of both parties; or
4) meeting other conditions prescribed by laws, administrative regulations or the CAC.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

In certain circumstances, prior notification or approval is needed. As mentioned in section 7, CIIOs and personal information processors, whose quantity of processing personal information reach that as prescribed by the CAC, shall pass the security assessment organised by the CAC when transferring personal information collected within China abroad. According to the Draft Measures for the Security Assessment of Cross-border Data Transfer, if a personal information processor has processed personal information of more than 1 million people, or if it has transferred personal information of more than 100,000 people or sensitive personal information of more than 10,000 people overseas accumulatively, the transfer by such processor shall be subject to security assessment.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

This is not applicable.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

This is not applicable.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The PIPL provides that any organisations and individuals shall have the right to file complaints or reports about illegal personal information processing activities with relevant authorities. The authorities receiving complaints or reports shall handle them without delay and notify the complainants and informants of the handling results.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The PIPL does not explicitly prohibit anonymous reporting. Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

Article 12 of the Public Security Video Image Information System Administrative Regulations (exposure draft, hereinafter the "**CCTV Regulations**"), which was issued by the MPS and regulates the use of CCTV for public safety purposes, stipulates that anyone who uses CCTV for public safety purposes shall notify the local public security department of the type and location of the camera installed.

14.2 Are there limits on the purposes for which CCTV data may be used?

Pursuant to Article 6 of the CCTV Regulations, it is prohibited to obtain state secrets, work secrets or trade secrets from a public security video image information system, or infringe on citizens' privacy by using such a system. Organisations that construct and use CCTV are required to keep in confidence the basic information (e.g., the system design, equipment type, installation location, address code) and collected data concerning state secrets, work secrets and trade secrets and shall not illegally disclose CCTV data concerning citizens' privacy. Such CCTV data shall not be bought or sold, illegally used, copied or disseminated, pursuant to Article 22. According to Article 21, investigative, procuratorial and judicial powers, public security and national security organs, as well as the administrative departments of the government at or above town level, may inspect, copy or retrieve the basic information or data collected through CCTV. Under circumstances of the security services, Article 25 of the Regulations on Administration of Security Services provides that the using of CCTV equipment shall not infringe on the legitimate rights and interests or privacy of individuals.

It is worth noting that the PIPL provides restrictions on image capturing, and personal identification equipment installed in public places. Such data collection activities shall be necessary for maintaining public security, comply with the relevant provisions of the State, and conspicuous prompting signs shall be set up. An individual's personal image and personal identification information collected may only be used for the purpose of maintaining public security and shall not be used for any other purpose, except with the individual's separate consent.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

On the one hand, Article 8 of the Labour Contract Law provides that employers are entitled to know about basic information of the worker in direct relation to the labour contract between them; therefore, some types of employee monitoring are permitted, though no specific rule explicitly addresses employee monitoring. On the other hand, it is prudent that the monitoring does not infringe the employee's privacy.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the PIPL, consent may not be needed if the processing of personal information is necessary for the implementation of human resource management in accordance with the internal labour rules and regulations and the collective contract concluded. While the processing of employees' personal information exceeds the human resource management scope, consent is still needed unless the processing falls in other legal bases as prescribed in Article 13 of the PIPL.

In practice, employers usually choose to add a provision in the labour contract or in the employee handbook or similar documents to inform employees of the processing of their personal information, and where necessary, to obtain their consent.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Article 4 of the Labour Contract Law requires employers to discuss with the employee representatives' congress or all employees, and negotiate with trade unions or employee representatives when formulating, revising or deciding on matters directly involving the vital interests of workers such as remuneration, working hours, rest periods and days off, labour safety and health, insurance and welfare, staff training, labour discipline and labour quota administration, etc. Article 43 further provides that employers shall notify the trade union when they unilaterally rescind a labour contract. However, such notifying or negotiating circumstances may not directly relate to employers' monitoring or processing of employees' personal data.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

If consent has been obtained from such employee, then yes. If the employer attempts to process such information without obtaining consent, it may go with the legal ground of "necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency". In spite of this, it is worth noting that whether an employer could process an employee's such information on a legal ground other than consent shall be assessed on a case-by-case basis.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Under Article 40 of the CSL, network operators are responsible for taking technical and other necessary measures to ensure the security of personal data they collect, and to establish and improve the system for user information protection. However, if the network operator as a controller appoints a third party to process personal data on its behalf, it shall ensure that such processor will provide an adequate level of protection to the personal data involved, as provided in Section 8.1 of the Standard.

The PIPL provides in its Article 9 that the personal information processor shall be responsible for its processing of personal information and take necessary measures to ensure the security of the personal information processed. For the definition of personal information processor in the PIPL, please refer to question 2.1.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Under Article 42 of the CSL, in case of (possible) divulgence, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority.

Under the PIPL, where personal information has been or may be divulged, tampered with or lost, the personal information processor shall immediately take remedial measures and notify the relevant authorities and the individuals concerned. The notice shall include the following matters:

1) the types, reasons and possible harm of the information that has been involved or may be involved in the divulgence, tampering with or loss of personal information;
2) the remedial measures taken by the personal information processor and the measures that can be taken by the individuals to mitigate harm; and
3) the contact information of the personal information processor.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes, please refer to question 16.2. Furthermore, according to the PIPL, where the personal information processor has taken measures to effectively avoid harm caused by divulgence, tampering with or loss of information, the personal information processor may opt not to notify the individuals concerned. If the authorities performing duties of personal information protection believe that harm may be caused, they may require the personal information processor to notify the individuals concerned.

