Cloud Computing 2024

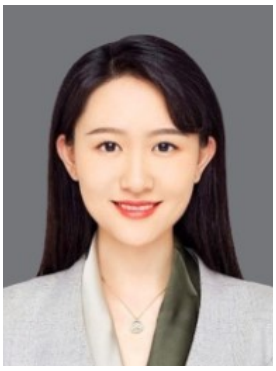
Last Updated October 08, 2024

China

Trends and Developments

Authors


Zhichao Duan


Ziqian Zhang


Hui Yuan

Han Kun Law Offices is a leading full-service law firm in China, widely recognised for providing tailored legal services and effective solutions to clients. Han Kun has professionals in eight offices in Beijing, Shanghai, Shenzhen, Haikou, Wuhan, Hong Kong, Singapore and New York. Most of Han Kun's practices have been consistently recognised as top Chinese law firm practices by authoritative international legal ranking organisations. The firm is also a trend-setter in the data field. The data protection team comprises more than a dozen lawyers – all of whom graduated from top Chinese or foreign universities. With a deep understanding of data laws both in China and abroad, the team represents some of the most prominent corporate names across the globe in solving their complex data compliance matters. By advising clients on cutting-edge matters, the data protecion team integrates expertise from within the firm and beyond to provide creative solutions that meet clients' needs.

Regulations on Cloud Computing in China

For more than a decade, the Chinese government has adopted various measures to promote the advancement of cloud computing in China. In 2010, the Ministry of Industry and Information Technology (MIIT) and the National Development and Reform Commission (NDRC) jointly issued an announcement to launch pilot projects in Beijing, Shanghai, Shenzhen, Hangzhou, and Wuxi. This initiative encouraged the relevant organisations to develop software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), as well as build cloud computing centres, bolster the research of core technologies, establish a nationwide industry alliance, and draft corresponding standards and regulations.

In 2013, the MIIT, the NDRC, and some other departments jointly issued Guiding Opinions on the Construction and Arrangement of Data Centres, providing political and financial incentives for the establishment of new data centres. In 2015, the MIIT included cloud computing in the 2015 Telecoms Catalogue and issued the first version of the Guidelines on the Construction of a Comprehensive Standardisation System for Cloud Computing. In the same year, the Fifth Plenary of the 18th Communist Party of China (CPC)'s Central Committee passed the 13th Five-Year Plan for Economic and Social Development, which listed cloud computing as a key field for the coming five years. These policies illustrate the Chinese central government's decade-long dedication to the development of cloud computing.

Following in the footsteps of the central government, many local governments issued policies to stimulate the growth of cloud computing. By way of example, in 2014, Guangdong Province announced its plan to turn the province into a national hub for cloud computing technology, a leading area for cloud computing application services, and a global manufacturing base for cloud infrastructure equipment and cloud terminals by 2020. In 2017, Shanghai proposed to increase its investment in cloud computing so that by 2020 the revenue from cloud computing technology and services will reach CNY150 billion and the revenue from cloud computing, big data, mobile internet, and other related industries will reach CNY500 billion.

China has recognised the importance of cloud computing to its global competitiveness and boosted the industry through diverse policies since 2010. Government policies will likely remain supportive, given that the 14th Five-Year Plan for National Informatisation – published in 2021 – continued to emphasise the significance of cloud computing as China seeks to accelerate digitised development.

Cloud computing: requirements and potential risks for cybersecurity, data security, and personal information protection

The upstream of cloud computing usually encompasses cloud infrastructure providers who supply servers, networking hardware (eg, routers and switches), storage devices, network security devices, and optical fibre. The midstream includes data centres and cloud service providers. The downstream consists of customers in various industries such as finance, manufacturing, and education. Providing or using cloud computing services usually relies on co-operation among multiple parties and may therefore lead to different data processing roles, data security compliance obligations and responsibilities.

Under the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), the cloud service users or the customers of cloud service providers (together referred to as "customers") usually serve as data handlers or personal information handlers ("handlers" – ie, the party who determines the purpose, method and scope of data/personal information processing, similar to the concept of controller under the EU's General Data Protection Regulation (GDPR)). Cloud service providers may generally be regarded as entrusted parties (ie, the party who processes data/personal information under the instruction of handlers, similar to the concept of processor under the GDPR).

