Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cloud Computing 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers

China: Law & Practice

Vincent Wang, Xinyao Zhao and Lewis Chen
Global Law Office

CHINA

Law and Practice

Contributed by:
Vincent Wang, Xinyao Zhao and Lewis Chen
Global Law Office

Contents

Global Law Office (GLO) dates back to the establishment of the Legal Consultant Office of China Council for the Promotion of International Trade (CCPIT) in 1979. With the approval of the Ministry of Justice of the People's Republic of China, it was renamed "China Global Law Office" in 1984, signalling its commitment to an international perspective and full engagement with the global community. Through over four decades of dedicated effort and growth, GLO has emerged as a leading, full-service law firm within China's legal landscape. From its inception, GLO has embraced the mission of "serving domestic and foreign clients with a globalised vision, globalised team, and globalised quality". This commitment has allowed it to consistently maintain a position at the forefront of the industry, even amidst the dynamic and ever-evolving global economic environment.

Authors

Vincent Wang is a partner at Global Law Office, working in the Shanghai office. His practice encompasses a wide range of industries, with particular expertise in navigating novel and complex legal challenges in the TMT sector. Examples of the industries Vincent covers include telecommunication, ecommerce, cybersecurity and data protection, electronic payments, internet-related businesses, high technology manufacture and engineering, new and emerging technologies (such as AI, blockchain, crypto-currency, IoTS, e-mobility, cloud computing, etc), e-automotive, new media and streaming entertainment, food and beverage, agriculture and farming, and cross-border trade and investment.

Xinyao Zhao is of counsel at Global Law Office. Xinyao is based in the Shanghai office, which she joined in 2018. Her main practice areas include cyber and data security, personal information protection, and corporate regulatory compliance. She specialises in advising both multinational and domestic companies in areas including telecoms, internet-related industries, IoT, automotive, ecommerce, fintech and healthcare. She has advised well-known international companies in completing their data compliance projects, providing support throughout the implementation process. Additionally, Xinyao has assisted domestic companies with their overseas business development in the USA, Europe, and Southeast Asia, focusing on data privacy compliance.

Lewis Chen is a mid-level associate at Global Law Office, based in the Shanghai office. His main practice areas cover privacy and data protection, fintech and TMT. He has participated in legal projects for well-known international companies including ByteDance, GE, PwC, etc, covering fintech, automobile, eCommerce, IoT, consulting and other industries. He has also assisted clients with legal matters relating to compliance investigations and mitigation, risk assessment, and the preparation of legal documents. Prior to joining Global Law Office, Lewis worked for a leading international law firm in Shanghai, focusing on data protection and fintech.

Global Law Office

36th Floor
Shanghai One ICC
No. 999 Middle Huaihai Road
Xuhui District
Shanghai 200031
China

Tel: (8621) 2310 8288
Fax: (8621) 2310 8299
Email: vincentwang@glo.com.cn
Web: www.glo.com.cn

环 球 律 师 事 务 所
GLOBAL LAW OFFICE

45th 1979-2024

1. Data Privacy Regulations

1.1 Data Privacy and Cloud Computing

Data Privacy Regulations That Are Applicable to Cloud Computing in China

In the area of data and privacy regulation, PRC law currently has the following major sources: (i) national laws, (ii) administrative regulations and rules, and (iii) national standards.

At the level of national laws, the Cyber Security Law of the PRC (CSL), the Data Security Law of the PRC (DSL), and the Personal Information Protection Law of the PRC (PIPL), are three fundamental laws regulating data and privacy issues, which are applicable to cloud computing and relevant data processing activities in the PRC.

Those three national laws are implemented mainly by administrative regulations, rules and regulatory documents issued by the competent regulatory governmental agencies. For example, the Measures on Assessing the Security of Cloud Computing Services specifies the security requirements of the Cyber Security Law and the Data Security Law in the scenario where the cloud computing services are provided to the administration agencies, the operators of Critical Information Infrastructure (CII) and the party offices.

In addition, the national standards, compulsory and recommended, also play an important role in implementing those three laws from the perspective of technical, organisational and law-fulfilling measures. The compulsory standards establish the minimum requirements for legal compliance, while the recommended standards showcase best practices. For example, the Information security technology – Security guidance for cloud computing service (GB/T 31167-2023) provides recommendations and guidance on security management and technical measures to protect data on the cloud through its life cycle.

Another unique security requirement applicable to the cloud services hosted in China is the Multi-Layer Protection Scheme (MLPS). MLPS is a requirement imposed in accordance with Article 21 of the CSL and focuses on the infrastructure security of the cloud service that facilitates the protection of the data and personal information processed in the cloud service.

Definition of Personal Data and Sensitive Data

Note that in this guide, personal data and personal information, sensitive data and sensitive personal information are used interchangeably with the same meaning.

According to Article 4 of the PIPL, personal data refers to all types of information of identified or identifiable individuals recorded in electronic or other means, excluding anonymous information.

