International
Comparative
Legal Guides

# Data Protection 2021

A practical cross-border insight into data protection law

**Eighth Edition**

**Featuring contributions from:**

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

# International Comparative Legal Guides

## Data Protection 2021

### Eighth Edition

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

# Expert Analysis Chapters



# Q&A Chapters

# Q&A Chapters Continued



ICLG.com

# China


Susan Ning

Han Wu

King & Wood Mallesons


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal personal data protection legislation in China is the *Cybersecurity Law of the People's Republic of China* (hereinafter, the "**CSL**"). It sets out general data protection requirements for network operators. China is also preparing specific personal information protection law and data security law. Please refer to question 18.1 for more information.

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

There are pieces of civil and criminal legislation that have an impact 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 provides a definition of personal information and sets out the legal basis for personal information processing, the obligations on the personal information processors, the rights of individuals to their personal information and so on. Most of the provisions of the *Civil Code* regarding the protection of personal information are restatements of requirements contained in the CSL, and national standards such as the *National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification*.

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.

Article 2 of the *Tort Liability Law* sets the right to privacy as one of the civil rights of citizens, along with right to life, right to health, etc.

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

There are many specific pieces of legislation in sectors of banking, insurance, medical, credit information, telecommunications and automobiles that impact data protection, such as the *Securities Law of the People's Republic of China*, the *Implementing Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests*, the *Measures for Administration of Population Health Information*, the *Medical Records Administration Measures of Medical Institutions*, the *Administrative Regulations on Credit Investigation Industry*, the *Several Provisions on Regulating the Market Order of Internet Information Services*, the *Measures for the Administration of Internet Email Services*, and the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, etc.

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

China has no single authority responsible for enforcing provisions relating to the protection of personal information.

Under the CSL, the Cyberspace Administration of China ("**CAC**") is responsible for the planning and coordination of cybersecurity and relevant supervisory and administrative work, while the Ministry of Industry and Information Technology ("**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 ("**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 the telecommunications administrations at the provincial level are responsible for the supervision and administration of personal information in the telecommunications and internet sector.

Also, the State Administration for Market Regulation ("**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*.

## 2 Definitions

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

- "**Personal Data**"
  "Personal Data", or personal information as in Article 76-(5) of the CSL, refers to various information that is recorded in electronic or any other form and used alone or in combination with other information to identify a natural person, including but not limited to the name, date of birth, ID number, personal biological identification

information, address and telephone number of the natural person. The *Civil Code* provides a similar definition of personal information.

- "**Processing**"
  The *Civil Code* provides the definition of "Processing". Article 1035 provides that processing of personal information includes the collection, storage, use, processing, transfer, provision and disclosure of personal information, etc.
  The CSL only provides definitions for a few key terms, and some of the definitions hereby listed are from the *National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification* (hereinafter, "**Standard**"). The Standard is issued by the General Administration of Quality Supervision, Inspection and Quarantine, and the Standardization Administration. Although not compulsory, it is considered good practice to follow. The Standard was updated in March 2020 and took effect in October 2020.
- "**Controller**"
  The CSL does not define "Controller", but Section 3.4 of the Standard defines it as organisations or individuals that have the right to decide on the processing purposes, methods and other aspects of personal data.
- "**Processor**"
  Under the CSL and the Standard, there is no corresponding concept of "Processor". However, the Standard provides the obligations that data processors should comply with in the case of "entrusted processing" in Section 9.1.
  The *Civil Code* defines "Information Processor" as individuals or entities that process personal information, which may include both "Controller" and "Processor".
  The new draft legislation *Personal Information Protection Law* (as introduced in question 18.1) also uses "Personal Information Processor", which is defined as any organisation or individual that independently determines the purpose and method of processing and other personal information processing matters.
- "**Data Subject**"
  The CSL, the *Civil Code*, and the draft *Personal Information Protection Law* do not define "Data Subject". The Standard defines it as the person identified by the personal data in Section 3.3.
- "**Sensitive Personal Data**"
  The CSL does not define "Sensitive Personal Data". Section 3.2 of the Standard defines it as the personal data that, if divulged, illegally disclosed or abused, can harm personal or property safety, or can easily result in damage to reputation, physiological as well as psychological health, or cause the person to be discriminated against. For example, an ID number, personal biological identification information, a bank account, the record and content of correspondence, credit information and the personal data of children under 14 years old, etc.
  Article 29 of the draft *Personal Information Protection Law* similarly defines sensitive personal information as personal information that may lead to discrimination or serious harm to personal or property security once disclosed or illegally used. Sensitive personal information includes an individual's race, ethnicity, religious belief, personal biological characteristics, medical health, financial accounts and personal whereabouts.
- "**Data Breach**"
  The CSL, the *Civil Code*, the draft *Personal Information Protection Law*, and the Standard 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.
- The Standard also provides definitions for other key terms, which, among others, include "**Anonymisation**" and "**De-identification**":
  - **Anonymisation**, as defined in Section 3.14, means making the data subject unidentifiable or unable to be correlated through technical processing of personal data, and the processed information cannot be restored. Anonymised personal data is no longer considered to be personal data.
  - **De-identification**, as defined in Section 3.15, means making the data subject unidentifiable or unable to be correlated if not combined with other information through the technical processing of personal data.

