CHINA FINALLY HAS ITS STATE COUNCIL LEVEL LEGISLATION FOR DATA SECURITY

OVERVIEW

On 30 September 2024, the State Council of the People's Republic of China promulgated the *Administrative Regulations on Cyber Data Security (2024)* (the "**CDS Regulations**"), which will take effect from 1 January 2025. The CDS Regulations supplement the three pillars of China's existing data security protection regime, namely the *PRC Cybersecurity Law (2017)* (the "**CSL**"), the *PRC Personal Information Protection Law (2021)* (the "**PIPL**") and the *PRC Data Security Law (2021)* (the "**DSL**", together with the CSL and the PIPL collectively the "**China Data Laws**").

This briefing provides an in-depth analysis of the key new requirements introduced by the CDS Regulations and their relevant impact.

KEY TAKEAWAYS

- The CDS Regulations supplement China's existing data security framework and fill the gap in the legislative hierarchy
- Detailed guidance on cyber incident response is provided, mandating timely reporting of security deficiencies and notifying affected parties of incidents impacting their rights and interests
- The CDS Regulations require the use of "dual lists" by all Processors to protect data subjects' rights
- Important data protection measures are further clarified and developed by the CDS Regulations

GENERAL COMPLIANCE FOR NETWORK DATA PROCESSORS

The China Data Laws already outline data security protection obligations for processors of network data ("Processors")[1], and the CDS Regulations introduce new requirements for Processors, which mainly include the following:

- The DSL provides, in general, that the State should establish a data security review mechanism and may carry out national security review.

  However, the CDS Regulations imposes an obligation on Processors to carry out the national security review when carrying out data processing activities that have affected, or may affect, national security.

- The PIPL requires Processors to agree with recipients on the purpose, term, method, and scope of processing, as well as rights and obligations of both parties when entrusting the processing of personal information ("PI") to others.

[1] Similar to the definition under the PIPL and DSL, Processors are defined under the CDS Regulations as individuals or organisations conducting network data processing activities, including the collection, storage, use, processing, transmission, provision, disclosure, and deletion of data on network, and autonomously deciding the purpose and method of processing.

The CDS Regulations extend this requirement to both the (a) provision and (b) entrustment of the processing of (x) PI and (y) important data, with records to be kept for at least three (3) years.

- Under the PIPL, non-PRC Processors processing PI of individuals within China, who are required to establish a dedicated entity or designate a representative within China[2], must report their name and contact information to the relevant government agency.

  The CDS Regulations clarify that the reporting should be made to the municipal-level cyberspace administration.

- The CDS Regulations also regulate the use of automated tools (commonly known as "web crawlers") for data collection. Prior to the adoption of the CDS Regulations, usage of web crawlers was primarily governed by the PRC Anti-Unfair Competition Law, whose application, however, requires a "competitive relationship" between the parties. In this regard, the CDS Regulations impose a general obligation on Processors to assess the impact on network services and prohibit illegal network intrusion or interference with the normal operation of others' network services.

  Moreover, PI inadvertently collected through web crawlers must be deleted or anonymised. If the deletion or anonymisation is technically not possible, Processors shall stop processing the PI, except for storage and/or adopting necessary security protection measures.

CYBER INCIDENTS RESPONSE

The CSL sets out the overarching principles for cyber incidents response, including monitoring, warning and handling cyber incidents, and developing contingency plans, which are to be undertaken by the cyberspace administration and other governmental authorities.

However, the CDS Regulations impose new specific actionable requirements on Processors. Processors need to establish contingency plans for network data security incidents, take immediate remedial actions and report any security deficiencies or vulnerabilities with respect to their relevant products or services to their clients and relevant authorities in a timely manner.

If there are national security or public interest implications, the report must be made to the relevant authorities within 24 hours. Although the timing requirement for this reporting duty can be challenging, the scope is limited to cyber incidents affecting "national security or public interest". While the triggers are not crystal clear given the possible interpretations of "national security or public interest", this at least allows Processors processing a relatively small amount of data to determine on when to report a cyber incident.