According to Article 28 of the PIPL, sensitive personal data refers to personal data, the leakage or illegal use of which could easily result in damage to the dignity of an individual, or harm to personal body and property, including biometric information, religion, specific identities, medical and health information, financial accounts, location tracking data, as well as the personal data of minors under the age of 14.

Requirements for Processing Personal Data in the Cloud

The data processor under the PIPL is the counterpart of the data controller under the GDPR, and the processing contractor of a data processor is the counterpart of the data processor under the GDPR. As it is inevitable to distinguish

the data controller and the data processor in the cloud environment, for convenience of non-PRC readers, we are using the terms "data controller" and "data processor" of the GDPR in this guide in our responses to the questions about the PRC law.

Therefore, in this article, we are using "data controller" to refer to the "personal information processor" that can autonomously decide the purpose and method of processing data under the PRC law; and "data processor" to refer to the "processing contractor" that is processing data upon the request of the controller.

Chinese laws and regulations do not provide special requirements for processing personal data in the cloud. Processing personal data in the cloud is subject to the same requirements provided in the PIPL for processing personal data in general.

Under the PIPL, the primary requirement for processing personal data is consent or separate consent. There are also legally defined exceptional processing scenarios where no consent or separate consent is required.

Consent and the requirement

Under Article 13 of the PIPL, processing personal data should have a proper legal basis, including consent, or other legal bases that may allow for consent to be waived as illustrated below. To ensure informed consent is obtained, before processing their personal data, a controller must inform individuals truthfully, accurately, and fully of the following information in a prominent way and in clear and plain language:

- the controller's name and contact details;
- processing purposes, methods, information types processed and storage period (which must be the shortest time required to fulfil the processing purpose);
- the option and procedure for individuals to exercise the statutory rights regarding their personal data; and
- other matters required by laws and administrative regulations.

Separate consent and the requirement

Under the PIPL, there are several processing activities that require separate consents, including processing sensitive personal data, cross-border transfers of personal data, providing personal data to a third party, publicly disclosing personal data, etc. While the PIPL itself lacks a precise definition of "separate consent", practical guidance can be found in the recommended national standard GB/T 42574-2023 (Information security technology – Implementation guidelines for notices and consent in personal information processing). This standard clarifies that separate consent signifies a specific, explicit agreement given by the individual solely for a particular processing activity concerning their personal data. Crucially, it does not encompass blanket consent given for multiple processing purposes simultaneously.

Exceptional consent-waiving processing

In addition to consent, the PIPL allows data controllers to process personal data based on several alternative legal grounds:

- where processing is necessary for:
  - (a) entering into or performing the contracts to which the individual is a party;
  - (b) managing human resources in accordance with labour rules or policies or collective employment contracts that are formulated or concluded lawfully;
  - (c) fulfilling statutory duties or responsibilities; and/or

(d) responding to public health incidents, or protecting the life, health and property security of individuals in urgent situations;

- processing personal data for the purpose of news reporting or public opinion-based oversight for the public interest, provided it remains within a reasonable scope; and
- processing the personal data disclosed by an information subject or otherwise lawfully disclosed, provided it remains within a reasonable scope in accordance with the PIPL.

Under these processing conditions, consent can be waived.

Obligations for Data Controllers and Processors in the Cloud Environment

Under PRC law, data controllers should undertake primary legal responsibilities regarding processing personal data, and data processors shall provide necessary assistance for compliance. That is because, in cloud services, data controllers are the customers (cloud tenants or platform users), and their technical capability to comply with the law will be subject to the technical limit provided by the cloud service providers (as data processor).

Data controller's obligations

According to the PIPL, data controllers using the cloud services are subject to the following key obligations:

- Lawfulness and transparency: According to Article 13 and Article 17 of the PIPL, data controllers must ensure that personal data is processed on a lawful basis and disclose data processing activities transparently to data subjects. This includes providing clear information about the purpose, method, and scope of data processing.
- Data security: As stipulated in Article 51 of the PIPL, and Articles 6 and 7 of the Information Security Technology – Personal Information Security Specification (GB/T 35273-2020), data controllers must implement adequate technical and organisational measures to ensure the security, integrity, and confidentiality of data. This includes using security measures such as encryption, anonymisation, access controls, and audit logging.
- Responding to data subject requests: Under Articles 45, 46, and 47 of the PIPL, data controllers are required to establish effective mechanisms to ensure that data subjects can easily exercise their legal rights, including for example, the right of access, correction, deletion, and the right to object to processing.
- Data breach notification: In the event of a data breach, Article 57 of the PIPL mandates that data controllers must take immediate remedial actions and notify both the data protection authorities and affected data subjects.

In the cloud environment, data controllers may expect data processors to provide data compliance measures or offer the technical mechanisms or flexibility to allow them to implement such measures independently. Therefore, cloud service providers, as data processors, may need to understand and anticipate such potential requirements in advance.

