THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 8

CHINA

Hongquan (Samuel) Yang[1]

I OVERVIEW

On 20 August 2021, China promulgated the Personal Information Protection Law (PIPL) with the aims to provide greater protections for personal information and create an omnibus data privacy legislation. Being effective from 1 November 2021, the PIPL is the most important personal data protection law in China, although the Cybersecurity Law (CSL), Data Security Law (DSL) and various industry regulations also play important roles in this area.

On 7 November 2016, the CSL was issued and it took effect on 1 June 2017. Among other things, the CSL covers the following aspects: personal information protection; general network protection obligations of the network operators and the multi-level protection scheme (MLPS); enhanced protection for the critical information infrastructure (CII); data localisation and security assessment for the cross-border transfer of personal information and important data; and security review of the network products and services.

On 10 June 2021, the National People's Congress enacted the DSL, which came into effect on 1 September 2021. Unlike the CSL and PIPL in which more detailed cybersecurity and personal data protection obligations are imposed on enterprises and other organisations, the DSL does not set out many detailed obligations for enterprises and other organisations. Instead, the DSL focuses primarily on the protection of overall national data security and sets out some high-level data management and protection methodologies and rules for government agencies, industry associations, enterprises, and other organisations. National security is a theme throughout the DSL.

The PIPL, the CSL and the DSL are believed to be three cornerstones of the overall data protection and cybersecurity legal regime of China. Besides these laws, China has been drafting a series of related implementation regulations and national standards.

II THE YEAR IN REVIEW

Recently, China has accelerated the legislative process and strengthened enforcement actions in the realm of data protection and cybersecurity. Notable highlights are as follows.

1 Hongquan (Samuel) Yang is a partner at AnJie Law Firm.

i New legislation or proposals

In parallel with the PIPL, the CSL and DSL, a series of implementation regulations and national or industrial standards have been published or proposed to provide further practical guidance.

On 30 July 2021, the State Council published the Regulations on Security Protection of Critical Information Infrastructure (CII Protection Regulations) which came into effect on 1 September 2021. The CII Protection Regulations provide for protection responsibilities of critical information infrastructure operators (CIIOs) and call for an information sharing mechanism among relevant national departments and CIIOs to ensure the timely collection, evaluation, sharing and releasing of information concerning network security threats, vulnerabilities and incidents.

On 12 March 2021, the Cyberspace Administration of China (CAC), Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS) and State Administration for Market Regulation (SAMR) jointly issued the Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (App Rules). The App Rules provide the scope of necessary personal information needed for 39 common types of mobile apps, including, inter alia, maps and navigation apps, online payment and shopping apps, mailbox and cloud drive service apps, remote meeting apps and mobile banking apps.

On 15 March 2021, the SAMR published the Measures for the Supervision and Administration of Online Transactions, which clarifies that online transaction operators shall not force or disguisedly force any consumer to consent on the collection or use of information not directly related to the business activities of online transaction operators by means of one-off general authorisation, default authorisation, bundled authorisation, cessation of installation and use, etc. To collect or use sensitive personal information, consumers' consent shall be obtained on an item-by-item basis.

On 11 January 2021, the People's Bank of China (PBOC) issued the Administrative Measures for Credit Reporting Business (Draft Credit Reporting Measures) to solicit public opinions. The Draft Credit Reporting Measures strengthens the supervision of credit reporting business for the life cycle of credit information (i.e., through collection, storage, utilisation, transfer to deletion).

Notably, according to the State Council's legislative work plan for 2021, the draft Data Security Management Regulation will be revised by the CAC this year. Once revised and passed, this Regulation will likely be positioned as implementation regulation of the DSL and CSL.

Relevant national and industrial standards passed in 2021 include GB/T 22240-2020 Information Security Technology – Classification Guide for Classified Protection of Cybersecurity; GB/T 39725-2020 Information Security Technology – Guide for Health Data Security; and JR/T 0223-2021 Financial Data Security – Security Specification of Data Life Cycle, among others.

ii Major enforcement actions

From 1 May 2021 (when the App Rules came into effect) to 11 June 2021, the CAC has released four announcements on a total number of 351 apps for their failure to perform personal information protection obligations. The main violations include excessively collecting personal information unrelated to the services provided by the apps and collecting personal information without obtaining the consent of the users.

In July 2021, the CAC commenced cybersecurity reviews against four overseas-listed companies (DiDi, Yunmanman, Huochebang and Boss Zhipin) for the first time since the promulgation of the Cybersecurity Review Measures in April 2020. As stipulated by the Cybersecurity Review Measures, a cybersecurity review shall be conducted where the purchase of network products and services by CIIOs will influence or might influence state security. Also in July 2021, the CAC released a draft revised version of the Cybersecurity Review Measures to solicit public opinions, which brings data processing activities and listing on foreign exchanges that might affect national security to the realm of cybersecurity review.

iii Major litigation cases

In April 2021, the final judgment was made in the first lawsuit over the use of facial recognition technology in China. This case was raised by a law professor who claimed that Hangzhou Safari Park's collection of facial images for verification purposes was unnecessary and unlawful, after the park replaced its fingerprint system with a facial recognition system at its front gates. The court stands with the plaintiff on the ground that the park unilaterally changed the methods of entry from fingerprint recognition to facial recognition during the performance of the contract without obtaining the plaintiff's consent, and, more importantly, the park's collection of facial images undermined the necessity principles and lacked legitimacy from the outset.

In March 2021, a court judgment stated that a leading technology company providing web crawling services for more than 2,000 banks, insurance companies and other organisations violated the Criminal Law since the web scraping company illegally stored nearly 20 million pieces of personal information.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In addition to the three cornerstones of the overall data protection and cybersecurity legal regime of China (the PIPL, the CSL and the DSL), there are privacy and data protection provisions dispersed in various laws and regulations, including:

a the Civil Code;
b the Criminal Law;
c the National Security Law;
d the E-commerce Law;
e the Law on the Protection of Rights and Interests of Consumers;
f the Tourism Law;
g the Anti-Terrorism Law;
h the Law on Resident Identity Cards;
i the Measures for Cybersecurity Review;
j the Implementing Measures of the People's Bank of China for Protection of Financial Consumers' Rights and Interests;
k the Interim Measures for the Administration of Online Taxi-Booking Business Operations and Services;
l the Administrative Provisions on Short Message Services;
m the Regulations on Management of Internet User Account Names;
n the Provisions on the Security Management of Personal Information of Users of Posting and Delivering Services;

o the Administrative Regulations on the Credit Investigation Industry;
p the Provisions on Cyber Protection of Personal Information of Children;
q the Regulations on Security Protection of Critical Information Infrastructure;
r the Several Provisions on Regulating the Order of the Internet Information Service Market; and
s the Provisions on Protecting the Personal Information of Telecommunications and Internet Users.