In addition, the CDS Regulations require Processors to notify affected parties in a timely manner if an incident damages the legitimate rights and interests of individuals or organisations. They must supply details of the incident, risks involved, consequences of the incident, and the remedial measures taken[3]. We note that the term "timely manner" here is not quantified, unlike the 24-hour requirement discussed above, which means that more time may be allowed based on the nature of the incident.

---

2 In accordance with Article 3(2) of the PIPL, this requirement applies to activities carried out to process the PI of persons within China, and such processing is:
(a) for the purpose of providing products or services to individuals in China;
(b) to analyse or assess behaviours of individuals in China; or
(c) otherwise required by relevant laws and administrative regulations.

3 As allowed by the CDS Regulations, such notifications can be made through various means, e.g., phone calls, text messages, instant messaging tools, emails, or public announcements.

PI PROTECTION AND DATA SUBJECTS' RIGHTS

The CDS Regulations build upon the PIPL to provide clearer compliance guidance for market participants regarding data subjects' rights. Key new developments include:

- Dual Lists: Article 17 of the PIPL requires a Processor to disclose relevant matters to data subjects in an authentic, accurate and complete manner [4] . The CDS Regulations further specify that disclosures must be clear, specific and accessible, and be displayed in a conspicuous place in a prominent way. New items to be disclosed as required by the CDS Regulations include:

  (i) where sensitive PI is to be processed, the necessity and impact of processing on data subjects' rights;

  (ii) handling of PI after the expiration of specified period and methods for determining the storage period if uncertain; and

  (iii) specific data subjects' rights (as discussed below).

  More importantly, the CDS Regulations introduce the requirement of "dual lists" for all Processors. This mandates the disclosure of relevant matters in the form of a list before:

  (i) the collection of PI, in which case matters to be disclosed have been explicitly set out under the PIPL and the CDS Regulations as discussed above; and

  (ii) the provision of PI to other Processors, in which case the purpose, method, types of PI to be provided and basic information of the other Processors will need to be disclosed.

- Data Subjects' Rights: Data subjects must be informed of their rights to access, copy, transfer, correct, supplement, delete, restrict processing, delete accounts or withdraw consent in the manner outlined above. Where a data subject requests to exercise his/her rights, Processors must process in a timely manner and provide convenient methods and channels to facilitate the exercise of these rights without any unreasonable condition.

- Rights to Data Portability: The CDS Regulations set out specific requirements for data subjects' right to data portability as generally outlined under Article 45 of the PIPL. A Processor is required to provide a mechanism for another Processor designated by an individual to access and obtain the relevant PI if relevant conditions are met[5].

  If the frequency of PI transmission requests significantly exceeds a reasonable range, Processors may charge necessary fees based on the cost of transmitting PI.

---

4 The relevant matters that shall be disclosed include:
(a) the name and contact information of the Processor;
(b) the purpose and method of processing, the type of PI processed, and the storage period;
(c) the method and procedure for data subjects to exercise relevant rights provided under the PIPL; and
(d) other matters as provided by laws and administrative regulations.

5 The relevant conditions include:
(a) the identity of the individual making the request can be verified;
(b) the PI requested for transmission is provided based on consent or collected based on a contract;
(c) the transmission of PI is technically feasible; and
(d) the transmission of PI does not adversely affect the legitimate rights and interests of others.

- Consent-based Processing of PI: Where the processing of PI is consent-based, in addition to other requirements already outlined under the PIPL, a Processor may not frequently seek consent from data subjects after it has been explicitly refused.

Based on our observation, the Chinese judiciary's approach also aligns with these rules. A recent PRC court judgement[6] emphasised that disclosures related to PI processing must be made in a conspicuous, clear, and understandable manner, ensuring authenticity, accuracy, and completeness, as mandated by Article 17 of the PIPL. The court noted that whether the common practice of displaying privacy notices and obtaining consent through checkboxes is sufficient depends on whether "enhanced" or "separate" consent is required. If so, a generic consent to the privacy policy would not be considered sufficient, and separate and independent disclosure and consent must be obtained.

Market participants are advised to revisit their privacy notices and/or the practice to respond to data subjects' rights requests to ensure compliance with the detailed guidance provided under the CDS Regulations.

