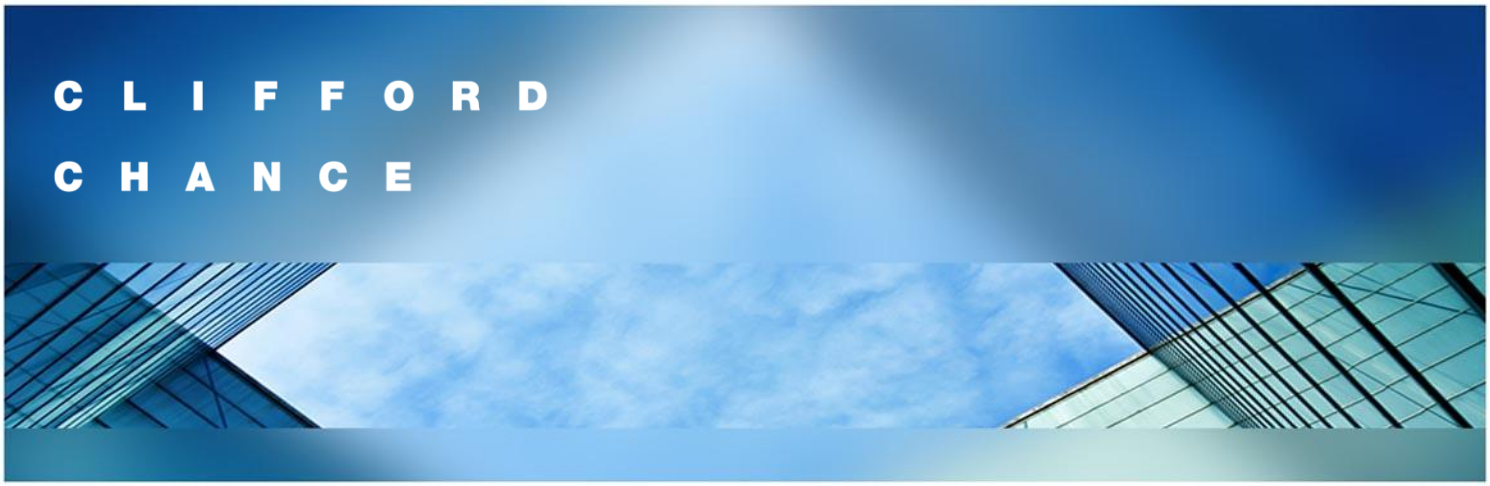

PRC DATA SECURITY LAW – A NEW MILESTONE IN DATA LEGISLATION

The Standing Committee of the National People's Congress passed the PRC[1] Data Security Law (the Data Security Law) on 10 June 2021, which will take effect from 1 September 2021. The Data Security Law is one of the cornerstones for China's legal framework on data and an important pillar for the country's national security regime.

In this briefing, we provide market participants with a more in-depth look at some of the key requirements of the new Data Security Law and their impact.

Key issues

- Companies must determine whether they are processing important data, and, if so, certain requirements under the Data Security Law will be applicable.
- National regulators may carry out national security reviews on data processing activities that have affected, or may affect, national security.
- Data processors are required to enhance risk monitoring, identify system loopholes, and report and take immediate measures to cope with data incidents.
- Prior consent must be obtained before providing information from the PRC to foreign judicial and enforcement authorities.

ENHANCED PROTECTION FOR IMPORTANT DATA

One of the key concepts under the Data Security Law is "*important data*". A company needs to first determine whether it is processing important data, and, if so, the corresponding requirements under the Data Security Law will become applicable, which mainly include:

- appointing a designated person to be responsible for the security of important data;
- conducting a periodic risk assessment on the processing activities of important data, with the assessment report to be submitted to PRC regulators; and
- compliance with rules on export of important data collected and produced within the PRC, which will be separately formulated. If the company is also a critical information infrastructure operator (CIIO), its export of important data will also be subject to rules under the PRC Cybersecurity Law issued in 2016 (the Cybersecurity Law).

What constitutes important data

The Data Security Law delegates power to make decisions on what constitutes important data to local governments and industry regulators. More specifically, in line with the grading system for cybersecurity protection under

[1] PRC or China means the People's Republic of China, which, for the sole purpose herein, does not include Hong Kong, Macau and Taiwan.

the Cybersecurity Law, the Data Security Law states that, at the national level, a data classification and grading system will be established. The central government will coordinate with different authorities to formulate a catalogue of important data with input from local governments and industry regulators.

In short, the Data Security Law lays the foundation for future legislation to define and protect important data. But before the official issuance of the Data Security Law, industry regulators had made several attempts to set the scope of, and the corresponding protective measures for, specific types of important data. In this regard, the automotive industry is a useful example of what industry-specific important data would cover. In May 2021, the Cyberspace Administration of China (CAC) sought public comments on the draft Relevant Provisions on Regulating Security of Automotive Data, under which "important data" in the automotive industry is defined as including:

- data on vehicle and people flows from important and sensitive areas (*e.g.*, military administrative zones, entities implicating state secrets, the Party and governmental organs above the county level);
- surveying and mapping data with a precision higher than those of maps published by the PRC government;
- operational data of automobile charging networks;
- data such as vehicle types and vehicle flow on roads;
- external audio and video data containing faces, voices, licence plates, etc.; and
- other data that may affect national security and public interests as determined by CAC and other authorities.

It is also worth noting that a new concept of "national core data" has been introduced in the final version of the Data Security Law, which is defined as data that may affect national security, national economic lifeline, substantial civil life and public interests. National core data will be subject to a more stringent regulatory regime according to the Data Security Law. Illegal transfer of national core data outside of the PRC will be subject to a fine of up to RMB10 million, and other punishments, such as the shutting down of business and/or the revocation of licences, and may even trigger criminal liabilities in the most severe cases.