Data processor's obligations

Data processors, usually the cloud service providers, are responsible for processing personal data on behalf of data controllers. Their obligations should be geared toward supporting the controller's compliance efforts and ensuring data protection standards are upheld, including:

- Processing in accordance with instructions: Per Articles 21 and 59 of the PIPL, data processors must strictly follow the data controller's instructions and must not process data beyond the scope authorised by the controller.
- Co-operation obligations: Under Article 59 of the PIPL, data processors are obligated to assist data controllers in fulfilling their legal responsibilities, such as providing necessary data for data subject requests.
- Sub-processor management: Under Articles 21 and 59 of the PIPL, if data processing tasks are subcontracted to other service providers, data processors must obtain prior written consent from the data controller and ensure sub-processors comply with applicable data protection requirements.
- Data deletion or return: Under Articles 21 and 47 of the PIPL, upon termination of the processing contract or conclusion of services, data processors must delete or return all personal data as instructed by the data controller and ensure no copies are retained.

1.2 Data Privacy and Cross-Border Transfers

CSL, DSL, and PIPL provide a general framework for cross-border data transfers. In addition to those three fundamental laws, a recent regulation, the Provisions on Promoting and Regulating Cross-border Data Flows, has been in effect since March 2024, further facilitating the cross-border transfer of personal data and other types of data outside of China. These laws apply to cross-border data transfers in the cloud environment as well.

According to the above laws, data controllers should undertake the legal obligation concerning cross-border data transfers in the cloud, and data processors should comply with data controllers' instructions concerning cross-border transfers (for example, the instruction of not transferring personal data outside of China).

Below is a summary of the key PRC laws with respect to cross-border data transfers:

- Regulatory mechanism regarding cross-border transfers of personal data: Data controllers transferring personal data outside of China should choose a proper compliance mechanism. Under Article 38 of the PIPL, such mechanisms include applying for a security assessment, signing the Chinese standard contractual clauses with the foreign data recipients, obtaining personal information protection certification, or meeting other conditions prescribed by the relevant laws and regulations or the Cyberspace Administration of China (CAC). Under the regulatory framework, the Provisions on Promoting and Regulating Cross-border Data Flows provide exemptions, in the hope of making cross-border data transfers easier for international businesses relating to China.
- Notification and separate consents: Before carrying out any cross-border transfer of personal data, the data controller must notify the data subjects about the details of the cross-border data transfer, and obtain separate consents from the data subjects, unless the data controller can rely on a legal basis other than consent of a data subject, as outlined in Article 13 of the PIPL.

Cloud providers as data processors must collaborate with data controllers to ensure that the data transfer arrangements meet Chinese regulatory requirements. This involves aligning cloud security protocols with Chinese standards and providing support for assessments that should be completed by the data controller under the

regulatory mechanism. Data controllers are advised to include specific clauses in their contracts with cloud service providers to address cross-border data transfer obligations. Please see details in **3. Data Ownership and Control**.

1.3 Penalties for Non-compliance With Data Privacy Regulations

Chinese data privacy laws do not impose penalties specifically for data controllers and data processors in the cloud environment. In practice, the penalties vary depending on the role of the legal entities. Below are penalties applicable to each role under Chinese laws and regulations.

Penalties for Data Controllers

Data controllers bear primary responsibility for ensuring the legality, security, and transparency of personal data processing activities. The penalties for non-compliance include administrative penalties, civil liabilities, and criminal liabilities in severe cases.

- Administrative penalties: According to Article 66 of the PIPL, data controllers can face warnings or substantial fines, up to RMB50 million or 5% of the previous year's annual turnover for severe infractions. Regulatory authorities may issue corrective orders requiring data controllers to immediately rectify any identified violations. In serious cases, authorities may order suspension or termination of specific data processing activities, potentially leading to significant business disruption. Profits derived from non-compliant data practices may also be confiscated.
- Civil liability and criminal liability: Data subjects whose rights have been harmed can sue data controllers for compensation. In case of severe violations, data controllers may face criminal charges. Penalties may include imprisonment of responsible individuals, criminal fines, and other legal consequences.

Penalties for Data Processors

Data processors, usually cloud service providers, are responsible for processing personal data according to the instructions of the data controllers. Processors can also face significant penalties for non-compliance.

- Administrative penalties: As is the case with data controllers, authorities can require data processors to rectify non-compliant behaviours. Although data processors generally face lower fines compared to those of data controllers, repeated, multiple or serious non-compliance can still lead to substantial penalties, including fines, warnings, or even suspension of services under the PIPL and other applicable laws. For severe violations, regulators may order data processors to suspend or cease processing activities or confiscate any illegal profits.
- Civil liability and criminal liability: In some cases, data processors may be held liable with data controllers or independently for damages suffered by data subjects or other legal entities and individuals concerned. This may happen when processors fail to follow controllers' instructions or neglect their own security responsibilities. For example, if a processor's negligence leads to data breaches, affected individuals may file claims for compensation against both the data controller and the processor. Data processors involved in illegal activities, such as unauthorised sale or misuse of personal data by the data processor deliberately, may face criminal prosecution. This includes fines, imprisonment, and other criminal sanctions.