  The draft *Personal Information Protection Law* provides a similar definition of the two terms.

## 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?**

Article 5 of the CSL grants the authorities the power 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 draft *Personal Information Protection Law* provides similar rules to the EU General Data Protection Regulation ("**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 products or services to natural persons in China;
2) where the purpose is to analyse and evaluate the activities of natural persons in China; and
3) other circumstances provided by laws and administrative regulations.

## 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.

Section 4e) of the Standard also sets out transparency as one of the basic principles, stating that the scope, purpose and rules of personal data processing should be publicly available and be clear, understandable and fair, and subject to external supervision.

The same principle has also been included in the draft *Personal Information Protection Law*. 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 the network operators to abide by the "lawful, justifiable and necessary" principles when collecting and using personal data.

Section 5.1 of the Standard further explains what "lawful" means – data controllers shall not deceive, inveigle or mislead the data subject into disclosing personal data, shall not conceal that the product or service it provides collects personal data, shall not obtain personal data from illegal channels and shall not collect information prohibited by law.

Among others, consent is the most common method for achieving lawfulness. Section 4c) of the Standard lists consent as a basic principle, which requires a personal data controller to obtain the data subjects' permission on the purpose, methods, scope and rules, etc. of processing the data.

It is to be noted that consent does not always equal lawfulness; Section 5.6 of the Standard further provides exceptions to the requirement of obtaining consent, where consent is not necessary prior to the collection and use of personal data. Nonetheless, be sure to bear in mind that the Standard is not an enforceable legal text, but a set of recommendations. Therefore, it is recommended to always obtain a data subject's consent where possible.

It is worth noting that the draft *Personal Information Protection Law* attempts to develop the legal basis for processing personal information. Except for obtaining consent, Article 13 provides some other legal grounds for processing of personal information, including:

1) the processing is necessary for the conclusion or performance of a contract to which the individual is a party;
2) the processing is necessary to fulfil statutory duties and statutory obligations;
3) the processing is necessary to respond to public health emergencies or protect natural persons' life, health and property safety;
4) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest;
5) processing within a reasonable scope of personal information that is publicly disclosed in accordance with this *Personal Information Protection Law*; or
6) under any other circumstance as provided by any law or administrative regulation.

- **Purpose limitation**

Article 41 of the CSL requires that network operators shall not collect any personal data that is not related to the services it provides. In Section 4b) of the Standard, there is also the "Clear Purpose Principle", where a data controller must have a clear and specific purpose for processing personal data.

It is also prohibited under Article 6 of the draft *Personal Information Protection Law* to conduct personal information processing unrelated to the processing purpose.

- **Data minimisation**

The CSL does not expressly provide requirements for data minimisation but only generally requires network operators to only collect personal data relevant and necessary for the provision of their services to data subjects.

Section 5.2 of the Standard sets out that, except when otherwise agreed with data subjects, data controllers shall only process the minimum type and amount of personal data necessary to fulfil the purpose the data subject has given consent to. After the purpose is fulfilled, the personal data should be deleted or anonymised promptly.

Furthermore, Article 6 of the draft *Personal Information Protection Law* provides that personal information processing shall be for a definite and reasonable purpose and shall be limited to the minimum scope for achieving the purpose of processing. The draft *Personal Information Protection Law* further provides in its second-reviewed version that the processing of personal information shall be conducted in a way that has the least impact on the interests of individuals.

- **Proportionality**

There is no explicit rule providing for a "proportionality principle" under the CSL or the Standard, but the data minimisation principle under the CSL and the Standard as well as the draft *Personal Information Protection Law* is similar in essence to the "proportionality principle", with both emphasising "processing of personal data only within a proper and necessary scope".

- **Retention**

Section 6.1 of the Standard provides that the storage period of personal information shall be the shortest time necessary to realise the purpose of authorised use of personal information, unless otherwise provided by laws and regulations or otherwise authorised or agreed by the personal information subject.

The draft *Personal Information Protection Law* provides in its Article 20 that unless otherwise stipulated in laws or administrative regulations, the retention period of personal information shall be the shortest time necessary for achieving the purpose.