China's legal regime on data protection and cybersecurity also includes the judicial interpretations made by the Supreme People's Court and the Supreme People's Procuratorate, such as:

a provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases involving the Processing of Personal Information Using Facial Recognition Technology;
b 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; and
c provisions of the Supreme People's Court on application of laws to cases involving civil disputes over infringement upon personal rights and interests by using information networks.

National standards are another key part of the data protection and cybersecurity legal regime in China. Though the majority of them are not compulsory, they are generally regarded as good-practice guidance by enterprises. Important national standards (including draft versions) are as follows:

a Information Security Technology – Personal Information Security Specification (Specification);
b Information Security Technology – Guidance for Personal Information Security Impact Assessment;
c Information Security Technology – Guide for De-Identifying Personal Information;
d Information Security Technology – Guide for Health Data Security;
e Information Security Technology – Specification for Financial Information Service Security;
f Information Security Technology – Requirements for Security of Face Recognition Data (Draft for comments);
g Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft for comments);
h Information Security Technology – Implementation Guide for Classified Protection of Cybersecurity;
i Information Security Technology – Evaluation Requirement for Classified Protection of Cybersecurity;
j Information Security Technology – Baseline for Classified Protection of Cybersecurity; and
k Information Security Technology – The Evaluation Method for Security Protection Capability of Critical Information Infrastructure (Draft for comments); etc.

The PIPL defines 'personal information' as all kinds of information relating to identified or identifiable natural persons as recorded by electronic or other means, excluding information after anonymisation. The PIPL defines 'sensitive personal information' as personal information that, once leaked or illegally used, may easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal whereabouts and other information of a natural person, as well as any personal information of a minor under the age of 14.

The CSL defines the terms 'network operator' and 'personal information'. Under the CSL, a network operator refers to the owner or manager of a network or the provider of a network service; personal information refers to various information that is recorded in electronic or any other form and used alone or in combination with other information to recognise the identity of a natural person, including but not limited to their name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person.

The Specification makes minor wording changes to the definition of 'personal information' under the PIPL and the CSL. According to the Specification, personal information means any information saved in electronic form or otherwise that can be used independently or together with other information to identify a natural person or reflect the activities of a natural person, including names, dates of birth, identification numbers, personal biometric information, addresses, contact information, records and content of communications, accounts and the passwords thereof, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information on transactions, etc.

The Specification also defines 'sensitive personal information' as personal information that may cause harm to personal or property security, or is very likely to result in damage to an individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused, including identification numbers, personal biometric information, bank accounts, records and content of communications, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information of transactions, personal information of children aged 14 or younger, etc. Also, the Specification clarifies that personal information formed by the personal information controller through the processing of personal information or other information that may cause harm to personal or property security, or is very likely to result in damage to an individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused, is personal sensitive information.

Without differentiating between the 'data controller' and 'data processor', the PIPL instead allocates liability and compliance requirements to a 'personal information handler', which refers to any organisation or individual that independently determines the purpose and method of processing in their activities of processing of personal information. This definition suggests that the term 'personal information handler' under the PIPL is akin to the concept of 'data controller' under the GDPR.

Unlike the PIPL, the Specification does provide the definition of 'personal information controller', which means an organisation or an individual who is capable of determining the purposes and means of the processing of personal information. However, the Specification does not define the 'personal information processor'.

According to the PIPL, the basic principles for personal information processing include:

a Lawfulness, fairness, necessity and good faith: personal information processing shall be conducted in accordance with the principles of legality, legitimacy, necessity and good faith. Personal information shall not be handled in a misleading, fraudulent or coercive way.

b Purpose limitation: personal information processing shall have a clear and reasonable purpose, conducted for a purpose directly relevant to the purpose of processing and in a way that has the least impact on the personal rights and interests. Any personal information processing shall be limited to the minimum scope necessary for achieving the purpose of processing and shall not be excessive.

c Transparency: personal information processing shall be conducted in line with the principles of openness and transparency, the rules on personal information processing shall be disclosed and the purpose, method and scope of processing shall be explicitly publicised.

d Accuracy and integrity: the quality of personal information shall be ensured when processing personal information so as to avoid any negative impact on personal rights and interest due to any inaccuracy or incompleteness of personal information.

e Accountability: personal information handlers shall be responsible for their personal information processing activities and take necessary measures to safeguard the security of the personal information which they handle.

Where a personal information handler processes personal information in a manner that violates the PIPL or fails to perform the obligations of personal information protection specified in the PIPL, the competent authorities performing personal information protection duties could order a correction, confiscate any unlawful income and issue a warning; any application program that illegally processes personal information will be ordered to be suspended or terminated; and, if correction is not made, a fine of up to 1 million yuan shall be imposed. For a serious breach of the PIPL, competent authorities performing personal information protection duties could impose a fine of up to 50 million yuan, or 5 per cent of last year's annual revenue, and may also order the suspension of related business operations or suspension of business for rectification, and report to other competent authorities to revoke the related business permit or business licence of the personal information handlers.

If in violation of the related provisions on personal information protection, according to Article 64 of the CSL, if network operators or providers of network products or services infringe upon any right in personal information that is legally protected, they will receive punishments from the competent authorities, such as rectification, warning, confiscation of illegal earnings and fines; if in severe violation, the punishment may cover suspension of related business, winding up for rectification, shutdown of their website, and revocation of their business licence. Also, stealing or otherwise unlawfully obtaining any personal information, or selling or unlawfully providing such information to others that does not constitute a crime will be punished through confiscation of the illegal earnings or a fine.

ii General obligations for data handlers

The CSL only provides some general principles for personal information protection, Article 41 of the CSL provides that:

> *Network operators shall abide by the 'lawful, justifiable and necessary' principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected. No network operator may collect any personal information that is not related to the services it provides. It shall collect and use, and process and store personal the information in the light of laws and administrative regulations and agreement with the users.*

Article 1037 of the Civil Code provides that:

> *A natural person may consult or copy his or her personal information with any information processor in accordance with the law; if any error is found in the information, the natural person has the right to raise an objection and request the information processor to take necessary measures such as corrections in a timely manner.*
>
> *Where a natural person discovers that an information processor has processed his or her personal information in violation of the provisions of laws and administrative regulations or the agreement between both parties, he or she shall have the right to request that the information processor promptly delete the information.*