2. Data Security Measures

2.1 Data Security and the Cloud

Security Measures Required by the PRC Law for Data Stored in the Cloud

The security of the cloud computing environment is jointly safeguarded by cloud service providers and their customers. The CSL requires operators to take security measures to protect the security of the cloud and services derived from it hosted in China and the data stored in the cloud:

- According to Article 10 of CSL, operators should comply with laws and regulations and compulsory national standards to adopt technical measures and other necessary measures, in order to ensure the security and availability of cloud services and other services derived from it, and to ensure the integrity, confidentiality and availability of the data processed in the cloud and the services derived from it.
- Article 21 of the CSL imposes a general requirement regarding data security measures to protect the security of networks and the integrity, confidentiality and availability of data processed in the cloud and the services derived from it, including: (i) measures to prevent computer viruses, cyber-attacks, network intrusions and other activities that endanger cybersecurity; (ii) measures to monitor and record network operation and cybersecurity events, and maintain the cyber-related logs for no less than six months; and (iii) measures such as data classification, and back-up and encryption of important data, etc.

The PIPL requires personal data controllers to take technical measures to ensure the security of personal data. Legal requirements in the PIPL apply to processing activities of personal data stored in the cloud, which are summarised below:

- Article 51 of the PIPL requires that personal data controllers shall, subject to the purpose and the method of processing personal data, types of personal data, impacts on personal rights and interests and possible security risks, take the following measures to ensure the compliance of personal data processing activities with provisions of laws and administrative regulations, and prevent unauthorised access to, and disclosure, falsification and loss of, personal data:
  - (a) formulating internal management systems and operating procedures;
  - (b) implementing category-based management of personal data;
  - (c) taking corresponding technical security measures such as encryption and de-identification;
  - (d) reasonably determining the permissions to process personal data and conducting security education and training for relevant employees on a regular basis;
  - (e) formulating and organising the implementation of emergency response plans for personal data security incidents; and
  - (f) other measures stipulated by laws and administrative regulations.

The Measures on Assessing the Security of Cloud Computing Services stipulates measures that cloud service providers should comply with when they are providing services to the government and party offices, and the operators of CII. Article 3 of the Measures provides that the security assessment of such cloud services should concentrate on, inter alia: (i) the security of the cloud platform technology, products and supply chain; (ii) the ability to manage security effectively and the strength of the cloud platform's

security protection measures; (iii) the feasibility and ease with which customers can transfer their data; and (iv) the business continuity of the cloud service provider.

In addition, there are a few recommended national standards concerning cloud computing services that specify security measures for cloud services. For example, the standard Information Security Technology – Security Capability Requirements for Cloud Computing Services (GB/T 31168-2023) highlights the security technical measures that cloud service providers need to deploy. There are eleven types of security measures in total, including system development and supply chain, system and communication protection, access control, data protection, management of configuration, operational maintenance, emergency response, audit, risk assessment and continuous monitoring, security management and personnel, and physical and environmental security. The goal of those measures is to ensure the confidentiality, integrity, and availability of data stored in the cloud.

Encryption Standards for Data in Transit and at Rest in the Cloud

- According to the above standard GB/T 31168-2023, cloud service providers should implement encryption measures to ensure the security of data in transit and at rest in the cloud. The standard recommends that cloud service providers take communication encryption and signature verification measures in compliance with the Chinese national encryption management regulations.
- However, if the cloud services are intended to support the administration agencies, the operators of CII and the party offices, such cloud services must adopt the encryption technologies recognised by the Chinese government to comply with the Administration Measures of Commercial Encryption (revised in 2023).

Access Controls in the Cloud Environment

- According to the above laws and national standards, cloud service providers should identify and authenticate personnel, processes, and devices before allowing them access to the cloud computing platform, and restrict the operations they can perform and the functions they can use. For example, the national standard GB/T 31168-2023 recommends different levels of access control measures, depending on the importance of the business and sensitivity of the data. Cloud services providers can adopt proper access control measures depending on the importance of the business and sensitivity of the data, as well as contractual requirements of the cloud customers.
- As a general requirement, cloud service providers are recommended to identify and recognise the users of their information systems and implement multi-factor authentication for privileged account network access. As an enhanced requirement, for example, when data stored on the cloud is critical and sensitive, cloud service providers are recommended to: (i) implement multi-factor authentication for account network access and ensure that at least one factor is provided by a device separate from the system to prevent simultaneous compromise or leakage of multi-factor authentication credentials; and (ii) implement anti-replay authentication mechanisms, such as dynamic passwords, for privileged account network access to ensure that the cloud computing platform can resist replay attacks.
- If the data on cloud is very sensitive, and the associated business operations are criti-

cally important, as an advanced requirement, cloud service providers are recommended to: (i) implement multi-factor authentication for local access to privileged accounts; and (ii) implement anti-replay authentication mechanisms, such as dynamic passwords, for network access by non-privileged accounts to ensure that the cloud computing platform can resist replay attacks.