Therefore, the customer is mainly responsible and accountable for fulfilling the compliance and security obligations required by relevant laws, and the cloud service provider must assist the handler in fulfilling its obligations and take measures to ensure the security of data. Although in most of the enforcement cases penalties are imposed on handlers, there are also cases where the entrusted party or cloud service providers were directly penalised for failing to take adequate security measures. Thus, cloud service providers still need to focus on their data security protection obligations.

In addition, under the Cybersecurity Law (CSL), both customers and cloud service providers may constitute the network operator and must comply with the obligations set forth in the CSL.

Special protection requirements for critical information infrastructure operations

The Security Protection Regulations for Critical Information Infrastructure (the "Regulations on CII") defines critical information infrastructure (CII) as key network facilities and information systems in important industries and fields (such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government, and science and technology for national defence) that may seriously endanger national security, national economy, people's livelihood, and public welfare once they are subject to any destruction, loss of function, or data leakage. Accordingly, CII is subject to special regulation under Chinese law.

Against the backdrop of digital transformation, many CII operators (CIIOs) are migrating their applications and data to the cloud and many new CIIOs opt to adopt a cloud-native approach, giving rise to new risks in network and data

security. In response to this trend, the Guiding Opinions on Implementing the Classified Protection System and the Security Protection System for Critical Information Infrastructure – promulgated in 2020 – stipulate that cloud platforms that meet the relevant identification criteria also fall under the scope of CII. Therefore, cloud service providers identified by the competent authorities as CIIOs should make sure they comply with the relevant requirements.

The CSL and the Regulations on CII constitute the pillars of CII regulation, laying out provisions on the identification of CII and the obligations of CIIOs. In addition, certain national standards (such as GB/T 39204-2022 Information Security Technology – Cybersecurity Requirements for Critical Information Infrastructure Protection) clarify the specific protection measures that CIIOs can adopt to ensure the security of CII.

A cloud service provider that is not identified as a CIIO may nonetheless be subject to CII regulation if it provides services to a CIIO customer. By way of example, Article 16 of Regulation on Network Data Security Management requires network data handlers that provide services for CIIOs to fulfil their obligations of network data security protection and provide secure, stable and continuous services in accordance with laws, regulations and contractual stipulations. Under the same article, without the consent of the contracting party, the network data handler may not access, obtain, retain, use, divulge or provide others with network data, nor may it conduct association analysis of network data.

Security technology risks

All liable parties should abide by the relevant security requirements, including but not limited to:

- Information Security Technology – Security Capability Requirements for Cloud Computing Services (GB/T 31168-2023);
- Information Security Technology – Security Reference Architecture of Cloud Computing (GB/T 35279-2017);
- Information Security Technology – Security Guidance for Cloud Computing Services (GB/T 31167-2023); and
- Information Security Technology – The Assessment Method for Security Capability of Cloud Computing Service (GB/T 34942-2017).

i) Logs

Data handlers are required by law to retain record logs on data processing, authority management, and personnel operations in the processing of the full life cycle of data for no less than six months. It is important to note that specific requirements for logs are scattered across various laws and regulations and that the form and content of the logs to be retained depend on the nature of the service provided.

ii) Cybersecurity Classified Protection System

China implements the Cybersecurity Classified Protection System (CCPS), which requires network operators and CIIOs to classify their information systems or networks into five levels based on their potential impact on individuals' rights and national security. Specifically, network operators must refer to Article 21 of the CSL to fulfil their obligations of security protection according to the requirements of the CCPS.