The PIPL sets out general personal information protection obligations for personal information handlers in Chapter V, which are as follows:

a Internal policies and operational procedures: establishing internal management rules and operational procedures.

b Data protection officer: appointing a personal information protection officer responsible for supervising the processing of personal information and the adopted protection measures, if the amount of the personal information processed reaches a certain threshold as determined by the CAC.

c Categorisation of personal information: implementing the categorisation management of personal information.

d Technical security measures: taking appropriate technical security measures such as encryption and de-identification; reasonably determining the authority to process personal information.

e Training: conducting security education and training for employees on a regular basis.

f Emergency plan: formulating and organising the implementation of emergency plans for personal information security incidents.

g Audit of personal information processing activities: conducting regular audits of personal information processing activities.

h Impact assessment: carrying out personal information protection impact assessments prior to certain kinds of processing activities, such as processing sensitive personal information, performing automated decision-making based on personal information, transferring personal information overseas or to third parties, etc.

i Data subject request: establishing an accessible mechanism to receive and handle the requests of data subjects.

j Data breach notification and reporting: in the case of a personal information breach, immediately taking remedial measures and notifying competent supervisory authorities and the data subjects concerned, unless the data controllers can take effective measures to avoid damage caused by the personal information breach.

k Additional obligations for personal information handlers who provide an important internet platform service, have a large user base or operate a complex type of business, such as developing platform rules to specify the standards for processing of personal information and the obligations of personal information protection to be met by product or service providers operating on their platform.

Collection of personal information

Under the PIPL, a personal information handler may process personal information only based on the following grounds:

a Data subject's consent: having obtained the consent of the person whose personal information is to be collected.

b Conclusion or performance of a contract: conducting personal information processing that is essential for the conclusion or performance of a contract to which the individual is a contracting party, or where it is necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded.

c Statutory obligations: conducting personal information processing that is essential for performing statutory responsibilities or obligations.

d Responding to public health incident and other emergencies: conducting personal information processing that is essential for responding to public health emergencies or for protecting the life, health or property safety of natural persons in emergency situations.

e Publicly available personal information: processing the personal information that has already been disclosed by the individual or otherwise legally disclosed in accordance with this law and within a reasonable scope.

f News report: conducting personal information processing within the reasonable scope of implementing news reporting, public opinion supervision and other actions for the public interest.

g Other circumstances under the law: having other circumstances as stipulated by laws and administrative regulations.

Adhering to the transparency principle, the PIPL generally requires that prior to the processing of personal information, an entity must provide individuals with the following information in a conspicuous way, in clear and easy-to-understand language, and in a truthful, accurate and complete manner:

a the name or personal name and the contact details of the controller;

b the purpose and method of processing;

c the categories of personal information;

d the retention period;

e the method and procedure for individuals to exercise their rights;

f the necessity of the processing and the impacts on the individual when processing sensitive personal information; and

g other matters to be notified in accordance with the provisions of laws and administrative regulations.

If the personal information handler informs the individuals of the above matters by formulating rules on personal information processing, such rules shall be made public

and shall be easily accessible and convenient for keeping. Any change to any above matter shall be informed to the individual. The PIPL further clarifies certain exceptions to the above-mentioned notice requirements:

a when processing personal information, the data controller may not inform the individuals of the matters as specified in Paragraph 10 if there is any circumstance that should be kept confidential and is not required to be disclosed as stipulated by laws or administrative regulations; and

b in case of emergencies where it is impossible to promptly inform the individuals as necessitated for the protection of the life, health or property safety of a natural person, the data controller shall timely inform the individuals after the emergencies are eliminated.

Where personal information handlers rely on consent as the lawful basis for processing, the consent to personal information processing shall be given by the individuals voluntarily and explicitly on the premise of full knowledge. An individual has the right to withdraw his or her consent and the personal information handlers shall accordingly provide convenient ways to withdraw such consent. The withdrawal of consent shall not affect the effectiveness of the processing activities before its withdrawal. If the purpose or method of processing or the categories of personal information change, the individual's consent must be obtained again.

Aside from this general consent requirement, the PIPL also puts forward more specific consent requirements in various specific circumstances:

a parental or other guardians' consent is required for processing personal information of minors below the age of 14;

b separate consent is required for the processing of sensitive personal information, providing personal information to third parties, for publicising personal information; and for transferring personal information overseas, and for the use of any personal image or personal identification information of an individual collected by any image capturing or personal identification equipment installed in a public place other than for the purpose of maintaining public security; and

c written consent is required if laws and administrative regulations have such special requirements.

Use of personal information

The principles of the PIPL set the threshold for the use of personal information (i.e., lawfulness, fairness, necessity and good faith; purpose limitation and necessity; transparency; accuracy and integrity; accountability).

Moreover, the PIPL stipulates specific requirements for automated decision-making, requiring that personal information handlers shall guarantee the transparency of their decision-making procedure and the fairness and justice of their results when using personal information to conduct automated decision-making. No unreasonable differential treatment of individuals in terms of transaction prices or other transaction terms may be implemented. When conducting business marketing and information push delivery through automated decision-making, personal information handlers shall simultaneously provide the option not to target personal characteristics of an individual, or provide the individual with a convenient channel for rejection.

iii Data subject rights

According to the PIPL, the personal information subject has the right to be informed, right to access, right to portability, right to correction, right to restriction of processing, right to object and right to delete. The Specification contains similar data subject rights.

Right to be informed

Individuals are entitled to know certain information in relation to the processing of their personal information. Prior to the processing of personal information, the following information should be provided to individuals in a conspicuous way , in clear and easy-to-understand language, and in a truthful, accurate and complete manner:

a the name or personal name and the contact details of the controller;
b the purpose and method of processing;
c the categories of personal information;
d the retention period;
e the method and procedure for individuals to exercise their rights;
f the necessity of the processing and the impacts on the individual when processing sensitive personal information; and
g other matters to be notified in accordance with the provisions of laws and administrative regulations.

Right to access and copy

Individuals have the right to access and copy their personal information from personal information handlers, except if there is any circumstance that should be kept confidential and is not required to be disclosed as stipulated by laws or administrative regulations or in case of emergencies where it is impossible to promptly inform the individuals as necessitated for the protection of the life, health or property safety of a natural person.

Where individuals request access to or the copying of their personal information, the personal information handler shall provide it in a timely manner.

