How China's new data protection law is reshaping businesses

April 2022

LOCKTON®

AUTHORS

Kegan Chan
Senior Vice President
Head of Analytics - Greater China
+852 2250 2867
kegan.chan@lockton.com

Melody Qian
Senior Vice President
Head of Global Professional &
Financial Risks - Greater China
+852 2250 2672
melody.qian@lockton.com

The Personal Information Protection Law (PIPL) sets new rules for processing personal data related to individuals living in China as well as Chinese citizens abroad. To comply with this law, businesses are having to reassess and rearrange their operations.

The background

The People's Republic of China's (PRC's) Government formally implemented the Cybersecurity Law on 1st June 2017. It introduced greater protection on personal privacy, higher requirements for enterprises' cyber security management as well as fines and penalties.

The Personal Information Protection Law (PIPL) was enacted on 1st November 2021 as China's first comprehensive legislation regulating the protection of personal information[1]. In parallel, China has introduced the Data Security Law (DSL) which created 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.

[1] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

How PIPL impacts your organisation

PIPL does govern personally identifiable information (PII) of any individual living in the PRC as well as PRC citizens living outside the country.

Individuals have more rights on the disclosure of their own personal data. They can edit, remove or restrict the use of their data, or withdraw consent given previously. Organisations who use automated decision-making or machine learning processes would be required to provide transparent explanations on how decisions are made in selecting Chinese individuals' personal data.

More stringent enterprise requirements on data sharing and transfer for which organisation and 3rd party data controllers to comply with. If an organisation posseses Chinese residents' data without a presence in China, it will have to either create a special agency or appoint representatives in China to be in charge of compliance. To transfer Chinese residents' data overseas, organisations are required to obtain consent.

Fines and penalties for organisations in relation to data breaches can reach RMB50m (or up to 5% annual revenue in the preceding year) and business cessation. Responsible personnel / managers can be fined from RMB100k – 1m along with prohibition from serving as a director / senior management for relevant enterprises for a certain period of time.

Data localisation when personal identifiable information (PII) volumes exceed the threshold (yet to be defined) set by the Cybersecurity Administration of China (CAC). Organisations meeting the criteria under China Cybersecurity Law for critical information infrastructure operator (CIIO) or process large volumes of Chinese personal data are subject to data localisation requirements. Foreign companies outside China will be bound by these new rules if they process data for providing goods or services to China, analyse behaviour of Chinese citizens or process important data.

Mandatory security controls when storing and processing PII, and training requirement for responsible personnel who handles the PII. To transfer Chinese resident data overseas, organisations are required to obtain consent, register the transfer with the government, or complete an assessment certified by a third party. Furthermore, they will need to implement technical security measures to prevent foreign-governments' access to the data and track onward transfer to other entities. Multinational conglomerates currently enhancing their data-transfer controls for EU's General Data Protection Regulation (GDPR) will need to apply an augmented approach to their Chinese data transfers and extend their assurance capabilities to the scope.

Important terms

Personal Identifiable Information (PII) are all kinds of information relating to identifying an individual (natural person) which are recorded by electronic or other means, excluding any anonymised information. PII also includes Critical Information Infrastructure (CII) and Sensitive Information (SI).

Processing information (article 4) means collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information and it must abide under the principle that it will have the least impact on individual rights and interests (i.e. not excessive) along with clearly addressing the purpose of collecting this information and obtaining the individual's consent.

Sensitive Information (SI) is information which once leaked or has been used illegally, may lead to infringement of a natural person's personal dignity or endanger the safety of persons or property, including information such as biometrics, religious beliefs, specific identities, medical health, financial accounts, and whereabouts, as well as the personal information of minors under the age of 14[2].

Critical Information Infrastructure (CII) is information which can result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or is leaked. Note that PIPL expands this requirement beyond CII operators to include all PII and SI handlers.

[2] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

With China's three cyber laws (CSL, DSL and PIPL) setting the new baseline for data controllership for non-Chinese multinational organisations, these organisations should take into account the key changes which may be applicable to their existing data. These include:

Dynamic Data Inventory

China requires classification of data in general, important and core categories. Multinationals with a significant presence in China will need to enhance their record of processing activities with new required fields and automate as much of this process as is feasible with data discovery, classification and workflow technologies.

Local Governance Staff

The legislation sets out extra requirements for appointing data responsible persons. If you are an offshore organisation that is processing the personal data of Chinese residents for the purpose of providing services or products, or for analysing and assessing their behaviour, you must establish a "dedicated office" or appoint a "designated representative" in China for personal information protection purposes, and also file the information of the entity or the representative with government authorities. Similar to the DPO (Data Protection Officer under the GDPR) to supervise PII handling activities, this representative's contact information must be publicly disclosed to the respective authorities.

Multilevel barriers to cross-border data transfers

To transfer Chinese resident data abroad, businesses must also meet one of the following conditions on top of obtaining their consent:

1. Pass a security assessment organised by the State cybersecurity and informatisation department (related to operators of Critical Information Infrastructure and organizations that transfer a large volume of personal information);
2. Undergo a personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatisation department;
3. Conclude a contract with the foreign receiving side in accordance with a standard contract formulated by the cyberspace and informatisation department, agreeing upon the rights and responsibilities of both sides;
4. Other conditions are provided in laws or administrative regulations or by the State cybersecurity and informatisation department.

