# China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies

Skadden

11 / 03 / 21

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

Two new Chinese laws dealing with data security and privacy came into force in the fall of 2021 that are likely to have an impact on many multinational companies operating in China or whose operations touch China. These two laws — the Data Security Law and the Personal Information Protection Law — provide more specificity about the data localization, data export and data protection requirements that first appeared in the Chinese Cybersecurity Law in 2017. This article discusses the key features of these new laws and the potential implications for multinationals operating in China.

## The Data Security Law

The Data Security Law (DSL) sets up a framework that classifies data collected and stored in China based on its potential impact on Chinese national security and regulates its storage and transfer depending on the data's classification level. The law is generally seen as a response to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which gives U.S. law enforcement agencies the authority to compel companies falling under U.S. jurisdiction to produce requested data regardless of where the data is stored.

### Categories of Data

"Core data" under the DSL — broadly defined as any data that concerns Chinese national and economic security, Chinese citizens' welfare and significant public interests — is afforded the highest degree of protection and regulation. "Important data" is the next-most sensitive level of data, but its scope is left undefined. The relevant national, regional and sector authorities are expected to issue catalogs in due course of what counts as "important data." The DSL applies to all data activities that take place in China as well as extraterritorially if the data activities are deemed to impair China's national security and public interest.

### Localization and Transfer of Data

The DSL clarifies and expands data localization and data transfer requirements for "core" and "important" data and for certain types of data handlers. For example, Critical Information Infrastructure Operators ("CIIOs") that handle data dealing with informational networks, infrastructure and natural resources must ensure that data that was generated in China is stored in China and that a security self-assessment is conducted before China-originated data is sent abroad. Furthermore, the DSL directs that additional rules and regulations be developed for non-CIIOs.

Both CIIOs and non-CIIOs are prohibited from providing any data *stored* in China, regardless of the data's sensitivity level and whether or not the data was initially *collected* in China, to any foreign judicial or law enforcement agency without the prior approval of the relevant PRC authorities. Companies found in violation of regulations concerning "core data" face penalties of up to RMB 10 million (~US$1.56 million), the forced shutdown of their businesses and potential criminal liabilities. Companies found in violation of regulations concerning "important data" face penalties of up to RMB 5 million (~US$780,000).

### Downstream Data Handlers

The DSL expands the scope of regulation to cover not just the initial collectors of data, but also downstream "intermediary services" that use data for commercial purposes. These downstream data handlers must ask the data providers from which they obtained the data to explain their data sources. The data handlers must also verify the identities of the parties


© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

to a data transaction and retain verification and transaction records. Data handlers that fail to comply with these requirements may face fines of up to RMB 2 million (~US$300,000), the forced shutdown of their businesses and the revocation of their business licenses.

### Data Security

The DSL requires companies doing business in China to establish and improve their data security systems, implement remedial measures when data security deficiencies are detected and promptly notify users and authorities of any data breaches. Companies handling data whose sensitivity rises at least to the level of "important data" are required to designate an officer or a management team responsible for the security of data and to submit regular risk assessments to the relevant PRC authorities. Companies that fail to protect their data may face fines of up to RMB 500,000 (~US$77,700). If a company fails to rectify its systems failures or if the failures resulted in large-scale data leaks, it may face fines of up to RMB 2 million (~US$300,000), the forced shutdown of its business and the revocation of its business licenses.

## The Personal Information Protection Law

The Personal Information Protection Law (PIPL) is China's first comprehensive legislation regulating the protection of personal information, and is modeled after the European Union's General Data Protection Regulation.

"Personal Information" is broadly defined to cover "any information related to identified or identifiable natural persons stored in electronic or any other format." So long as the information is "related to identified or identifiable natural persons," even if the information is not sufficient to identify a specific individual, the PIPL still applies. However, personal information irreversibly anonymized is not covered.

The PIPL generally applies to all types of data activities (*e.g.*, collection, storage, usage, reorganization, transmission, provision, disclosure and deletion) involving the personal information of data subjects in China, as well as activities outside China that are aimed at providing products or services to individuals in China or analyzing their behavior. Violations of the PIPL could face penalties of up to RMB 50 million (~US$7.78 million), 5% of a company's annual revenue and disgorgement of all illegal gains.