The Specification further provides that where a personal information subject raises a request to access their personal information that is not voluntarily provided by itself, the personal information controller may decide whether to agree to the request or not and give reasons, after comprehensively taking into account the likely risks and damage that may arise to the personal information subject's legal rights and interests if it disagrees with his or her request, technical feasibility, costs of agreeing to the request, and other related factors. Moreover, a personal information controller may, upon the request of a personal information subject, make it possible for the subject to obtain a copy of the following categories of his or her own personal information, or directly transit a copy of the following categories of his or her own personal information to a third party, provided that the technology is practicable:

a the subject's basic information and information about his or her identification; and
b the information about the subject's health, psychological status, education and employment.

Right to portability

Where individuals request their personal information to be transferred to another personal information handler they designate, if such request meets the conditions of the state cybersecurity and information department, personal information handlers shall provide a channel to transfer their personal information.

Right to correction

Where individuals discover that their personal information is incorrect or incomplete, they have the right to request personal information handlers to correct or complete their personal information. Where individuals request to correct or complete their personal information, the personal information handler shall verify the personal information and correct or complete it in a timely manner.

Right to restriction of processing and right to object

Individuals have the right to restrict or object the handling of their personal information by others, unless otherwise provided by laws and administrative regulations. The PIPL broadly states that individuals have the right to restriction of processing and the right to object, while not providing specific circumstances to trigger these rights.

Right to delete

Personal information handlers shall, on their own initiative, delete personal information in any of the following circumstances: otherwise, the individual has the right to request the deletion if the personal information handlers fail to do so:

a the handling purpose has been achieved is unable to be achieved, or the personal information is no longer required for the handling purpose;
b the personal information handlers cease to provide products or services, or the agreed retention period has expired;
c the individuals withdraw their consent;
d the personal information handlers violate laws, administrative regulations, or the agreements in handling personal information; or
e other circumstances provided by laws and administrative regulations.

Where the retention period provided in laws and administrative regulations has not expired, or it is technically difficult to delete personal information, the personal information handler shall cease to handle the personal information, except for storage or taking necessary safeguard measures.

iv Specific regulatory areas

Workplace privacy

There are no specific provisions in Chinese laws and regulations regarding workplace privacy protection. It is generally believed that in the daily operation management, for the need of supervision and management of employees' work, enterprises may to some extent monitor the behaviour of employees, which is generally considered to fall under the enterprise's business autonomy scope and has certain legitimacy. For example, normally companies will not be challenged for obtaining images of employees through a camera, fingerprints of employees through attendance machines, or information about employees' location

through an app location function, which often involves collection of sensitive information of employees (whereabouts and tracks, biometric information, etc.). However, for the purpose of protecting the privacy of employees, enterprises should first ensure that the above-mentioned monitoring measures, as well as the employee information they collect, are for a legitimate purpose and are necessary for business operations, and avoid collecting or monitoring any employee information during non-working hours and outside the workplace. Second, the type, purpose, manner of collection and protective measures of the information collected should be notified to the employee, and the employee's written consent should be obtained.

Children's privacy

According to the Provisions on Cyber Protection of Personal Information of Children, network operators that collect, use, transfer or disclose personal information of children shall, in a notable and clear way, notify children's guardians of their practices, and obtain the consent from children's guardians.

Health and medical privacy

The Measures for the Management of Population Health Information (on Trial), the Law on Licensed Doctors of the PRC, the Nurses Ordinance, the Regulations for Medical Institutions on Medical Records Management and the Information Security Technology – Guide for Health Data Security provide the requirements for medical institutions and staff to protect patients' personal information. For example, the Regulations for Medical Institutions on Medical Records Management require that, 'medical institutions and medical staff shall strictly protect patient privacy. Any leakage of patients' medical records for non-medical, non-teaching or non-research purposes is forbidden'.[2] It also provides the keeping, saving, borrowing and copying of the medical records.[3]

Biometric information

According to the PIPL, biometric information belongs to sensitive personal information. Only when personal information handlers have specific purposes and sufficient necessity and under circumstances of strict protection measures, shall they be allowed to process biometric information. Additionally, separate consent of the individual and prior personal information protection impact assessments are needed to process biometric information.

The Specification also provides guidance on collection and use of personal biometric information. According to the Specification, personal biometric information includes personal gene, fingerprint, voiceprint, palmprint, auricle, iris, facial recognition features, etc. Before collecting personal biometric information, personal information controller should serve a separate notice to the personal information subject of the purpose, method and scope of the collection and use of the personal biometric information, as well as the storage period and other processing rules and obtain the personal information subject's explicit consent. In principle, personal biometric information should not be shared or transferred. If it is truly necessary to share or transfer personal biometric information owing to business needs, the personal information controller should separately inform the personal information subject of

2 Article 6 of the Regulations for Medical Institutions on Medical Records Management.

3 Article 16 of the Regulations for Medical Institutions on Medical Records Management.

the purpose of the sharing and transfer, the category of the personal biometric information involved, the identity and data security capacity of the data recipient, and obtain the personal information subject's explicit consent.

The Specification also emphasises that personal biometric information should be stored separately from personal identity information. In principle, the original personal biometric information (such as samples, images, etc.) should not be stored. The measures that can be taken include but are not limited to:

a storing only the summary information of personal biometric information;

b using personal biometric information directly in the collection terminal; and

c deleting the original image, which can extract personal biometric information after using facial recognition features, fingerprint, palmprint, iris to identify, authenticate and other functions.

Financial privacy

The Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information and the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests provides the obligations that banking and financial institutions should fulfil. According to the two notices, personal financial information includes personal identity information, personal property information, personal account information, personal credit information, personal financial trading information, derivative information and other personal information obtained and preserved in the process of establishing a business in relation with a person. In protecting personal financial information, banking financial institutions should strictly abide by the legal provisions, establish and improve the internal control by-laws, improve the information security technology prevention measures, strengthen the training of the professionals and intensify professionals' awareness of personal financial information security. Provision of personal financial information collected inside China abroad is not allowed unless otherwise required by laws and regulations and the PBOC.

The newly published Draft Credit Reporting Measures by the PBOC tightens the regulation of credit reporting activities. According to the Draft Credit Reporting Measures, credit reporting agencies shall:

a obtain the consent of individuals, and clearly inform individuals of the purpose of collecting credit information, source of information, scope of information, and possible adverse consequences of disagreement with the collection of information;

b adhere to the principle of 'minimum and necessary' and not collect excessive information;

c examine and verify any information provider's business legality, source of information, information quality, information security and authorisation of individuals or enterprises, to ensure the legitimacy, accuracy and sustainability of the collection of credit information;

d clarify with information providers their respective rights and obligations in terms of data correction, objection handling and information security; and

e develop a plan for collecting individual credit information, and report such matters as collected data items, degree of association with credit and the protection of the rights and interests of individuals to the PBOC.

v Technological innovation

Cookies

For the use of cookies, the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps provides that, 'For the collection of personal information by using cookies and similar technologies (including scripts, clickstreams, web beacon, flash cookie, embedded web links, SDK, etc.), the purposes and types of personal information collected shall be clearly presented to the users.'[4] For the use of cookies, generally companies will describe such use in the privacy policy, rather than setting up a separate pop-up on the web page.