- **Other key principles**

Article 42 of the CSL and Section 4f) of the Standard provide that a data controller should have the security capabilities that match the security risks it faces and take adequate measures to protect the confidentiality, integrity and availability of personal data. Furthermore, Article 8 of the draft *Personal Information Protection Law* stipulates that the quality of personal information should be guaranteed, so as to avoid adverse effects on personal rights and interests caused by processing inaccurate and incomplete personal information.

## 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**

Section 8.1 of the Standard provides that a data controller should provide a personal data subject with access to:

1) the data or the type of data about him or her held by the controller;
2) the source(s) and the purpose of such personal data; and
3) the identity or type of any third party who has obtained the above personal data.

The *Civil Code* and the draft *Personal Information Protection Law* allow a data subject to consult or copy his or her personal information from any information processor.

- **Right to rectification of errors**
  Article 43 of the CSL provides that each individual is entitled to require any network operator to make corrections if he or she has found errors in such information collected and stored by such operator. The Standard, the *Civil Code* and the draft *Personal Information Protection Law* provide similar rules.
- **Right to deletion/right to be forgotten**
  Under Article 43 of the CSL, each individual is entitled to require a network operator to delete his or her personal data if he or she finds that the collection or use of such information by such operator violates the laws, administrative regulations or the agreement by and between such operator and him or her. In addition to the provisions under the CSL, the draft *Personal Information Protection Law* further clarifies the scenarios where the personal information shall be deleted, including: (i) where the purpose of processing has been achieved or it is no longer necessary to process personal information for achieving such purpose; (ii) where the personal information processor stops providing products or services or the agreed storage period has expired; and (iii) where the individual withdraws his/her consent; or (iv) other circumstances specified in laws and administrative regulations.
  Apart from the above circumstances, Section 8.3 of the Standard further provides that if the data controller shares and transfers the personal data to a third party, or publicly discloses the personal data illegally or in breach of the agreement between the controller and the subject, and the subject demands that the data be deleted, the controller should stop such sharing, transferring and publicly disclosing, and notify the relevant parties to delete the relevant data. Section 8.5 provides that a data subject shall be provided channels to close his or her account and the relevant personal data shall be deleted/anonymised; data controllers shall not set unnecessary or unreasonable conditions when data subjects request to close an account. Further, Section 6.4 provides that if a personal information controller suspends operation in regard to its products or services, it shall delete or anonymise the personal information it holds.
- **Right to object to processing**
  Under the draft *Personal Information Protection Law*, a data subject has the right to restrict or refuse others to process his/her personal information.
  Under the Standard, a data subject's withdrawal of consent can be seen as a right to object to processing. It is to be noted that, pursuant to Section 7.7 of the Standard, a personal data subject will not be provided with a right to object but a right to appeal and a right to obtain manual review of the decisions when such decisions are made by information systems based on automated decisions (such as personal credit, loan limits or interview screening based on user profiling), which significantly influence the data subject's rights and interests.
- **Right to restrict processing**
  The CSL does not provide explicitly for the right to restrict processing. Under the draft *Personal Information Protection Law*, a data subject has the right to restrict or refuse others to process his/her personal information.
- **Right to data portability**
  The CSL does not provide explicitly for the right to data portability. Section 8.6 of the Standard recommends data controllers to provide methods for data subjects to obtain copies of their personal information. The right of data portability is of two kinds: (1) the data controller provides a copy of certain personal data to the data subject; and (2) the data controller directly sends the copy to the third party designated by the data subject where technically feasible.
  The personal data that can be portable are confined to four kinds: data subjects' basic personal data; personal identification information; personal health and physiology information; and personal education and occupational information.
- **Right to withdraw consent**
  Personal data subjects have complete freedom and control in respect of the handling of their personal data. Although it is not explicitly provided in the CSL, Section 8.4 of the Standard provides practical guidelines regarding the revocation and modification of consent, and specially mentions two different scenarios: (1) the withdrawal of consent for refusing to receive commercial advertisements; and (2) the withdrawal of consent for data sharing, transfer and public disclosure. The draft *Personal Information Protection Law* states that an individual shall have the right to withdraw his or her consent to personal information processing activities conducted on the basis of his or her consent, and requires processors of personal information to provide convenient ways for data subjects to withdraw their 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.
- **Right to complain to the relevant data protection authority(ies)**
  The right of individuals to complain to data protection authorities has been recognised in a number of pieces of legislations. 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.
- *Other key rights – please specify*
  The draft *Personal Information Protection Law* added a provision in its second-reviewed draft on the protection of personal information-related rights of the deceased, i.e., the rights of the deceased shall be exercised by his/her close relatives.