The competent authorities actively enforce the CCPS. By way of example, in 2017, the police force in Anhui Province investigated a school whose website was hacked. The police determined that the school had not performed its obligations as a network operator and fined the school CNY15,000 and the liable person CNY5,000. To avoid warnings and fines, relevant businesses and organisations should regularly test their security management systems and evaluate their compliance with the CCPS.

iii) Procuring qualified cybersecurity products

Certain cybersecurity products (such as firewalls and intrusion detection systems) are classified as Critical Network Equipment (CNE) and Specialised Cybersecurity Products (SCPs) in the Catalogue of Critical Network Equipment and Specialised Cybersecurity Products. Pursuant to Article 23 of the CSL, CNE and SCPs should not be sold or supplied until such equipment or product successfully obtains security certification or passes security tests conducted by a qualified organisation. Therefore, cloud service providers should procure qualified CNEs and SCPs to ensure the security of their systems and data, as well as the security of supply chains.

iv) Obligations upon security incidents

Several Chinese laws and regulations set forth the obligation of reporting to the competent authorities and notifying personal information subjects upon discovering security incidents (ie, incidents or risks of cybersecurity attacks or data breaches), including Article 59 of the CSL, Article 29 of the DSL, Article 57 of the PIPL, and the Regulations on the Reporting of Cybersecurity Incidents (Draft for Comments) (the "Incident Draft"). The Incident Draft provides that if a security incident involves more than one million people, the operator should report it to the authorities within one hour. In addition, there has been a precedent enforcement case where a major cloud service provider was penalised for not reporting security incident to the authority.

Personnel risks

To ensure data security, network operators should implement management measures for individuals with access to systems and data, including current or former employees, system administrators, contractors, or business partners.

Network operators should conduct background checks on these individuals, formulate internal security management systems and operating instructions, and maintain personnel records, as well as conduct monitoring and audits.

Data localisation and cross-border data transfer

Under Chinese law, certain types of data should be stored in China. When cross-border data transfer is indeed necessary, these types of data can only be transferred overseas after receiving approval from the competent authorities. By way of example, the Measures on Real Name Collection and Delivery of Postal and Courier Items set forth that user information and important data collected and generated by delivery enterprises when collecting users' real names and delivering postal and courier items in China should be stored in China. The Measures for the Administration of Population Health Information (for Trial Implementation) provide that population health information must be stored in China and may not be hosted or leased on servers outside China.

Furthermore, China implements a data export regulation system for important data and personal information through such regulations as:

- the Provisions on Promoting and Regulating Cross-Border Data Flows;
- the Measures (Negative List) for Outbound Data Transfer from China (Beijing) Pilot Free Trade Zone (for Trial Implementation); and
- the Administrative List (Negative List) for Outbound Data Transfer from China (Beijing) Pilot Free Trade Zone (Edition 2024).

Under these regulations, if the data to be transferred overseas falls under certain categories, data handlers must pass data export security assessments, file standard contracts, or obtain personal information protection certifications.

In a cloud computing scenario, as outlined earlier, the customer is usually identified as the personal information handler and is thus responsible for fulfilling the aforementioned obligations of data localisation and export compliance. Nevertheless, cloud service providers should also assist their customers in performing the relevant compliance obligations through contractual agreements.

Qualifications for providing cloud services

Pursuant to the Provisions for Foreign-Funded Telecommunications Enterprises, the proportion of foreign investment in enterprises operating value-added telecommunications services should not exceed 50%, unless otherwise provided by laws or regulations. In addition, the Measures (Negative List) for Foreign Investment provide that foreign investment in value-added telecommunications is limited to telecommunications services that China agreed to open to foreign investors in its accession to the WTO, which does not include services such as B11. Therefore, in principle, companies applying for licences such as B11 should not have any foreign investment.

Under such regulations, foreign enterprises usually conduct telecommunications businesses in the following three ways.

- CEPA model – the government of the Chinese mainland has signed the Closer Economic Partnership Arrangement (CEPA) and a series of supplementary agreements with the governments of Hong Kong SAR and Macau SAR to strengthen trade and investment co-operation, including preferential policies for investment in value-added telecommunications services. By way of example, with regard to B11, CEPA raises the limitations on the proportion of foreign investment to 50%. Therefore, foreign enterprises may invest in entities in the Chinese mainland through their service providers in Hong Kong SAR and Macau SAR for favourable VAT treatment.
- Variable interest entity (VIE) model – foreign entities may establish a wholly foreign-owned enterprise (WFOE) in the Chinese mainland. The WFOE may control a domestic operator (ie, the entity that obtains a value-added telecommunications licence and conducts business) through a series of agreements. However, such VIE models may be subject to regulatory concerns in practice.
- Co-operating with licensed value-added telecommunications providers on the Chinese mainland – foreign entities may sign co-operation agreements with cloud service providers holding value-added telecommunications licences in the Chinese mainland ("domestic entities") to provide IP licences and technical support. The domestic entity would sign service contracts with customers to provide cloud services with the same technical standards as the foreign entity. In addition, data collected would mainly be stored in local data centres operated by the domestic entity and remain isolated from data centres of the foreign entity. At present, some prominent cloud service providers adopt this approach to provide cloud services in the Chinese mainland.