Automated decision-making

The PIPL stipulates that when using personal information to conduct automated decision-making, personal information handlers shall guarantee the transparency of their automated decision-making and the fairness and justice of their results. No unreasonable differential treatment of individuals in terms of transaction prices or other transaction terms may be implemented. . When conducting business marketing and information push delivery through automated decision-making, personal information handlers shall simultaneously provide the option not to target personal characteristics of an individual, or provide the individuals with a convenient channel for rejection. In the case of automated decision-making, if any decision has a material impact on individual rights and interests, the individual has the right to require the relevant personal information handler to give an explanation and refuse the said personal information handler making decisions only by means of automated decision-making.

The Specification also provides that where the information system used by the personal information controller in business operations has an automatic decision-making mechanism and can have a significant impact on the rights and interests of personal information subjects (for example, automatically determining the subject's credit status and the quota of credit loans available to the subject, or used for automated screening of interviewers), the personal information controller shall:

a carry out the personal information security impact assessment in the planning and design stage or before the first use, and take effective measures to protect the personal information subject according to the assessment results;

b carry out the personal information security impact assessment regularly (at least once a year) during use, and improve the measures to protect the personal information subject according to the assessment results; and

c provide a complaint channel for personal information subjects for automatic decision-making results, and allow manual review of the automatic decision-making results.

4 Item 21, part 2 of the Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps.

Anonymisation and de-identification

Under the PIPL, anonymisation refers to the process of handling any personal information to make it unable to identify a specific natural person and unable to be restored to its original state. After anonymisation treatment, such information does not belong to personal information. De-identification refers to the process of handling any personal information to make it unable to identify a specific natural person without the help of additional information.

The Information Security Technology – Guide for De-Identifying Personal Information provides some practical guidance for the application of de-identification technologies, which describes the objects and principles of de-identification as well as the process and administrative measures to perform de-identification.

Facial recognition

On 27 July 2021, the Supreme People's Court issued the Provisions on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Face Recognition Technology to Process Personal Information (FRT Provisions), which came into effect on 1 August. With the aim of curbing the abuse of facial recognition technology (FRT) at the judicial level, the FRT Provisions set forth some detailed circumstances where using FRT is considered to be infringing national persons' civil legal rights.

Among other things, the Provisions provide that where an information processor falls under any of the following circumstances in the processing of facial information, the People's Court shall decide that it is an infringement on the personality rights and interests of a natural person:

a failing to disclose the rules for the processing of facial information or to clearly indicate the purpose, method or scope of processing; and

b where the processing of facial information is subject to an individual's consent, the separate consent of the natural person or his or her guardian is not obtained, or the written consent of the natural person or his or her guardian is not obtained in accordance with laws and administrative regulations.

The FRT Provisions also provide that facility management enterprises and other building management entities shall not use face recognition as the only verification method for entry and shall provide other reasonable verification methods.

The Information Security Technology – Requirements for Security of Face Recognition Data (Draft for comments) put forwards some basic security requirements, security processing requirements and security management requirements for facial recognition data. It divides typical applications of facial recognition technology into three categories: verification (1:1 matching), identification (1:N matching) and analysis (no 1:1 matching or 1:N matching is carried out, and only statistics, detection or feature analysis are performed on the collected facial images).

When carrying out facial verification or facial recognition, at least the following requirements should be met:

a the security or convenience of the non-facial recognition method is significantly lower than that of the facial recognition method;

b in principle, facial recognition should not be used to identify minors under the age of 14;

c alternative identification method other than facial recognition should be provided to the data subject;

d security measures should be provided to ensure the informed consent of data subjects; and

e facial recognition data should not be used for purposes other than verification and recognition, including but not limited to evaluating or predicting the work performance, economic status, health status, personal preferences of the data subject.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

China has not yet concluded any international data protection framework or agreements.

Article 37 of the CSL stipulates that:

> *Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail.*

Although the CSL provides the obligations for the CIIOs to localise the personal information and important data collected and generated inside China, it does not elaborate on the definition and specific scope of the CII and the 'important data'; nor does it provide operational guidelines for the specific requirements of data localisation and security assessment for cross-border data transfer. Related implementation regulations and national standards are still in the process of being drafted.

In May 2019, the CAC issued the Measures on Data Security Management (Draft for Comments), which provides that, 'important data' refers to the kind of data that, if divulged, may directly affect national security, economic security, social stability and public health and security, such as undisclosed government information, large-scale population, genetic health, geography and mineral resources, etc. Important data usually does not include information related to the production and operation and internal management of enterprises or personal information, etc.'[5] and '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.'[6]

In June 2019, the CAC issued the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments). It provides 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.'[7] 'If it is identified by the security assessment that the

5 Article 38 of the Measures on Data Security Management (Draft for Comments).

6 Article 28 of the Measures on Data Security Management (Draft for Comments).

7 Article 3 of the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments).

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 allowed.'[8]

According to the Measures on Data Security Management (Draft for Comments) and the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments), whether the important data and personal information can be transferred abroad should be decided by the government. Whether these controversial requirements will pass as they are remains to be seen.

The DSL also contains some high-level restrictions for cross-border flow of data, which should be read in conjunction with Article 37 of the CSL. Article 31 of the DSL provides that:

> *The security administration of the cross-border transfer of important data collected and generated by critical information infrastructure operators during their operation in China shall be subject to the provisions of the Cybersecurity Law of the People's Republic of China; the administrative measures for the cross-border transfer of important data collected and generated by other data handlers during their operation in the People's Republic of China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council.*

The same data localisation obligations for CIIOs can also be found in the PIPL. Article 40 of the PIPL provides that:

> *Critical information infrastructure operators and personal information handlers who handle personal information up to the amount as specified by the national cyberspace authorities shall store within the territory of the People's Republic of China the personal information which they collect and generate within the territory of the People's Republic of China. If it is really necessary to provide such information overseas, critical information infrastructure operators and personal information handlers shall pass security assessment organised by the national cyberspace authorities; if any law, administrative regulation or the national cyberspace authorities stipulate that security assessment may not be conducted, such provision shall prevail.*

Under the PIPL, a personal information handler can only transfer personal information overseas when it meets at least one of the following conditions:

a having passed the security assessment organised by the national cyberspace authorities;

b having undertaken personal information protection certification conducted by professional agencies in accordance with the regulations of the national cyberspace authorities;

c having signed a contract with the overseas receiving parties in accordance with the standard contract formulated by the national cyberspace authorities, to stipulate the rights and obligations of the parties, and supervising their personal information processing activities to ensure that the personal information protection levels under the PIPL are met; or

d meeting other conditions stipulated by laws, administrative regulations or the national cyberspace authorities.