## 6 Registration Formalities and Prior Approval

### 6.1 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?

There are such requirements regarding the cross-border transfer of data. As for operators of CII, if the personal information or important data generated or collected by CII operators within the territory of China needs to be transferred abroad for business purposes, a security assessment shall be conducted pursuant to the measures developed by the CAC together with

competent departments of the State Council. Under the draft *Personal Information Protection Law*, personal information processors that process the personal information reaching or exceeding the threshold specified by the CAC in terms of quantity shall conduct the security assessment organised by the CAC if it is necessary to transfer personal information abroad.

Besides, according to certain draft regulations, network operators shall conduct security assessments on transmitting data abroad. Both the Cross-border Transfer of Personal Information (Draft for Comment) issued in June 2019 and the *Personal Information Protection Law* (Draft for Public Consultation) issued in October 2020 stipulate that before the cross-border transfer of personal information, network operators shall apply to the local cyberspace administrations at the provincial level for security assessment for cross-border transfer of personal information.

Furthermore, Article 28 of the Administrative Measures on Data Security (Draft for Comment) provides that network operators shall assess the potential security risks prior to releasing, sharing or selling important data or transferring such data abroad, and shall report to the competent regulatory department for approval. If the competent regulatory department is unclear, network operators shall report to the cyberspace administrations at the provincial level for approval. Apart from the outbound transmission of important data, the newly issued *Data Security Law* requires the processor to regularly carry out risk assessment on its important data processing activities, and submit the risk assessment report to the relevant competent authority.

**6.2 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)?**

The Cross-border Transfer of Personal Information (Draft for Comment) stipulates in Article 4 that network operators shall provide the following materials for security assessment for cross-border transfer of personal information, and shall be responsible for the authenticity and accuracy of the materials:

1) an application form;
2) contracts signed between network operators and recipients;
3) reports on analysis of the security risks for cross-border transfer of personal information and security measures; and
4) other materials required by the national cyberspace administration.

Specifically, the contract of cross-border data transfer shall at least specify:

1) the purposes of cross-border transfer of personal information and the types and storage periods of such information;
2) the subjects of personal information are the beneficiaries of the terms in the contracts that involve the rights and interests of the subjects of personal information;
3) when the legitimate rights and interests of the subjects of personal information are damaged, they may directly claim compensation from either network operators or recipients or from both parties, or entrust an agent on their behalf to do so, and network operators or recipients shall provide compensation, unless it is proved that they have no liability;
4) if changes of the legal environment in the recipients' countries make it difficult to perform contracts, contracts shall be terminated, or security assessment shall be reconducted; and
5) the termination of contracts shall not exempt network operators and recipients from their responsibilities and duties stipulated in the relevant terms of the contracts concerning the legitimate rights and interests of the subjects of personal information, unless the recipients have destroyed the personal information received or have anonymised the information.

As for the report of risk assessment of important data processing, the *Data Security Law* requires the processors to include the types and quantities of important data to be processed, the details of data processing activities, the data security risks faced and the corresponding measures.

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

Article 3 of the Cross-border Transfer of Personal Information (Draft for Comment) specifies that provision of personal information to different recipients shall be subject to separate security assessments, and multiple or continuous provision of personal information to the same recipient does not need go through multiple assessments.

Moreover, Article 3 provides that a new security assessment shall be carried out every two years or in case of changes of the purpose of cross-border transfer of personal information or the type or overseas storage period of such information.

**6.4 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 see question 6.1 regarding who must notify the authority.

**6.5 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 see question 6.2 regarding the information to be included in the notification.

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

The Cross-border Transfer of Personal Information (Draft for Comment) does not specify the sanctions for average network operators. Article 18 only provides that network operators that transfer personal information across borders in violation of the provisions shall be punished in accordance with relevant laws and regulations.

Article 66 of the CSL sets out the sanctions for CII operators' failure to seek approval from the authority. Specifically, it shall be warned and ordered to make rectifications, and shall be subjected to confiscation of illegal earnings and a fine ranging from RMB50,000 to RMB500,000, and may be subjected to suspension of a related business, winding up for rectification, shutdown of websites and revocation of business licences. The supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from RMB10,000 to RMB100,000.

Article 37 of the Administrative Measures on Data Security (Draft for Comment) provides that for any network operator violating the provisions, the competent departments shall, in

accordance with relevant laws and administrative regulations and depending on the circumstances, take disciplinary actions such as disclosing misconduct publicly, confiscating illegal incomes, suspending relevant business operations, ceasing business operation for rectification, shutting down websites, or revoking the relevant business permits or business licences. If the violation constitutes a crime, criminal liability shall be investigated.