Handling of Security Accidents and Breaches in the Cloud

- According to the CSL, PIPL, and the Administrative Measures on Data Security in the Fields of Industry and Information Technology, cloud service providers should develop emergency response plans for the cloud computing platforms and conduct regular drills to ensure the availability of critical information resources in emergencies. In detail, cloud service providers should establish an emergency response plan, and should track, record, and report incidents to relevant personnel. Cloud service providers should also have disaster recovery capabilities and establish necessary back-up and recovery facilities and mechanisms to support the continuity plan of customers' businesses.
- When a data security incident occurs, cloud service providers should promptly carry out emergency response measures according to the emergency response plan. Upon completion of incident handling, a summary report should be prepared within the specified timeframe, and an annual report on data security incident handling should be submitted to the local industry regulatory authorities.

3. Data Ownership and Control

3.1 Data Ownership in Cloud Agreements

Data Ownership and Control in Cloud Agreements

As a basic principle in a typical cloud business, data in the cloud is owned and controlled by the cloud service customers unless otherwise agreed. The cloud service providers and the cloud service customers are recommended to specify in the cloud agreement that:

- All data and data related assets provided by the customer to the cloud service provider as well as data collected, generated, or stored during the operation of the customer's business on the cloud computing platform, are owned and controlled by the customer. Both parties may further stipulate in the agreement that the cloud service provider should ensure the customer retains full rights and obligations over these resources, including the ability to access, utilise, and manage their data on the cloud as needed.
- The cloud agreement may emphasise the customer's control over their data, ensuring that the cloud service provider cannot interfere with or restrict the customer's rights, and providing mechanisms for the customer to efficiently access and manage their data at all times.

Data Subjects' Rights Over Their Data

In the cloud environment, personal data subjects have rights to their personal data as defined in the PIPL, including the right to know and the right to decide how their personal data is processed, unless otherwise provided by the laws and regulations.

Specifically, the data subjects have the following rights:

- the right to check and copy their personal data;
- the right to transfer personal data to a third party designated by the data subjects;
- the right to rectify and supplement their personal data;
- the right to request the deletion of personal data; and
- the right to seek an explanation from the data controller regarding the rules governing the processing of their personal data.

How Can Data Subjects Exercise Their Rights to Access, Rectify, or Delete Their Data

Data subjects need to submit their requests directly to the controller. PIPL requires the data controller to establish a convenient mechanism for accepting and processing requests from personal data subjects in a timely manner.

In the cloud environment, cloud service customers may need support from cloud service providers to fulfil the data subjects' requests concerning their personal data; for example, the right to access, rectify and delete their personal data stored in the cloud. Therefore, in the cloud agreement, the cloud service customer and the cloud service provider may specify the mechanism and procedures to deal with the personal data subjects' requests in detail, as well as Standard Operation Procedures (SOP) that must be followed by both parties.

3.2 Data Portability

Article 45 of the PIPL provides data subjects with a data portability right: Where an individual requests to transfer his/her personal data to a personal data controller designated by him/her that meets the conditions stipulated by the CAC, the personal data controller shall provide a way for the transfer. The PIPL and its relevant laws have not provided details regarding how to respond to the data portability request in the cloud.

The recommended national standards, GB/T 35273-2020 Information security technology – Personal information security specification, provides the best practices regarding data portability. Upon request from the data subject, the data controller should provide a method for the data subject to obtain copies of the following types of personal data or, where technically feasible, directly transfer copies of the following types of personal data to a third party designated by the data subject: (i) basic personal information and identity information, and (ii) health and physiological information, educational and employment information.

To ensure that the right to data portability is respected, both the cloud customer and the cloud service provider are advised to clearly define in the cloud agreement how such requests will be handled.

3.3 Data Retention and Deletion

The general legal requirement provided in the PIPL concerning data retention and deletion applies to processing in the cloud.

- According to PIPL, the cloud service customer, as the controller of the data, should follow the principle of data minimisation when determining the data retention period in the cloud, and the controller of the data needs to delete personal data proactively after expiration of the retention period or upon request of the data subjects to delete the personal data. In such a case, the cloud service provider as the processor should delete the personal data as

provided in the cloud agreement or requested by the cloud customer accordingly.
- According to Article 47 of the PIPL, where the retention period as stipulated by laws and administrative regulations does not expire, or the deletion of personal data is technically impossible or difficult to achieve, the data controller shall stop the processing of such data other than storing and taking necessary security protection measures. In the cloud environment, the cloud service providers need to facilitate and provide practical measures to delete such personal data.