16.4 What are the maximum penalties for data security breaches?

Under Article 64 of the CSL, in case of severe violation, an operator or provider in breach of data security may face fines of up to RMB 1 million (or 10 times the illegal earnings), suspension of a related business, winding up for rectification, shutdown of any website(s) and revocation of a business licence. The persons directly in charge may face a fine of up to RMB 100,000.

As for the penalties under the PIPL, please refer to question 8.2.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The PIPL has defined the scope of the "authorities performing duties of personal information protection", including the following:

1) the CAC, which is responsible for coordinating the protection of personal information and relevant supervision and administration work;
2) other relevant national departments (such as the MIIT, the MPS, and the SAMR), which are responsible for protecting, supervising and administering the protection of personal information within the scope of their respective duties; and
3) relevant departments of local people's governments at or above the county level.

These authorities perform the following data protection duties:

1) carrying out publicity and education on personal information protection, and guiding and supervising personal information processors to protect personal information;
2) accepting and handling complaints and reports related to personal information protection;
3) organising the evaluation of applications and other organisations on the protection of personal information, and disclosing the evaluation results;
4) investigating and handling illegal personal information processing activities; and
5) other duties stipulated by laws and administrative regulations.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, and no court order is needed. For example, pursuant to Article 50 of the CSL, if any information prohibited by laws and administrative regulations from release or transmission is found, the CAC and other competent authorities may require the network operator to stop the transmission of such information, take measures such as deletion and keep the records. If any such information is from overseas, they may block the transmission.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The CAC and relevant data protection authorities may issue a ban in the form of an administrative penalty, together with other punitive measures such as a fine, an order to rectify, etc. In the recent special rectification action on app providers, the CAC, MIIT and its local branches usually issue a list of app providers and describe their illegal processing of personal information (such as excessive collection, lack of notification to users), and in cases where the app providers fail to make rectifications, the CAC, MIIT and relevant authorities may even request the apps to be removed from app stores.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

So far, there is no public record of Chinese data protection authorities exercising their powers directly against companies established in other jurisdictions. In most cases, authorities may talk with the local subsidiary of an international company for its violations of the CSL or other data protection regulations.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Both the PIPL and DSL prohibit processors of personal information/data from providing personal information/data to foreign judicial or law enforcement authorities without the approval of competent authorities. If there are treaties or agreements in relation to judicial assistance or cooperation entered into between China and the respective foreign country, the relevant companies may respond to such requests following such treaties or agreements. Any entity or responsible person in violation of such requirement may be subject to administrative penalties.

18.2 What guidance has/have the data protection authority(ies) issued?

The CAC has not issued any guidance particularly concerning e-discovery requests from foreign law enforcement agencies.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As mentioned in section 8, regulations on automotive data processing and algorithm recommendation services have been the major enforcement focus of the CAC in recent years. In terms of the automotive data, it is said that the CAC has conducted a pilot project regarding the annual report of automotive data security management by automotive data processors. Regarding the filing of algorithms, the CAC has recently launched the algorithmic filing system, which has been available since March 1, 2022. It is expected that algorithm recommendation service providers file information regarding the algorithms they applied through this system.

Cross-border data transfer is another point of the CAC's recent enforcement activities. As mentioned above, the Draft Measures for the Security Assessment of Cross-border Data Transfer issued in October 2021 aim to specify the rules and procedures on restrictions of cross-border data transfer. Meanwhile, it is said that the CAC is preparing the standard contract that can be used by companies to ensure that the transfer of personal information is compliant with relevant laws.

Furthermore, the cybersecurity review is also a hot topic. In July 2021, the Cybersecurity Review Office, a unit of the CAC, announced the cybersecurity review into a well-known ride-hailing company Didi, which has set a precedent for how the government will handle national security issues related to cybersecurity and data. Meanwhile, the updated Cybersecurity Review Measures have added that online platform operators holding personal information of more than 1 million users shall declare for cybersecurity review when they enter into IPOs in other countries. Since then, companies seeking to enter into an IPO overseas shall pay additional attention to the requirements on cybersecurity and evaluate whether their activities may raise national security concerns.

19.2 What "hot topics" are currently a focus for the data protection regulator?

Please refer to question 19.1.

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her articles include "*New Trends of the US Personal Data Protection – Key Points of the New FCC Rules*", "*Big Data: Success Comes Down to Solid Compliance*", "*Does Your Data Need a "VISA" to Travel Abroad?*", and "*A Brief Analysis on the Impact of Data on Competition in the Big Data Era*", among others. Susan was recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in 2019 in *LEGALBAND China*.
Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payments, consumer goods, finance, Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to branches of multinational companies in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the US and other cross-jurisdictions. Han was elected as one of "40-under-40 Data Lawyers" by *Global Data Review* in 2018. Han was also recognised as a "Next Generation Partner" by *The Legal 500* in 2021 and named one of the 2021 *ALB China* Top 15 TMT Lawyers.
In the areas of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity incidents, among others.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5749
Fax: +86 10 5878 5599
Email: wuhan@cn.kwm.com
URL: www.kwm.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group