As for the failure of reporting risk assessment of important data processing, the *Data Security Law* provides that the relevant processors shall be subject to an order to make corrections and a warning. They may concurrently be imposed a fine of RMB50,000 to RMB500,000, and the person directly in charge and any other directly liable person may be fined RMB10,000 to RMB100,000. Furthermore, the processors who refuse to make corrections or cause serious consequences (such as a large amount of data leakage) shall be fined RMB500,000 to RMB2 million. Such processors may also be ordered to suspend relevant business, suspend business for rectification, have their relevant business licences revoked, and the person directly in charge and other directly liable person may be fined RMB50,000 to RMB500,000. There are also administrative penalties on violation of national core data management rules and rules on cross-border transfer of important data.

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

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

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

Please refer to question 6.3. Furthermore, Article 9 of the Cross-border Transfer of Personal Information (Draft for Comment) provides that network operators shall, before 31 December of each year, report the situations of cross-border transfer of personal information and contract performance in the current year to the local cyberspace administrations at the provincial level.

As for important data processing, the *Data Security Law* does not explicitly provide the frequency to renew the report.

### 6.9 Is any prior approval required from the data protection regulator?

For CII operators, it is widely recognised that prior approval is required when transferring data abroad for business needs.

For transfer of personal information by network operators, Article 5 of the Cross-border Transfer of Personal Information (Draft for Comment) provides the procedures for the cyberspace administrations to conduct the security assessment. Article 2 specifies that if it is identified by the security assessment that the cross-border transfer of personal information may affect national security or damage public interest, or that it is difficult to effectively protect the security of personal information, cross-border transfer of such information shall not be permitted.

As to transfer of important data, the Administrative Measures on Data Security (Draft for Comment) expressly require network operators to obtain prior approval of competent regulatory authorities or cyberspace administrations.

As for important data processing, there is no requirement of prior approval in the *Data Security Law*.

### 6.10 Can the registration/notification be completed online?

It remains unclear whether the notification can be completed online.

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

No, but there are public records of the operators that violate the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (the "**Provisions**"). It is provided in Article 20 of the Provisions that the telecommunications authorities record the activities of telecommunications business operators and internet information service providers that have violated the Provisions into their social credit files and make public such information.

### 6.12 How long does a typical registration/notification process take?

Article 5 of the Cross-border Transfer of Personal Information (Draft for Comment) provides that security assessment shall be completed within 15 working days, and the time limit may be appropriately extended for those with complex situations. Detailed implementation measures or guidelines are expected to be formulated.

## 7 Appointment of a Data Protection Officer

### 7.1 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.

It is provided in Article 21 of the CSL that network operators should appoint network security officers to protect the security of the network. Further, it is provided in Article 34 that a CII operator shall also appoint a security management officer. The appointment of such officers is mandatory. Furthermore, Section 11.1 of the Standard specifies that the personal data controller shall appoint a Data Protection Officer and set up a Data Protection Department.

The draft *Personal Information Protection Law* requires a personal information processor that processes personal information reaching or exceeding the threshold specified by the national CAC in terms of quantity to appoint a person in charge of personal information protection to be responsible for conducting supervision of personal information processing activities as well as the protection measures taken. Furthermore, where the personal information processor is located outside China, it shall establish a special agency or designate a representative within China to be responsible for relevant matters of personal information protection, and submit the name and contact information of relevant agency or the representative to the department performing duties of personal information protection.

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

Although the appointment of a Data Protection Officer is a good practice to follow, set by the Standard, there is no sanction for failing to do so under the CSL. Nonetheless, there are sanctions

for failure to appoint a network security officer and, in case of a CII operator, a security management officer, under Article 59 of the CSL.

Operators that fail to appoint a network security officer can expect warnings and orders for rectifications. A fine ranging from RMB10,000 to RMB100,000 may be imposed if the operator refuses to make rectifications, or in case of severe consequential damage. A fine ranging from RMB5,000 to RMB50,000 may be imposed on the person directly in charge.

CII operators that fail to appoint a security management officer can expect warnings and orders for rectifications. A fine ranging from RMB100,000 to RMB1 million may be imposed if the operator refuses to make rectifications or in case of severe consequential damage. A fine ranging from RMB10,000 to RMB100,000 may be imposed on the person directly in charge.

Under the draft *Personal Information Protection Law*, any illegal processing of personal information, or failure to adopt necessary security protection measures shall be subject to order of rectification and confiscation of illegal gains; if rectification is refused, a fine of not more than RMB1 million shall be imposed on the processor; and a fine of not less than RMB10,000 but not more than RMB100,000 shall be imposed on the directly liable person in charge and other directly liable persons. Where the circumstances are serious, except for the order of rectification and confiscation of illegal gains, a fine of not more than RMB50 million or not more than 5% of its turnover of the previous year shall be imposed. The processor may also be ordered to suspend relevant business or to suspend business for rectification; its business licence may further be revoked. Furthermore, a fine of not less than RMB100,000 but not more than RMB1 million shall be imposed on the directly liable person in charge and other directly liable persons.