4. Vendor Management

4.1 Due Diligence

Conducting thorough due diligence is crucial to ensuring compliance with Chinese laws and regulations, particularly those related to data security, cybersecurity, and personal information protection. The following is a short, high-level checklist for basic due diligence based on applicable Chinese legal requirements:

- Check the cloud service provider's compliance with relevant laws, including the CSL, DSL, and the PIPL. According to the CSL, its implementation regulations, and law enforcement practice, cloud service providers providing services through the cloud hosted in China should obtain the proper level of MLPS certification. Depending on the nature of the business and the volume of personal data that is to be processed in the cloud, the cloud service provider needs to obtain level 2, 3 or 4 MLPS certification.
- Check whether the cloud service provider has sufficient and state-of-the-art security measures, including, for example, data encryption, access controls, and incident response protocols.
- Check the cloud service provider's reputation and history concerning data breaches and security incidents. This involves reviewing the provider's standing in the market, customer feedback, industry recognition, and any past legal or compliance issues that could affect their reliability.

4.2 Data Protection in Cloud Service Agreements

A cloud service agreement is critical to ensure data protection in the cloud environment. The cloud service agreement may include the following data protection requirements. Details regarding data processing can be found in **4.3 Data Processing Agreements and the Cloud**.

- Customers' control over data: The agreement shall specify that, without the customers' authorisation, any access, modification, disclosure, use, transfer, or destruction of data should not be permitted. Upon termination of the service contract, all data should be returned to the customer, and data should be completely deleted per the customers' instructions.
- Cloud service providers' measures to protect data: Effective management and technical measures should be taken to ensure the confidentiality, integrity, and availability of customer data and business systems. It is recommended to list specific security measures in the cloud service agreement.
- The SLA should comprise specific technical and management parameters of the security of cloud services. The SLA is recommended to be prepared based on the nature of the customer's business and data and the obligation of the cloud customer to protect their data in the cloud.

- Periodic supervision and audit are effective measures to make sure the cloud service providers comply with the applicable laws. Details can be found in **7. Compliance and Audits**.

4.3 Data Processing Agreements and the Cloud

Article 21 of the PIPL provides the necessary coverage of a data processing agreement (DPA), which should include: the purpose, time limit and method of processing personal data, type of personal data and protection measures, as well as the rights and obligations of both parties, and mechanisms for supervising the data processor's personal data processing activities.

According to the above law, national standards, and mainstream market practice in the PRC, a well-structured DPA should define the responsibilities of both parties. Here is an overview of how DPAs are typically structured in a cloud business in the PRC:

- Scope of data processing: The DPA may provide details about, if applicable, (i) what kind of data will be processed, the purpose of the processing, and the types of processing; (ii) the period during which the data will be processed, typically tied to the duration of the service contract or until the data is securely deleted or returned; and (iii) types of data and data subjects, including descriptions of the categories of personal data and the categories of data subjects.
- Obligations of the data processor (ie, the cloud service provider): This section may include, for example, (i) a requirement that the processor comply with applicable data protection laws and regulations; (ii) the technical and organisational measures the processor must implement to protect the data's confidentiality, integrity, and availability; (iii) data access and confidentiality; and (iv) a data breach notification provision.
- Obligations of the data controller (cloud customer): This section may include customers' obligations to provide clear and lawful instructions to data processors.
- Data subject rights: The controller must manage data subject rights, such as access, rectification, deletion, and portability requests, and may require the processor's timely assistance in fulfilling these rights.
- Sub-processing: The DPA should provide the conditions under which the processor can engage sub-processors.
- Liability and indemnification: The DPA often includes indemnification clauses specifying how each party will handle potential claims arising from data processing.

4.4 Exit Strategies and Data Migration

The recommended national standard GB/T 31167-2023 Information security technology – Security guidance for cloud computing services in its Article 9 provides guidance on how to determine proper exist strategies and data migration in practice, including:

- Negotiate on exit conditions in advance: Before signing contracts or any written documents such as service commitments from cloud service providers, it is advisable for the cloud service providers and the cloud customers to negotiate in advance on the conditions for exit, as well as the responsibilities and obligations of both parties upon exit.
- Negotiation on migration interfaces and plans: The customer and the cloud service provider should negotiate the interfaces and plans for migrating data and business systems out of the cloud platform, which can

ensure a smooth transition and minimise disruption during the exit process.
- Return of migratable data: During the exit process, the cloud service provider should return the customer data specified as migratable in the contract or service commitment documents.
- Ensuring business availability and continuity: While migrating data and business systems back to the customers' own data centre or another cloud platform, the customer and service provider should ensure business availability and continuity. Effective measures may include parallel operation of the original business system and the newly deployed system for a certain period.
- Revocation of access: The cloud service provider should promptly cancel physical and electronic access to the customer's resources once the service has been exited.
- Provider's ongoing responsibilities post-exit: Even after the customer exits the cloud service, the provider should still uphold certain responsibilities and obligations, such as confidentiality requirements.

5. Data Breach Notification

5.1 Requirements to Report Data Breaches

The CSL, DSL, and PIPL stipulate the reporting obligations in the event of data breaches. In addition to these general legal requirements, the CAC, China's data protection regulator, further refines specific reporting requirements through its regulatory rules. There are two sets of different requirements regarding personal data breaches and cybersecurity incidents, which are detailed below.

