NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Manatū Aorere

China's Data Governance Framework takes shape: Implications for New Zealand businesses

Market Report

JANUARY
2022

Prepared by the New Zealand Embassy in Beijing

Summary

- China recently enacted two key legislative pieces of its comprehensive cybersecurity and data governance framework – the *Data Security Law and the Personal Information Protection Law* – both of which build on, and work in concert with, the *Cybersecurity Law* enacted in 2017.
- These three laws create a framework for categorising different types of data and establish rules governing how entities operating in China need to manage and store their data. Although much of the specific detail remains to be defined, the framework will impact Aotearoa New Zealand companies that handle data relating to China and Chinese citizens.
- This reports highlights some areas that may be of interest, but is not exhaustive. Companies that think some of their operations will fall within the new laws would be best to seek legal advice on the matter.

Report

In 2020 China designated data as a "fifth factor of production" (alongside land, labour, capital, and technology), elevating it to a key economic resource expected to drive future economic growth. In this context China's new data governance framework can be seen as an attempt to establish a system of "law-based governance" where the economic benefit of "safe" data can be realised, while sensitive data are identified and protected.

Data Security Law

China's *Data Security Law (DSL)* came into effect on 1 September and is primarily concerned with regulating data handling and processing activities that could have a national security impact (unofficial translation here).

The **law applies to all individuals, companies, and government departments engaging in the collection and use of data in China** and imposes a range of high-level data protection and security obligations on these entities. At present the law is broadly defined in most areas, with many specific details to be determined in forthcoming implementing rules, regulations, and official documentation.

Specific obligations outlined in the law of potential interest to companies handling data in China include requirements to:

a. Establish data security management systems across their entire workflow, adopt technical measures to safeguard data security, and conduct data security training;
b. Monitor potential risks, and in the event of data security incidents notify users and report incidents to the relevant regulatory authorities.

One of the notable features of the DSL is that a "hierarchical system for data protection" will be established, under which all data would be categorised according to its importance in "economic and social development, as well as the degree of danger to national security, public interests", among other considerations.

The DSL refers to a category of "important data", for which additional obligations apply, including requirements to:

a. Designate a data security officer and set up a management office to fulfil data security protection responsibilities;
b. Periodically conduct risk assessments on their data processing activities;
c. Submit a risk assessment report including details of the type of data being processed, and how security risks are being addressed.

The law notes that specific security management measures for entities exporting "important data" collected or produced within China will be drafted in the future.

A second category of data mentioned in the DSL is "core national data", broadly defined as "data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests". Data categorised as "core national data" will be subject to an even stricter management system.

The process of categorisation has already begun for data relating to certain industries and involves local, regional, and central government entities.

Data relating to smart cars is one of the few areas where classification guidelines have already been published by the Cyberspace Administration of China (CAC), which may indicate how data may be categorised in other areas. These guidelines set out what constitutes "important data" and "core national data" for this particular industry, and what types of data require approval before they can be exported

The DSL also includes a number of provisions relating to the cross-border provision of data including an article stating that entities in China must not provide data stored "within the mainland territory of the PRC" to the justice or law enforcement institutions of foreign countries without the approval of "the competent authorities of the PRC".

The law does contain specific details of sanctions for non-compliance, particularly in terms of cross-border data provision. For example, fines of up to two million RMB (NZ$500,000) could be levied in cases where "corrections are refused or a large data leak or other serious consequences are caused".

Personal Information Protection Law

The *Personal information Protection Law (PIPL)* came into effect on 1 November (unofficial translation here) and sets out some potentially far-reaching rules and obligations for those handling personal information in China or relating to Chinese citizens.

Entities that will be considered "personal information processors" are defined as "organisations or individuals that independently decide the purpose and method of processing of personal information". The law defines "personal information" as "all kinds of information related to identifiable natural persons recorded by electronic or other means, excluding information processed anonymously".

The **PIPL explicitly applies to foreign organisations that process personal data overseas for the purposes of, amongst others, "providing products and services to Chinese consumers as well as analysing the behaviours of Chinese consumers"**. The implication of this extraterritorial application is that foreign entities in this position will have to establish designated agencies or appoint representatives based in China to take responsibility for issues related to the handling and protection of personal information.

Of further potential interest to foreign entities handling data related to China is the section relating to cross-border data transfers. The PIPL states that companies wanting to transfer personal information out of China must meet one of a number of criteria before this is possible. One option is for an entity to pass an assessment or undergo certification as administered by the Cyberspace Administration of China (CAC). Another is for entities to sign a "standard contract" issued by the CAC agreeing the rights and responsibilities of both sides. In addition, entities would also need to obtain separate consent from individuals regarding transfer of their personal information.

Subsequent regulations

Some implementing regulations have already been published, which provide additional detail in certain areas. Most notably for foreign companies, the CAC released a draft document (link in Chinese) on October 29 2021 which sets out some more detail of the procedures for obtaining approval to export sensitive data from China, a requirement under both the PIPL and DSL.

The new regulations clarify the competent authority for data assessments as the CAC, and state explicitly that all companies seeking to export "important data" are required to apply for an assessment. In addition, any critical infrastructure operator, or entity that cumulatively exports the personal information of more than 100,000 individuals would also need to apply.

The regulations also clarify that companies do not have to apply every time they export data but can seek approval for continuous export of certain types of data, however this must be applied for every two years. In addition to the type of data

being exported, the CAC's data assessment process will consider whether the transfers are legal and necessary, the scope and method of transfer, and whether the data protection laws of the country meet China's standards.

The wide scope of the laws means that Aotearoa New Zealand businesses operating in China, or those outside Chain handling data on Chinese citizens, will need to continue to keep informed about their ongoing and emerging obligations and seek legal advice as appropriate.

More reports

View full list of market reports from MFAT at www.mfat.govt.nz/market-reports

If you would like to request a topic for reporting please email exports@mfat.net

To get email alerts when new reports are published, go to our subscription page.

To contact the Export Helpdesk

Email exports@mfat.net
Call 0800 824 605
Visit Tradebarriers.govt.nz

Disclaimer

This information released in this report aligns with the provisions of the Official Information Act 1982. The opinions and analysis expressed in this report are the author's own and do not necessarily reflect the views or official policy position of the New Zealand Government. The Ministry of Foreign Affairs and Trade and the New Zealand Government take no responsibility for the accuracy of this report.