### 7.3 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 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 Data Protection Officer.

### 7.4 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 Data Protection Officer to cover multiple entities.

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

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

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

Section 11.1 of the Standard provides that the Data Protection Officer's responsibilities include but are not limited to:

1) comprehensive and overall implementation of the organisation's personal data security and direct responsibility for the 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.

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

The currently effective law does not require the appointment of a Data Protection Officer to be registered or notified to the relevant data protection authorities.

Under the draft *Personal Information Protection Law*, the name, contact information, among others, of the person in charge of personal information protection shall be submitted to the competent authority.

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

Section 5.6 of the Standard provides the contents that the privacy policy should include, and the name of the Data Protection Officer is not within it. Nevertheless, it is recommended to appoint a person whom the public can contact for the purpose of dealing with users' queries and complaints regarding privacy and data protection issues.

Under the draft *Personal Information Protection Law*, a personal information processor shall publish the contact information of the person in charge of personal information protection.

## 8 Appointment of Processors

### 8.1 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?

The currently effective law does not have such requirements, but Article 9.1 of the Standard provides that a data controller may enter into an agreement with a trusted processor for it to process personal data on the controller's behalf. Furthermore, the draft *Personal Information Protection Law* requires a personal information processor who entrusts others to process personal information, to agree with the entrusted party on the purposes of the entrusted processing, processing period, processing methods, categories of personal information, protection measures, as well as the rights and obligations of both parties, among others.

**8.2 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.)?**

There is no requirement for the formalities of the agreement. As for the content, Article 9.1 of the Standard stipulates that it should address the responsibilities and duties of the processor, including the requirements for processing the personal data, whether it can reassign a processor, the assistance it shall provide to the data controller, the responsibility to give feedback to the data controller and the responsibility in respect of terminating the agreement.

## 9 Marketing

**9.1 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 Procedures 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.

**9.2 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.

**9.3 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 draft *Personal Information Protection Law* requires the relevant processor to provide options not specific to individuals' characteristics simultaneously, or provide methods for individuals to refuse such marketing or push.

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

The CSL, the *Advertisement Law* and the *E-commerce Law* apply to operators providing products and services within the territory of the PRC, while for foreign operators providing products or services to the PRC 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 we understand that it is possible that the relevant provisions will apply. The draft *Personal Information Protection Law* applies to the processing of personal information of natural persons within China for the purpose of providing products or services to natural persons within China or analysing or assessing the conduct of natural persons in China. Therefore, the marketing sent by a personal information processor from other jurisdictions could be subject to the draft *Personal Information Protection Law* if it falls in the cases above.

**9.5 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 RMB800,000 for its infringement of the *Advertisement Law*, the breaches including, among others, sending direct advertisements via email without obtaining prior consent of the recipients.

**9.6 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.

**9.7 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 RMB30,000.

E-commerce platforms not clearly marked "advertisement" for bid-ranked products may face a fine of up to RMB100,000, 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 9.2 shall be ordered to make the correction within a stipulated period, their illegal income shall be confiscated, and a fine ranging from RMB50,000 to RMB200,000 may be imposed. In serious cases, a fine ranging from RMB200,000 to RMB500,000 should be imposed concurrently.

As for the penalties under the draft *Personal Information Protection Law*, please refer to question 7.2.

## 10 Cookies

**10.1 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 fall within the definition of personal information (the CSL stipulates that personal data refers to information that can be used alone or in combination with other information to identify a natural person, while the Standard also provides that information such as online browsing records is personal data), it is understood that the general regulations on personal data apply to the use of cookies.

**10.2 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.

**10.3 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.

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

Please refer to the maximum penalties for other general breaches.

## 11 Restrictions on International Data Transfers

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

The CSL provides that the personal information and important data collected by a CII operator during their operations within the territory of China shall be stored domestically, and the cross-border transfer of personal information and important data by a CII operator for business needs shall be subject to a security assessment.

For restrictions on international transfer of personal information and important data, please refer to questions 6.1–6.12. It is anticipated that both the Cross-border Transfer of Personal Information (Draft for Comment) and the Administrative Measures on Data Security (Draft for Comment), which are still under review by the relevant authorities, will be subject to further revision.

It remains uncertain whether the current requirements in the draft measures will take effect in the future.