Personal Data Breaches

In the event of personal data breaches, the PIPL requires the personal data controller to notify the competent authorities in a timely manner. This enables the authorities to understand the situation at the outset and take accurate and effective regulatory measures. The specific matters to be reported are detailed in **5.3 Notifying Data Breaches**.

According to Article 66 of the PIPL, personal data controllers failing to fulfil reporting obligations will be subject to administrative penalties. The penalties start with orders to rectify, warnings, confiscation of illegal gains, and orders to suspend or terminate relevant application services; refusal to correct will result in fines of up to RMB1 million. For more severe violations, higher fines may be imposed, along with suspension of business operations or revocation of relevant business licenses or permits.

Cybersecurity Incidents

In the event of cybersecurity incidents, in a proposed draft, the CAC detailed the reporting procedures and contents in Administrative Measures for the Reporting of Cybersecurity Incidents (Draft for Comments) (the "Draft"):

- reporting entities: network operators that construct or operate networks or provide services through networks within the PRC – ie, the cloud service provider, or the customer of the cloud service, depending on the victim of the incidents;
- reporting recipients: CAC, industry competent authorities (if any), and the police (where a crime is suspected);
- reporting contents: organisational details of the reporting entity, incident discovery and impact assessment, incident development, preliminary cause analysis, investigation and

analysis requirements, response and plans, site protection status, and additional information; and
- reporting timeline: based on the classification of security incidents into four classes (general, relatively severe, severe, and extremely severe), the Draft requires that relatively severe, severe, or extremely severe cybersecurity incidents must be reported within one hour; if certain details are not available within one hour, reporting must occur within 24 hours.

The Draft stipulates that network operators failing to report cybersecurity incidents as required may face legal liabilities under CSL, DSL, and PIPL, which could include orders to rectify, warnings, and fines. If competent authorities consider the circumstances severe, heavy fines or even business suspension/termination may be imposed. However, the Draft also provides that if a company has taken reasonable and necessary protective measures to minimise the harm of data breaches and proactively reported as required, liability may be exempted or mitigated accordingly. Otherwise, the personal data subjects must be notified.

While the exact timeframe for the Draft's finalisation and implementation remains uncertain, its content and regulatory approach signal the government's preferred handling of data breach response and reporting for network operators (including cloud service providers and customers) based or operating in the PRC.

5.2 Investigating and Remedying Data Breaches

The CSL requires network operators to formulate emergency response plans for cybersecurity incidents. When the incident happens, network operators must immediately activate the emergency response plans, take remedial measures, and report to the competent authorities.

Therefore, for cloud service providers and customers, developing an emergency response plan is crucial for investigations and remediation upon a data breach that occurred in the cloud. More information regarding data breaches can be found in **2.1 Data Security and the Cloud** and **4.1 Due Diligence**.

5.3 Notifying Data Breaches

Notification Obligations Under the PIPL

Article 57 of the PIPL sets out a general notification mechanism of notification, which includes the two aspects detailed below.

Notifying personal data subjects and regulatory authorities

As a default rule under the PIPL, the personal data controller has the obligation to notify affected subjects and authorities. Notification to the authorities is mandatory, whereas notification to the personal data subjects is not.

Article 57 provides that if the personal data controllers take measures that can effectively prevent harm from the breach, they can be exempt from notifying the affected personal data subjects, unless specifically required by the authorities. The PIPL does not explicitly define a clear threshold for when notification becomes necessary. Nor does it outline specific timelines for such notifications.

Information to be notified

The notification should include information such as: (i) the categories of personal data that have been or may be leaked, altered, or lost, the causes for such incidents, and the potential harm they may cause; (ii) the remedial measures taken by the personal data controllers and the

mitigation measures that personal data subjects may take; and (iii) the contact information of the personal data controller.

Key Considerations

It is important to note that the above is only a high-level legal requirement provided by the PIPL. In practice, regulators may request more extensive information based on their working rules and specific cases. Cloud service customers may want to consider the following in handling data breach notification matters:

- Clarifying the definition of a personal data breach, roles of both parties, notification recipients, notification timelines and methods, remedial measures, etc, in the cloud service agreement.
- Designating emergency contacts for each party and establishing effective communication channels.
- Reviewing the cloud service provider's emergency response plan or SLA to ensure a swift response can be carried out in the event of a data breach.
- Clarifying the liability and indemnification of the defaulting party in the absence of proper notification.

6. International Data Transfers

6.1 Cross-Border Transfer Regulation

Please refer to details in **1.2 Data Privacy and Cloud Computing**.

6.2 Data Localisation

PRC law does not have a generally applicable and absolute data localisation requirement. However, the CSL, DSL, and PIPL impose localisation requirements on certain specific types of data and outline the administrative requirements for cross-border transfers of such data.