8 Article 2 of the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comments).

If personal information handlers provide personal information overseas, they shall take any necessary measure to ensure that the activities of processing of the personal information provided by them carried out by overseas recipients meet the standards of personal information protection provided in this Law. Moreover, they shall inform the data subject of the name or personal name and contact information of the overseas recipient, the processing purpose and method, the type of personal information to be processed, as well as the way and procedures by which the data subject can exercise his or her rights and interests against the overseas recipient, and obtain the separate consent of the data subject. Furthermore, cross-border transfer of personal information is also subject to a personal information protection impact assessment.

As for the forensics of cross-border electronic data evidence, Article 4 of the Law on International Criminal Judicial Assistance provides that:

> *No foreign institution, organisation or individual may conduct criminal proceedings prescribed by this Law within the territory of the People's Republic of China without the approval of the competent authority of the People's Republic of China, and no institution, organisation or individual within the territory of the People's Republic of China may provide evidentiary materials and assistance prescribed by this Law to foreign countries.*

Article 36 of the DSL stipulates that:

> *The competent authority of the People's Republic of China shall handle the request for providing any data from a foreign judicial body and law enforcement body in accordance with relevant laws and the international treaty or agreement which the People's Republic of China has concluded or acceded to, or under the principle of equality and mutual benefit. Any organisation or individual within the territory of the People's Republic of China shall not provide any foreign judicial body and law enforcement body with any data stored within the territory of the People's Republic of China without the approval of the competent authority of the People's Republic of China.*

Similarly, Article 41 of the PIPL also stipulates that:

> *Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.*

Compared to the rules under the Law on International Criminal Judicial Assistance, this new requirement appears to apply to all types of data and personal information as well as all types of foreign legal proceedings. Thus, the new requirement set forth by the DSL and PIPL will have a greater impact on cross-border legal proceedings and law enforcement activities.

V COMPANY POLICIES AND PRACTICES

Based on existing regulations and draft regulations, it appears that personal information handlers and network operators will eventually be required to establish a complete privacy or data management programme. Relevant data protection and cybersecurity requirements can be found mainly in the DSL, the CSL and the PIPL.

Some high-level compliance obligations stipulated by the DSL include:

a Internal data security management system: creating and developing data security management system across the whole data flow.

b Education and training: organising and conducting data security education and training.

c Technical security measures: taking appropriate technical measures and other necessary measures to ensure data security.

d Multi-level protection scheme (MLPS): MLPS forms the basis for various data security protection obligations, such as establishing a whole-process data security management system, organising data security education and training, and taking appropriate technical measures.

e Data security officer (DSO): controllers that process important data shall designate responsible personnel and management bodies for data security and fully implement data security protection responsibilities.

f Incident detection and emergency plans: strengthening security risk monitoring, adopting remedial measures where security risks such as data security flaws and vulnerabilities are detected, taking disposal measures and notifying the impacted individuals if required by law and reporting to relevant competent authorities.

g Risk assessment: controllers that process important data shall periodically conduct risk assessments for their data processing activities, and submit the risk assessment report to relevant competent authorities. The risk assessment report shall include the categories and quantities of important data processed by the controller, how data is processed, the data security risks and their countermeasures.

The CSL provides some high-level generic network security requirements. For example, under the CSL network operators should formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity, and implement the responsibility for cybersecurity protection. In addition, network operators shall formulate contingency plans for cybersecurity incidents, and promptly deal with system bugs, computer viruses, network attacks and intrusions and other security risks; network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent such information from being divulged, damaged or lost. If personal information has been or may be divulged, damaged or lost, it is necessary to take remedial measures immediately, inform users promptly according to the provisions and report the same to the relevant competent departments.

The PIPL provides that a personal information handler is required to fulfil the following personal information protection requirements:

a Internal policies and operational procedures: creating internal management policies and rules and operating procedures.

b Categorised management of personal information: implementing categorised management of personal information.

c Technical security measures: taking appropriate security technical measures such as encryption and de-identification.

d Access privilege: reasonably determining the operating permission for personal information processing.

e Education and training: conducting security education and training for employees on a regular basis.

f Emergency plans: creating and organising the implementation of emergency plans for personal information security incidents.

g Data protection officer (DPO): appointing a personal information protection officer responsible for supervising the processing of personal information and the adopted protection measures, if the amount of the personal information processed reaches a certain threshold as determined by the CAC.

h Auditing: the controller shall conduct regular audits of personal information processing activities. For any considerable risk existing in a personal information processing activity or any personal information security incident discovered by authorities performing personal information protection duties in the course of performing their duties, the authorities may, according to their powers and procedures as prescribed, conduct a regulatory talk with the legal representative or main responsible person(s) of the controller concerned, or request the controller to entrust a professional institution to audit the compliance of the personal information processing activity. The controller shall adopt measures as required to rectify and eliminate any hazard discovered.

i Impact assessment and processing activity recording: carrying out personal information protection impact assessments prior to certain kinds of processing activities, including: processing sensitive personal information; performing automated decision-making based on personal information; entrusting any other person with personal information processing, providing personal information to other personal information handlers, or disclosing personal information; transferring personal information overseas; and other personal information processing activities with a significant impact on the rights and interests of data subjects.

j Data subject request: establishing an accessible mechanism to receive and handle the requests of data subjects.