**11.2 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.).**

With the data subjects' consent, companies can transfer data abroad provided a security assessment is properly carried out. In addition to obtaining the data subject's consent, companies would need to prove that their transfer of personal data overseas arose from business needs under certain circumstances, and shall submit security assessment results with competent authorities for approval according to the draft measures (see question 11.1).

The draft *Personal Information Protection Law* attempts to develop the rules on cross-border data transfer. Article 38 provides that where a personal information processor needs to provide personal information outside China due to business or other needs, it shall at least meet any of the following conditions:

1) security assessment organised by the national cyberspace administration has been passed;
2) personal information protection certification has been conducted by a specialised institution according to provisions issued by the national cyberspace administration;
3) a standard contract formulated by the CAC has been concluded with the overseas recipient, agreeing on both parties' rights and obligations, and supervision is conducted to ensure that personal information processing activities of the overseas recipient meet the personal information protection standards provided in this law; or
4) other conditions provided in laws or administrative regulations or by the CAC.

**11.3 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.**

For CII operators, Article 37 of the CSL stipulates that personal

data and important data collected or generated in China must be stored domestically. The transfer of such information overseas arising out of business needs is permitted, subject to the prior consent of the data subject, completion of a security assessment and approval from competent industry authorities.

For general network operators' cross-border transfer of personal information and important data, please refer to questions 6.1–6.12.

**11.4 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.

**11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?**

This is not applicable.

## 12 Whistle-blower Hotlines

**12.1 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 draft *Personal Information Protection Law* 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.

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

The draft *Personal Information Protection Law* does not explicitly prohibit anonymous reporting. Anonymous reporting is generally permitted.

## 13 CCTV

**13.1 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.

**13.2 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.

In the draft *Personal Information Protection Law*, the installation of image collection or personal identification equipment in public places shall be necessary for maintaining public security and comply with relevant regulations, and conspicuous signs shall be erected. The collected personal images and personal identification information can only be used for the purpose of maintaining public security, and shall not be disclosed to the public or provided to others, except with the separate consent of individuals.

## 14 Employee Monitoring

**14.1 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 shall not infringe the employee's privacy.

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

Yes, the collecting of personal data generally requires consent from the data subject – this principle also applies to employee monitoring. In practice, such consent is normally obtained through a provision in the labour contract or in the employee handbook or similar documents.

**14.3 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 Data Security and Data Breach

**15.1 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 draft *Personal Information Protection Law* similarly requires the processor of personal information to take necessary measures to ensure that personal information processing activities comply with the provisions of laws and administrative regulations, and prevent unauthorised access to as well as the leakage, theft, tampering or deletion of personal information. For the definition of personal information processor in the draft *Personal Information Protection Law*, please refer to question 2.1.

**15.2 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) disclosure, damage or loss of data collected, the network operator is required to take immediate remedies and report to the competent authority. Section 9.1 of the Standard provides that the report should include the type, quantity, content and nature of the affected data subjects, the impact of the breach, measures taken or to be taken, and the contact information of relevant persons.

**15.3 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. A network operator is required to take immediate remedies and notify the affected data subjects in case of (possible) data breaches pursuant to Article 42 of the CSL. Section 9.2 of the Standard stipulates that the content of the notification should include, but not be limited to, the nature and impact of the breach, the measures taken or to be taken, the suggestions for data subjects to mitigate risks, remedies for the data subjects and the contact information of the Data Protection Officer. Under the draft *Personal Information Protection Law*, notification to individuals may not be needed where the personal information processor is able to effectively avoid the harm caused by information leakage. However, if the relevant authority considers that the leakage may cause harm to individuals, it is entitled to require the personal information processor to notify individuals.

**15.4 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 RMB1 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 RMB100,000. As for the penalties under the draft *Personal Information Protection Law*, please refer to question 7.2.

## 16 Enforcement and Sanctions

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

| Investigatory/ Enforcement Power | Civil/ Administrative Sanction | Criminal Sanction |
|---|---|---|
| The public security departments have investigatory power regarding criminal and administrative infringement on personal data, and enforcement power with relevant administrative and criminal sanctions. | The court is responsible for civil sanctions. | The court has the power to impose criminal sanctions. |
| The CAC, the telecommunications department, the public security department and other authorities concerned have investigatory power regarding administrative infringement on personal data, and enforcement power with relevant administrative sanctions. | The CAC, the telecommunications department, the public security department and other authorities concerned have the power to impose administrative sanctions. | This is not applicable. |

**16.2 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.

**16.3 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. For relevant cases, please refer to question 18.2.

**16.4 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.

## 17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

In the case of foreign e-discovery requests from foreign law enforcement agencies, companies must obtain the consent of the personal data subject and carry out security assessments with the relevant authority before transmitting any personal data or important data abroad. In terms of security assessments of CIIs, the CSL provides that if there are different provisions under laws and administrative regulations, such provisions shall apply.