- Data localisation for CIIO: CIIOs are required to store the personal data they collect and process within China. Any cross-border transfer of data by operators of CIIs is subject to prior approval from the competent government authorities. CIIs are identified in strategically important sectors such as national defence, energy, and finance. Government authorities overseeing these industries will notify CIIOs individually about their designation as CIIs and the corresponding data localisation requirements.
- Data localisation for specific types of data: Certain specific types of data that are crucial to state security and the public interest are subject to data localisation requirements. Examples include geographic and mapping information, health and medical information (such as patient records), and other sensitive categories. The localisation requirements for such types of data can be found in the industrial regulations that are publicly available.
- Data localisation for "Important Data": Important Data is a specially defined type of data under Chinese law that is highly sensitive from the perspective of national security and the general welfare of the public. Important Data must be stored in China unless prior approval is obtained. While Important Data is intended to be identified by relevant industrial regulators, the process for formally designating data as "Important" has been slower than anticipated.
- No data localisation for personal data: For general personal data (not falling within the scope of specific types of data and Important Data as outlined above), there is no data localisation requirement.

Data localisation requirements have a direct effect on the compliance of cloud computing services. The slow and ambiguous identification of Important Data raises concerns regarding data transfers in and out of the PRC. Cloud service providers and users need to have a data compliance strategy in place that allows them to address the concern of data localisation requirements in the PRC.

6.3 Conflicts of Law

Among cross-border data transfers, it is not uncommon for legal systems or judicial procedures of different jurisdictions to clash. For instance, in cross-border litigation, a US governmental agency may require a company in China to present data information in its routine regulatory check or special investigation. However, under the DSL and PIPL, submitting personal information or data stored in China to foreign law enforcement authorities is subject to prior approval from the competent Chinese regulatory authority. The approval process in China may be complex and time-consuming, making it difficult to meet the demands of the foreign law enforcement authority in a timely fashion. The conflicts of laws between different jurisdictions may therefore increase compliance costs and legal risks for multinational companies.

Addressing such an issue requires clearly understanding the nature and type of the data request from the foreign authority, and the scope and procedure of the PRC data cross-border approval. Although potentially complex and time-consuming, successful resolution involves collaboration between PRC counsel well-versed in Chinese law and foreign counsel familiar with the requesting country's law enforcement procedures.

7. Compliance and Audits

7.1 Cloud Computing and Compliance/ Audits

In China, the personal data processing compliance audit was introduced in the PIPL in 2021, and regulatory requirements related to it have been gradually taking shape since then. In 2023, the CAC released the draft Administrative Measures for Compliance Audit of Personal Information Protection (the "Audit Measures") for public comment, but to date it has not come into effect. The Audit Measures draft applies to personal data processing activities conducted by personal data controllers in all scenarios, including cloud-based processing.

In July 2024, the national recommended standard Data Security Technology- Personal Information Protection Compliance Audit Requirements (the "Standard") was introduced for public comment, which provides more comprehensive and practical guidance based on the Audit Measures.

Cloud service providers and cloud service customers should comply with the above in their personal data processing once they become final and effective. The following is a summary of the key aspects of personal information protection compliance audits in the Audit Measures and the Standard.

Occurrence of Compliance Audit

As an independent supervisory mechanism to confirm and ascertain a personal data controller is processing personal data in accordance with the law, a compliance audit is mandatory. Companies that process personal data are required to conduct audits on a regular basis (every one or two years, as the case may be). Audits can be performed internally by the company itself or by engaging third-party professional agencies.

Additionally, if the regulatory authorities find that there is a significant risk in the processing of personal data or if a personal data breach occurs, the authorities may require the personal data controller to engage a third-party agency for a compliance audit. This is a type of audit process triggered by regulators.

A compliance audit generally involves several processes, including audit preparation, audit implementation, audit reporting, issue rectification, and archive management.

Key Areas of Compliance Audit

The scope of a compliance audit can be very broad, covering almost all aspects of personal data processing activities and the obligations provided by the PIPL. Key areas include, but are not limited to the following:

- the legal basis for personal data processing;
- transparency and completeness of privacy policies;
- fulfilment of notification requirements;
- the whole life cycle management of personal data processing;
- methods for personal data subjects to exercise their legal rights; and
- organisational structure, managerial and technical measures, and data protection policies.

Independence, Fairness, and Comprehensiveness of Compliance Audit

The Standard provides an essential guide to understanding and complying with the principles of independence, fairness and comprehensiveness of a compliance audit, covering aspects such as the audit process, implementation management, evidence management, qualifications of auditors, etc.

In terms of evidence management, the Standard requires that the audited party must ensure the authenticity, completeness, and validity of the evidence provided. Only evidence that meets both formal and substantive requirements can be accepted and used in the audit report.

Implementation of Compliance Audit Findings and Recommendations

The Standard highlights that once the audit report is completed and delivered, the audited party should address the identified issues within a specified timeframe. Auditors have the right to confirm the status of rectification.

Penalties for Non-compliance

Personal data controllers who fail to conduct compliance audits as required or improperly perform such audits will be subject to administrative penalties under Article 66 of the PIPL. In cases where the violation is even more severe and constitutes a crime, criminal liability may also be imposed.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com