VI DISCOVERY AND DISCLOSURE

Article 18 of the Anti-Terrorism Law requires that:

> *telecommunications business operators and internet service providers shall provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by public security authorities and national security authorities in accordance with the law.*

Article 35 of the DSL also provides that:

> *Where public security bodies and national security bodies need to consult any data in order to safeguard national security or investigate a crime in accordance with the law, they shall, in accordance with the relevant provisions of the State, undergo strict approval procedures and proceed with the matter in accordance with the law; and the relevant organisations and individuals shall render cooperation.*

In addition, the Specification stipulates that in principle personal information shall not be publicly disclosed. When the personal information controller is authorised by law or has reasonable grounds for public disclosure, it should meet the following requirements:

a conduct a personal information security impact assessment in advance and take effective measures to protect the personal information subject based on the assessment results;

b inform the subject of personal information of the purpose for the public disclosure and categories of personal information to be disclosed, and obtain the explicit consent of the subject of personal information in advance;

c before publicly disclosing personal sensitive information, the subject of personal information should also be informed of the content of personal sensitive information involved;

d accurately record and store the public disclosure of personal information, including the date, scale, purpose and scope of public disclosure;

e bear the corresponding responsibility for the damage caused by the public disclosure of personal information to the legitimate rights and interests of personal information subjects;

f personal biometric information should not be publicly disclosed; and

g analysis results of personal sensitive data such as race, ethnicity, political views and religious beliefs of citizens should not be publicly disclosed.

However, a personal information controller need not seek the authority and consent of personal information subjects in advance where:

a the sharing, transfer or public disclosure is related to the performance of obligations under laws and regulations by the personal information controller;

b the sharing, transfer or public disclosure is in direct relation to state security or national defence security;

c the sharing, transfer or public disclosure is in direct relation to public security, public sanitation, or major public benefits;

d the sharing, transfer or public disclosure is in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;

e the sharing, transfer or public disclosure is for the sake of safeguarding significant legal rights and interests, such as the life and property, of personal information subjects or other individuals, but it is difficult to obtain their consent;

f the personal information to be shared, transferred or publicly disclosed is voluntarily made public by personal information subjects themselves; and

g the personal information is collected from information that has been legally and publicly disclosed, such as legal news reports and information published by the government.

Information disclosure required by foreign government agencies shall comply with Article 4 of the Law on International Criminal Judicial Assistance and Article 36 of the DSL.

VII PUBLIC AND PRIVATE ENFORCEMENT

Enforcement agencies

Article 8 of the CSL provides that 'The national cyberspace administration authority is responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration work. The competent telecommunication department

of the State Council, public security departments and other relevant authorities shall be responsible for protecting, supervising and administering cybersecurity within the scope of their respective responsibilities in accordance with the provisions of this Law and other relevant laws and administrative regulations. Responsibilities of relevant departments under local people's governments at or above the county level for protecting, supervising and administering cybersecurity shall be determined in accordance with the relevant.'

For undesirable practices, the main measure taken by the CAC is to interview the responsible persons of relevant network operators. For example, on 6 January 2018, the Network Security Coordination Bureau of the CAC interviewed relevant representatives of Alipay and Zhima Credit and pointed out that the way of using and collecting personal information in Alipay and Zhima Credit is not in line with the spirit of the Specification.

The competent telecommunications department under the State Council (i.e., the MIIT) from time to time issues notifications to organise and carry out administrative checks on network security in the telecommunications and Internet industries. For example, on 30 May 2019, the Network Security Administration of the MIIT issued a circular on the administrative inspection of network security in the telecommunications and internet industries in 2019, requiring all telecommunications and internet enterprises to cooperate in the network security inspection work.[9] At the same time, local telecommunications authorities usually notify enterprises that fail to implement their network security obligations. For example, on 12 July 2018, the Shanghai Communication Administration notified four internet enterprises that their network security requirements had not been implemented effectively.[10]

The MPS is mainly responsible for the protection of cybersecurity levels. For example, it issued the Regulation on Network Security Graded Protection (Draft for Comment) in June 2018 and the Provisions on Internet Security Supervision and Inspection by Public Security Organs in September 2018. At the same time, the MPS has launched the campaign 'Network Clearance Campaign' to punish illegal activities on the internet.[11]

In recent years, with the frequent occurrence of security incidents on mobile internet, China has established the App Special Governance Panel, an organisation formed by the NISSTC and three other associations to assist government in investigating and evaluating unlawful collection and use of personal information by Apps.

In addition, the competent authorities of various industries also have the right to supervise violations in their industries. For instance, the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests provides that 'A financial consumer shall, when having any dispute on financial consumption with a financial institution, file the complaint with the financial institution first in principle. If the financial institution refuses to accept the complaint or fails to handle the complaint within a certain time limit, or the financial

9 MIIT, the Circular on Doing a Good Job in the Administrative Inspection of Network Security in the Telecommunications and Internet Industries in 2019. http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c6983820/content.html.

10 MIIT, The Shanghai communication administration notified four internet companies in which the implementation of network security requirements was inadequate. http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057733/c6254778/content.html.

11 The MPS notification of launching the 2018 'Net Action' campaign, http://www.mps.gov.cn/n2254536/n2254544/n2254552/n6422073/index.html; The MPS notification of typical cases of launching the2019 'Net Action' campaign, http://www.mps.gov.cn/n2254536/n2254544/n2254552/n6528162/index.html.

consumer is of the opinion that the financial institution's processing result is irrational, the financial consumer may file a complaint with the PBC branch at the place where the financial institution is located, the disputes occur or the contract is signed.'

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations face significant compliance challenges in relation to data localisation requirements. requirements stipulated by the CSL, the DSL and the PIPL respectively.

Article 37 of the CSL provides that:

> *Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the PRC. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail.*

Article 31 of the DSL provides that:

> *The security administration of the cross-border transfer of important data collected and generated by critical information infrastructure operators during their operation in China shall be subject to the provisions of the Cybersecurity Law of the People's Republic of China; the administrative measures for the cross-border transfer of important data collected and generated by other data handlers during their operation in the People's Republic of China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council.*

Article 40 of the PIPL provides that:

> *Critical information infrastructure operators and personal information handlers who handle personal information up to the amount as specified by the national cyberspace authorities shall store within the territory of the People's Republic of China the personal information which they collect and generate within the territory of the People's Republic of China. If it is really necessary to provide such information overseas, critical information infrastructure operators and personal information handlers shall pass security assessment organised by the national cyberspace authorities; if any law, administrative regulation or the national cyberspace authorities stipulate that security assessment may not be conducted, such provision shall prevail.*

However, until now, neither the operational guidelines to identify the specific scope of CII and 'important data' have been issued; nor has the threshold amount of personal information processing been prescribed by the national cyberspace authority. It is difficult for foreign organisations to predict whether they will fall under the strict data localisation rules.