The PIPL imposes the following key obligations on data handlers:

### Consent Requirements

Before collecting or handling someone's personal information, a data handler must obtain the data subject's voluntary, clear and informed consent. Data handlers collecting or handling "sensitive personal information" — a category that includes the data subject's biometrics, religious beliefs, health, finances, geographical locations and young children — must, in addition, show the specific purpose and necessity of the data collection and follow certain stringent data protection measures specified in the PIPL. There are, however, a number of exemptions under the law where prior consent is not required, including, for example, performance of a contractual or statutory duty, responding to an emergency involving life and property, news reporting on a matter of public concern and where the information is already found in the public domain.

### Data Localization and Data Deletion Requirements

The PIPL provides that, if the volume of personal information being handled by the data handler reaches certain thresholds, the data localization requirement may be triggered, and the data handler would also be required to appoint an information protection officer to supervise the proper handling and protection of the personal data collected.

Data handlers are required to delete the collected personal data when the purpose of the collection has been achieved, when the information no longer serves its disclosed purposes, when the service is no longer being provided, when the retention period has expired, when the user rescinds consent or when the processing activities contravene relevant laws and regulations.

### Restrictions on Transfer of Personal Information to Third Parties and Overseas

Before a data handler can transfer personal information to third parties, either within China or overseas, it must first obtain the data subjects' informed consent and ensure that the data recipient's use of the data and data-handling methods abide by the terms of the data subject's consent.

For cross-border transfers, the data handler must also ensure that the foreign recipient of the data has in place data protection requirements that are no less stringent than those imposed by the PIPL. Depending on the classification of the data handler based on the sensitivity and volume of data in its possession, additional requirements may apply. For example, CIIOs and companies in possession of a large volume of personal data must complete a mandatory security review led by the Cyberspace Administration of China before transmitting any data overseas.

### General Compliance Requirements

The PIPL requires companies handling personal data to conduct regular self-audits to assess their information security risks and implement corresponding policies and safeguards. Increasingly stringent rules may apply depending on whether a company qualifies as a "major internet service platform," has a "large number"

of users and engages in "complex business activities," but those terms are not defined in the law. Companies that make use of algorithms and similar automated decision-making functions to analyze data subjects' personal information must abide by certain "transparency" and "fairness" principles set forth in the PIPL that prohibit certain types of discriminatory pricing and marketing activities based on the data subject's personal status and protected characteristics.

## Implications

### Reassessment of Existing Storage Practices of Data Originating in China

With the passage of the DSL and the PIPL, multinational companies with operations in China would be well advised to assess and, if necessary, reconfigure their information technology systems to ensure compliance with PRC law, and to seek the advice of local PRC counsel before exporting data that was initially gathered in China or that is currently stored in China.

### Providing Chinese Data to Foreign Regulators or Foreign Courts

In the past, subject to state secrecy and data privacy screening by qualified Chinese lawyers, multinational companies with operations in China were able to respond to foreign regulators' subpoenas and requests for information directly, without first obtaining the approval of the Chinese authorities, even if the requested data concerned Chinese individuals or the multinational companies' China-based operations. Similarly, in connection with foreign litigation proceedings, multinational companies were able to collect responsive documents in China and produce them to opposing counsel in discovery without the PRC authorities' prior approval.

This is no longer the case under the newly enacted DSL and PIPL. Together with other laws that the PRC authorities enacted since 2018 — for example, the Criminal Judicial Assistance Law and Article 177 of the Chinese Securities Law — companies seeking to comply with U.S. and other foreign regulators' information requests, or fulfill their discovery obligations in ongoing U.S. litigation, should consult Chinese counsel before transmitting such information overseas.

### Restrictions on Marketing Activities

The PIPL enacts new requirements that regulate companies' marketing activities using their prospective customers' personal information. As noted above, the PIPL regulates the use of algorithms and other automated systems that have the effect of discriminating against certain classes of consumers. Consent is also required in most circumstances. Multinational companies seeking to market their products and services to prospective Chinese customers using personal data would be prudent to seek legal advice before undertaking such marketing activities.

## Contacts

**Ryan D. Junck**
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

**Bradley A. Klein**
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

**Akira Kumaki**
Partner / Tokyo
81.3.3568.2448
akira.kumaki@skadden.com

**Ken D. Kumayama**
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

**Steve Kwok**
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com

**Eve-Christie Vermynck**
Counsel / London
44.02.0751.9709
eve-christie.vermynck@skadden.com

**Siyu Zhang**
Associate / Hong Kong
852.3740.4816
siyu.zhang@skadden.com