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. Furthermore, the *International Criminal Judicial Assistance Law* issued on 26 October 2018 sets out rules and procedures regarding the enforcement of international criminal judicial assistance in China, including assistance requests of domestic agencies to foreign authorities, and foreign agencies' requests of assistance in China. Pursuant to Article 4 of the *International Criminal Judicial Assistance Law*, domestic businesses must obtain authorisation from a competent authority of China before disclosing any information or providing any assistance requested by foreign law enforcement agencies.

Similar rules have been set in recent pieces of draft legislation. For example, pursuant to the draft *Personal Information Protection Law*, where it is necessary to provide personal information to any party outside of China for international judicial assistance or administrative law enforcement assistance, an application shall be filed with the relevant competent department for approval according to the law. Furthermore, the *Data Security Law* provides that the relevant Chinese authorities shall handle data requests of foreign judicial or administrative agencies in accordance with relevant laws and international treaties and agreements or in accordance with the principle of equality and reciprocity. Unless approved by relevant authorities, no domestic entity or individual is allowed to provide data stored in China to any foreign judicial or administrative agencies. Any entity or responsible person in violation of such requirement will be subject to administrative penalties.

**17.2 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.

## 18 Trends and Developments

**18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.**

2020 has seen an acceleration of developments in China's cybersecurity and data protection regimes. Most noticeable is the publication of two major pieces of legislations for public consultation.

On 21 October 2020, the Draft *Personal Information Protection Law* was finally unveiled to the public. By comprehensively deepening China's personal information protection system, the Draft strengthens the protection of personal information while taking into account the complexity of economic and social life. The release of the nearly 8,000-character Draft marks China's first attempt to systematically and legislatively define, establish, and integrate the provisions on the protection and regulation of personal information. The Draft not only incorporates China's legislative, regulatory and practical achievements regarding data security in recent years, including the CSL, but also takes references of the varied legislative experience of the other jurisdictions in data protection such as the GDPR. The Draft was further reviewed by the Standing Committee of the National People's Congress in 2021 and the second-reviewed version was released on 29 April 2021.

Furthermore, the Standing Committee of the National People's Congress published the Data Security Law on 10 June 2021, which will take effect on 1 September 2021. The *Data Security Law* stipulates that different security requirements will apply to data falling into different levels of sensitivity and relevant authorities will also formulate catalogues of "important data" within their jurisdictions, and implement enhanced security measures to protect these important data. It also stipulates that data activities that may affect national security will be subject to security reviews organised by government authorities.

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

The illegal processing of personal information by apps and the ecological governance of network information are points of concern for data protection regulators at present.

During the year 2020, both the MPS and the MIIT have initiated a number of investigations on the illegal collection and use of personal information by app operators. As a result, lots of apps were notified by the authorities to make rectifications. In March 2021, the CAC, MPS, MIIT and SAMR issued the *Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*, which will take effect on 1 May 2021 and specify the scope of necessary personal information for 39 types of apps.

In January 2020, the CAC launched a six-month campaign of ecological governance of network information in order to rectify negative and harmful information such as obscene pornography, vulgarity, violence, terror, gambling scams, etc., on websites,

mobiles, forums, instant messaging tools, live broadcast platforms and other key links, and to investigate and close illegal websites and accounts.

In April 2020, the MPS launched the "Jingwang 2020" campaign to continue the fight against infringement of Chinese citizens' personal information.

In December 2020, the SAMR published its consultation draft of the *Antitrust Guidelines on the Platform Economy* where it points out that data may constitute necessary facilities under certain circumstances and data-driven algorithms may be used to reach monopoly agreements.

**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 publications 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 is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in *2019 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 payment, 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
1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
P. R. 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 multinational companies' branches 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 United States and other cross-jurisdictions. Han was elected as one of the "40-under-40 Data Lawyers" by *Global Data Review* in 2018, and was recognised as Next Generation Partner by *The Legal 500* in 2021.

In the area 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
1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
P. R. China

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

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key countries in Europe, as well as a presence in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies and business and legal media, including *Acritas*, *Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific Awards*, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, among others. In the field of cybersecurity and data protection, King & Wood Mallesons was recognised as the "Best Law Firm" for Data Protection and Privacy in the 2018 *China Business Law Awards*, and a "Tier 1 Law Firm" for Cybersecurity and Data Compliance in *2020 LEGALBAND* China, and was recognised as one of the first-tier PRC law firms in data protection by *The Legal 500* in 2021.

**www.kwm.com**

KING&WOOD MALLESONS
金杜律师事务所

# ICLG.com

## Other 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
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

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group