Nevertheless, a number of industries have also enacted restrictions on specific data localisation, as described below.

i Banking

The Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information and the Notice of the People's Bank of China on Issuing the Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests both provide that personal financial information acquired inside China shall be stored, processed and analysed inside China and no personal financial personal information acquired inside China should be transferred abroad, except as otherwise required by law, regulation or provisions.

ii Insurance

Article 82 of the Standards for the Financial and Accounting Work of Insurance Companies (2012) requires that 'the business and financial data in the financial information system of an insurance company shall be stored inside the territory of China and backed up off-site.'

iii Credit investigation industry

Article 24 of the Regulation on the Administration of Credit Investigation Industry provides that credit investigation institutions shall arrange, save and process information collected inside China within the territory; and if transferring the information abroad, it shall abide by relevant laws and regulations.

iv Mails and express mails

Article 16 of the Measures for the Administration of the Real-Name Receipt and Delivery of Mails and Express Mails provides that delivery enterprises should store the user information and important data collected and generated by it during its receiving and sending activities inside China within the territory.

v Population health information

Article 10 of the Measures for the Administration of Population Health Information provides that responsible units shall not store information on the population on any server outside China, nor shall they host or lease any server outside China.

Article 30 of the National Health and Medical Big Data Standards, Safety and Service Management Measures (trial) provides that specifies that, if it is indeed necessary to provide health and medical Big Data abroad due to business needs, it shall be subject to security assessment and audit as required by relevant laws and regulations.

vi Online taxi-booking business operations and services

Article 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services provides that an online taxi booking platform company shall store and use the personal information collected and business data formed in China; and the information and data shall not be provided abroad, unless otherwise required by laws and regulations.

vii Map

Article 34 of the Regulation on Map Management provides that an internet map service entity should set the server storing map data inside China.

viii Network of civil aviation

Article 28 of the Interim Measures of Civil Aviation Network Information Security Management (Draft for Comment) stipulates that personal information and important data collected and generated by important information systems in operation inside China shall be stored within the territory.

IX CYBERSECURITY AND DATA BREACHES

According to the DSL, the state shall establish a centralised, efficient, and authoritative mechanism for data security risk assessment, reporting, information sharing, supervision, and early warning. The national data security coordination mechanism shall make overall planning for and coordinate relevant departments in strengthening their work in the collection, analysis, determination, and early warning of the data security risk information.[12] Notably, the state shall establish a data security review system, where data handling activities that affect or may affect the national security will undergo national security review.[13] When carrying out data activities, enterprises shall strengthen risk monitoring, and take immediate remedial measures when data security defects and loopholes are found. When data security incidents occur, users shall be informed in time and reported to relevant competent authorities.[14]

The CSL is more focused on cybersecurity than personal information protection and has proposed the concepts of 'network operation security' and 'network information security'. Article 21 of Chapter III (Network Operation Security) provides that the state implements a multiple-level protection scheme (MLPS) for cybersecurity and network operators should prevent the network from interference, damage or unauthorised access and network data from being divulged, stolen or falsified.

Article 25 of the CSL provides that network operators should formulate contingency plans for cybersecurity incidents and deal with system bugs, computer viruses, network attacks and intrusions in a timely manner; if the incident endangers cybersecurity, network operators shall immediately initiate the contingency plan, take remedial measures and report to the relevant competent authority.

In addition, the CSL provides separately that operation security of CII. The CII is related to national economy and people's livelihoods, national security and public interests, and involves important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services and e-government. But the CSL does not specify the specific scope of CII and security protection methods.

According to the Article 21 of the CSL, all network operators in China are obligated to participate in the MLPS. From late 2018 to May 2019, the MPS and other departments jointly issued several national standards on the MLPS. These standards include network infrastructure, important information systems, large internet websites, big data centres, and cloud computing platforms, 'internet of things' systems, industrial control systems, and public service platforms. In addition, these standards put forward new security expansion requirements for new technologies of cloud computing, internet of things, mobile internet, industrial control and big data.

12 Article 22 of the DSL.

13 Article 24 of the DSL.

14 Article 29 of the DSL.

Article 40 of Chapter IV Network Information Security provides that 'Network operators shall strictly keep confidential users' personal information that they have collected, and establish and improve the users' information protection system.' Article 55 of the CSL provides that '[f]or the occurrence of cybersecurity incidents, it is necessary to activate contingency plans for cybersecurity incidents immediately, investigate and assess such incidents, require network operators to take technical measures and other necessary measures to eliminate potential security hazards, prevent expansion of the harm, and promptly issue warning information in relation to the public to society.'

X OUTLOOK

With the promulgation of the CSL the DSL and the PIPL, the Chinese data protection and cybersecurity legal regime has been formulated. These three laws complement each other and constitute the cornerstones of China's legal regime for cybersecurity and data protection.

Appendix 1

ABOUT THE AUTHORS

HONGQUAN (SAMUEL) YANG

AnJie Law Firm

Hongquan (Samuel) Yang leads AnJie Law Firm's technology, data protection and cybersecurity practice. He has worked as in-house counsel and external lawyer in the technology, media and telecoms sector for nearly 20 years and is regarded as a true expert in these areas in China. He advises clients on a wide range of regulatory, commercial and corporate matters, especially in the areas of telecommunications, cybersecurity, data protection, the internet, social networking, online games, hardware and software, technology procurement, transfer and outsourcing, distribution and licensing, and other technology-related matters.

Samuel has been recognised as a Global Leader: Data (*Who's Who Legal*, 2021), a Leading Individual: TMT (*The Legal 500* 2020, 2021), a Leading Individual: Data (*The Legal 500* 2021), a recommended TMT lawyer (*Chambers and Partners*, 2021), a Band 1 Cyber Security and Data Protection Lawyer (*LEGALBAND* 2019, 2020) and one of the Top 15 Cyber Security and Data Protection Lawyers in China (*LEGALBAND* 2021). *The Legal 500* commented that Samuel and his team at AnJie have a particular strength in 'telecoms-related regulatory and general commercial legal services' and 'issues such as cyber security and data protection areas' and have 'built a real niche' in these areas, and he 'is probably one of the leading authorities on data protection, and his good industry knowledge is helpful in assisting clients to mitigate their risks.' *Chambers and Partners* commented that he 'is a capable partner, a very effective person, and he responds rapidly and is very client-oriented.'

Samuel mainly serves Fortune 500 companies, large state-owned enterprises and leading Chinese internet companies. Samuel is a regular contributor to many legal journals and his publications regarding Chinese data protection and cybersecurity laws are well-received and widely reproduced.

ANJIE LAW FIRM

19/F, Tower D1
Liangmaqiao Diplomatic Office Building
No. 19 Dongfangdonglu
Chaoyang District
Beijing 100600
China
Tel: +86 10 8567 5988
Fax: +86 10 8567 5999
yanghongquan@anjielaw.com
www.anjielaw.com

an LBR business

ISBN 978-1-83862-810-9