SAFEGUARDING SECURITY OF IMPORTANT DATA

The general principle for identifying important data based on a data classification and grading system has been provided under the DSL.

In addition, the CDS Regulations clarify that relevant authorities should (a) notify Processors in a timely manner upon self-identification and filing by Processors or (b) publish determinations regarding whether relevant data qualifies as important data. This is beneficial for Processors who previously might need to make their own judgment on whether any processed data falls into the category of important data.

Moreover, the CDS Regulations provide the following new and/or detailed requirements for the protection of important data.

- Important data Processors must establish a network data security management department and appoint responsible officer(s) to implement relevant security measures and handle security incidents.
- For merger, spin-off, dissolution, or bankruptcy that might negatively impact the security of important data held by the concerned Processor, such Processor shall report important data disposal plans to relevant provincial or central-level regulatory authorities and provide information about the recipients.
- Processors who process PI of more than ten (10) million individuals are considered important data processors and shall perform the above two obligations.
- Before providing, entrusting others to process or jointly processing important data, Processors must conduct a risk assessment, except when performing statutory duties. Processors processing important data must conduct annual risk assessments and submit the risk assessment report to relevant provincial or central-level regulatory authorities. Large network platforms (definition see below) are also subject to such annual assessment requirement.

OTHER ASPECTS

The CDS Regulations have also set out relevant data security protection obligations for network platform service providers. Additional "gatekeeping" obligations are imposed upon large network platform service providers, which

6 This case (file no. (2022) Yue 0192 Min Chu No. 6486) was adjudicated by the Guangzhou Internet Court and recognised as one of the first PRC cases concerning PI protection.

are defined as network platforms with (i) more than 50 million registered users or 10 million monthly active users, and (ii) complex business types, whose data processing activities would significantly impact national security, economic operations, and the livelihood of the people.

In terms of penalties, for relevant rules that overlap under the China Data Laws, violations will be subject to penalties provided under those laws. As for other new rules introduced under the CDS Regulations, penalties will be determined based on the severity of the violation and the monetary fines will follow a progressive structure, with a maximum cap of RMB 10 million for severe cases, rather than being linked to the turnover of violating Processors as stipulated under the PIPL.

CONCLUSION

The promulgation of the CDS Regulations marks a significant enhancement to China's data security regime. These measures complement the existing framework established by the China Data Laws and mark another milestone for the enforcement of the relevant data and privacy laws, as law enforcers will have clearer legal basis. Market players are advised to revisit and update their privacy or other data security related policies, contractual agreements, and operational procedures to meet their applicable obligations set forth in the CDS Regulations.

CONTACTS

Stella Cramer
Partner

T +65 6410 2208
E stella.cramer
@cliffordchance.com

Ling Ho
Partner

T +852 2826 3479
E ling.ho
@cliffordchance.com

Terry Yang
Partner

T +852 2825 8863
E terry.yang
@cliffordchance.com

Brian Harley
Counsel

T +852 2826 2412
E brian.harley
@cliffordchance.com

Clarice Yue
Counsel

T +852 2825 8956
E clarice.yue
@cliffordchance.com

Jane Chen
Senior Associate

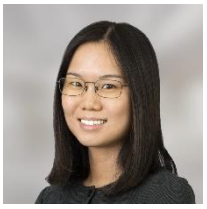
T +86 10 6535 2216
E jane.chen
@cliffordchance.com

Jessy Cheng
Senior Associate

T + 86 10 6535 4935
E jessy.cheng
@cliffordchance.com

Shuai Gao
Associate

T + 86 10 6535 4915
E shuai.gao
@cliffordchance.com



Sharon Zhang
Registered Foreign Lawyer

T +852 2826 3554
E sharon.zhang
@cliffordchance.com

Any content above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers. This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 33/F, China World Office 1, No. 1 Jianguomenwai Dajie, Chaoyang District, Beijing 100004, People's Republic of China

Clifford Chance, 25/F, HKRI Centre Tower 2, HKRI Taikoo Hui, 288 Shi Men Yi Road, Shanghai 200041, People's Republic of China