Meanwhile, China is gradually easing the above-mentioned limits and has adopted a broader opening-up initiative on foreign investment in value-added telecommunications. In April 2024, the Notice of the Pilot Programme for Expanding the Openness of Value-Added Telecommunications Businesses to Foreign Investment proposes to carry out a pilot programme in certain regions of Beijing, Shanghai, Hainan and Shenzhen.

In the pilot programme, restrictions on the foreign equity ratios for some value-added telecommunications services including internet data centres, content delivery networks, internet service providers, online data processing and transaction processing, information-releasing platforms and delivery services contained in information services (excluding the operation of internet news information, online publishing, online audio and video, and internet culture) – as well as information protection and processing services – will be removed. On 23

October 2024, the MIIT organised a seminar on the pilot programme for expanding the opening-up of value-added telecommunications services and formally launched the pilot programme in the four pilot regions.

Special regulation for financial sector

Certain industries face special requirements for the use of cloud services given their high sensitivity. This section will briefly introduce the relevant regulations using the financial sector as an example.

Related policies

A series of policies indicate that authorities in the financial sector support the use of cloud computing, as follows.

- The 13th Five-Year Plan for the Development of Information Technology in China's Financial Industry, released in 2017, proposes to steadily promote research on the application of system architecture and cloud computing technology and to strengthen policy research and guidance on the application of cloud computing in the financial sector.
- The Financial Technology (Fintech) Development Plan (2019–21) – published in 2019 – further proposes to co-ordinate the planning of cloud computing applications in the financial sector, with the goal of building a safe and controllable cloud service platform for the financial sector.
- The Financial Technology Development Plan (2022–25) – released in 2021 – proposes to accelerate the application of cloud computing technology, providing financial services with efficient management of cross-region data centre resources, elastic provisioning, cloud-network linkage, and multi-location multi-activity deployment capabilities.

Financial cloud standards

In the meantime, the financial sector has introduced financial standards on cloud computing technology and applications ("financial cloud standards") to ensure network and data security, including but not limited to:

- JR/T 0166-2020 Financial Application Specification of Cloud Computing Technology – Technical Architectures (the "Architecture Standard");
- JR/T 0167-2020 Financial Application Specification of Cloud Computing Technology – Security Technical Requirements (the "Security Standard"); and
- JR/T 0168-2020 Financial Application Specification of Cloud Computing Technology – Disaster Recovery (the "Recovery Standard").

The financial cloud standards apply to both financial institutions (ie, financial cloud service users) and financial cloud service providers, setting forth special requirements for financial clouds. By way of example, Article 5.2 of the Architecture Standard provides that cloud computing deployment models in the financial sector mainly include private clouds, group clouds, and hybrid clouds composed of the previous two kinds of cloud. Article 6.1 of the Security Standard

further provides that the operating environment of cloud computing data centres used to serve the financial sector should be physically isolated from other industries. Therefore, financial clouds should not be operated as public cloud models or on public clouds.

In addition to standards specifically regulating financial clouds, requirements for financial clouds may also be addressed in other financial sector standards on personal information and data. By way of example, Article 6.1.6 of JR/T 0171-2020 Personal Financial Information Protection Technical Specification stipulates that the erasure of personal financial information in cloud environments should be performed in accordance with the standard JR/T 0167-2018.

Han Kun Law Offices

9/F
Office Tower C1
Oriental Plaza
1 East Chang An Avenue
Dongcheng District
Beijing 100738
China

+86 10 8525 5500

+86 10 8525 5511/5522

beijing@hankunlaw.com
(mailto:beijing@hankunlaw.com)
www.hankunlaw.com/en/
(http://www.hankunlaw.com/en/)