DATA SECURITY REVIEW AND DATA INCIDENT REPORT

The Data Security Law addresses the data aspect of the National Security Law, which was last amended in 2015 and was once more focused on foreign investments. The Data Security Law provides, in general, that the State should establish a data security review mechanism and may carry out national security review on data processing activities that have affected, or may affect, national security. The decision from a data security review is final, and no remedy or relief can be sought in the PRC in relation to such decisions. The procedures for data security reviews are not provided in the Data Security Law, which we understand will be formulated by the relevant PRC authorities in due course. The latest development in this regard is the proposed amendment to the Measures for Cybersecurity Review issued in 2020. The draft amendment was issued in July 2021 for public comments, which, among others, proposed to bring data processing activities under the same security

review mechanism mainly applicable to CIIO-related activities at the current stage.

National regulators are clearly determined to tackle data/cyber-security issues as one of the top regulatory priorities. In recent months, there have been several investigations (sometimes conducted jointly by several ministries), resulting in removal of apps from app stores and/or allegations of suspected illegal collection of personal information.

The obligation to ensure data security is also imposed on each data processor. Specifically, according to Article 29 of the Data Security Law, data processors are required to enhance risk monitoring, identify system loopholes, and report and take immediate measures to cope with data incidents. While the implementing rules are still pending, some recent developments, particularly the Administrative Provisions on Security Loopholes of Network Products (the Loopholes Rules) issued in July 2021, may help to provide guidance. For example, under the Loopholes Rules, a network product provider must report loopholes on a platform set up by the PRC Ministry of Industry and Information Technology within two days of discovering the loophole (to find out more about the Loopholes Rules, please see our previous alerter). Data incident reporting requirements may follow the same vein, subject to the issuance of any further rules.

PRIOR CONSENT FOR PROVIDING DATA TO FOREIGN JUDICIAL AUTHORITIES

Article 36 of the Data Security Law provides that, unless with prior consent from competent PRC authorities, no entity or individual within the PRC may provide data stored in the PRC to foreign judicial or enforcement authorities. Violation of Article 36 may lead to a fine of up to RMB5 million, other punishment such as the shutting down of business and/or revocation of licences, as well as penalties to persons in charge.

Similar restrictions are imposed by some recent legislation, for example, the PRC Securities Law (2019 Amendment) (the Securities Law), which prohibits the export of information relating to securities business activities without prior approval; the PRC Futures Law (Consultation Draft) also has the same provision for futures business activities as in the Securities Law.

It remains to be seen how Article 36 will operate in practice. For example, market participants will need further clarity on the definition of "judicial and enforcement authorities". Will tax, competition and financial regulators, in the context of regulatory filings to get clearance, registration and/or approval, be categorised as enforcement authorities? Also, with respect to data that has already been transferred outside the PRC for other reasons, will Article 36 still apply if foreign law enforcement bodies request access to such data later? There is no clear answer and each entity concerned must design their own data strategy depending on, among others, the industry it is engaged in, the data concerned and its long-term plan in the PRC.

A DATA REGIME THAT REFLECTS PRC POLICY PRIORITIES

The approach reflected to the Data Security Law can be contrasted with the influential European data protection regime embodied in the GDPR and emerging US privacy legislation, such as the Californian Consumer Privacy Act. Whereas, the GDPR and other similar laws focus on striking a balance between the protection of privacy in personal information and the free flow of data and other business interests, China's data security regime places greater emphasis on national security and public interest concerns.

These differences in underlying drivers can have a significant impact on the formulation of the laws, their interpretation and enforcement. For example, with respect to data export, under the GDPR, transfer of data outside the European Economic Area is only permissible if (i) a decision is made by the European Commission recognising the protection of personal information by the recipient's country is adequate, (ii) appropriate safeguards are adopted, or (iii) under a statutory exception. At present, for personal data generally, the Data Security Law does not set such restrictive requirements for data export, although the pending Personal Information Protection Law (the PI Protection Law) will introduce a substantially similar regime. However, if the data concerned constitutes important data or raises national security concerns in the PRC, the applicable rules are stricter than the GDPR, including separate security review and possible data localisation requirements, consistent with PRC policy priorities around national security and cyber sovereignty.

CONCLUSION

Shortly after the promulgation of the Data Security Law, the draft PI Protection Law was sent for the final reading by the legislative body of the PRC. It is clear that the legislative process is being accelerated. With the finalisation of the fundamental laws (the Data Security Law, the Cybersecurity Law and the PI Protection Law), implementing rules and industry guidance are expected to be issued in short order. Companies must prepare to comply with an increasing level of enforcement by, where necessary, adjusting regional and potentially global business models and IT systems, aligning data compliance programmes and risk management systems across jurisdictions, negotiating / renegotiating data terms and reskilling staff to minimise export of data unless necessary and equip the relevant China business with regulatory expertise.

CLIFFORD
CHANCE

CONTACTS

Terry Yang
Partner

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

Lei Shi
Partner

T +86 21 2320 7377
E lei.shi
@cliffordchance.com

Brian Harley
Consultant

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

Kimi Liu
Counsel

T +86 10 6535 2263
E kimi.liu
@cliffordchance.com

Yan Li
Senior Associate

T +86 10 6535 2284
E yan.chen
@cliffordchance.com

Jane Chen
Associate

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

Jessy Cheng
Associate

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

Roy Wang
Trainee

T +86 21 2320 7326
E roy.wang
@cliffordchance.com

Any advice 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 2021

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.