For multinationals currently enhancing their data-transfer controls for GDPR or California Privacy Rights Act (CPRA), readiness will need to apply a similar but augmented approach to their Chinese data transfers and extend their SOC 2 assurance capabilities to this scope.

Multiple mandatory assessments

China's data privacy and security laws require risk and impact assessments across a broad array of use cases. Companies that automate their data privacy and protection impact assessments for the Americas and EMEA now have a driver to extend this capability to the Asia-Pacific region. One of the requirements include a Personal Information Impact Assessment[3] if your organisation is involved in one of the following operations:

- Processing sensitive personal information; or
- Using personal information to conduct automated decision-making; or
- Entrusting personal information processing, or providing personal information to other data controllers, or disclosing personal information; or
- Providing personal information abroad; or
- Other personal information processing activities with a major impact on individuals.

Consent management for use of all personal information

Under the PIPL, organizations can process personal information only on a lawful basis. PIPL provides seven lawful basis for the processing of personal information. Please find these lawful basis here and ensure that your organization relies on one of these basis for the processing of personal information. Your organization's processing activities should have a clear and reasonable purpose and shall be directly related to the processing purpose. Please note that, unlike the GDPR, "legitimate interest" is not a recognized lawful basis under the PIPL. China's rules amplify the impact on consumer-facing companies of similar consent requirements in Europe and the United States at the same time as technology platforms are restricting the use of tracking mechanisms such as cookies, putting a premium on permission-based consumer relationships.

Faster incident response and breach notification

Under the PIPL, data processors must take "immediate" action and notify multiple business and government stakeholders as well as affected individuals about any incidents, risk of data breaches and remedial actions they've taken within five working days after completing an investigation of the breach. If the incident involves important data or personal data on more than 100,000 individuals, companies must report the breach to the appropriate regulators within 8 hours[4].

This timeline is among the most stringent globally and will require state-of-the-art detection, response and resilience capabilities typically seen only in advanced financial and technology companies.

[3] https://securiti.ai/blog/pipl-compliance-checklist/
[4] https://www.huntonprivacyblog.com/2022/01/26/china-releases-draft-regulations-on-network-data-security-management/

Implement data classification and management mechanisms

The PIPL requires organisations to formulate internal management structures and operating rules to classify data as:

1. general data
2. important data
3. core data

The classification depends on the data's impact and degree of importance to national security and public interests. Consistent with the CSL and DSL, the PIPL will require these categories of data to be protected based on China's Multi-Level Protection Scheme ("MLPS"), which mandates data security standards for different classifications of data. For example, data handlers will be required to implement security measures (e.g., data back-ups, encryption, access controls) and strengthen protections around their data processing systems, transmission networks and storage environments, based on the MLPS.

Platform transparency reports

If your organisation handles a large digital platform, the PIPL outlines that data processing organisations should enforce fair, transparent and impartial data-processing rules for the product and service providers who use it. This may require the publication of social-responsibility reports on data handling, the establishment of a personal information protection compliance system, and the creation of an independent, external body to supervise personal information protection.

Audit trail and controls on data processing agreements with third-party processors

An organisation's internal audit department usually constitutes the third line of defence in organisational internal controls but generally has not maintained a data privacy function. The new PIPL in China does not explicitly require internal audit privacy expertise but if PIPL applies, data privacy is likely to join cybersecurity as a top risk and will require ongoing monitoring and control.

However, if the organisation engages third parties for processing activities, then it must ensure to conclude an agreement with the third parties setting the time limit, the processing method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information processing activities of the third parties.

There is currently no clear timeline for complying with the PIPL, but there is reason to believe that it could be up to one and a half years.

The PIPL's relationship to other China cyber laws and comparison with global laws

There are now three laws governing data and information protection in China:

1. The Cybersecurity Law of the People's Republic of China (CSL), implemented on 1st June 2017.
2. The Data Security Law (DSL), enacted on 1st September 2021 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.
3. The Personal Information Protection Law of the People's Republic of China (PIPL), enacted on 1st November 2021.

COMPARISON OF THE THREE MAJOR DATA AND INFORMATION SECURITY LAWS[5]

	Cybersecurity Law	Data Security Law	PIPL
Purpose	Ensure cybersecurity, secure cyberspace sovereignty, national security, and public interests.	Ensure data security and focus on data processing activities, data development, and data utilisation.	Protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information.
Priority	Security of the cyberspace	Security of the data itself, data processing activities, and safety supervision.	Protection of personal information.
Scope of Application	Network construction, operation, and maintenance in China.	Data processing activities carried out within or outside China.	Personal information processing of natural persons within China and personal information processing of natural persons outside China under certain conditions.
Definition of data	Various electronic data are collected, stored, transmitted, processed, and generated through the network.	Any recording of information by electronic or other means.	No definition of data
Who are regulated	Network operators.	Any organisation or individual that processes data.	Any organisation or individual that processes personal information.
Extraterritorial jurisdiction	Not applicable.	Applicable under certain conditions.	Applicable under certain conditions.
Cross-Border data transfer	Security review shall be carried out in accordance with relevant measures.	Relevant administrative measures formulated by the Cyberspace Administration of the State and the relevant departments under the State Council shall be followed.	Safety assessment might be required by the Cyberspace Administration of the State.

[5] https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/ China's Data Security Law in Effect Sept. 1, 2021: Prepare for Compliance (china-briefing.com)

For multinational corporations operating in the Greater Bay Area and perhaps the rest of Mainland China, compliance with the three China laws may present a challenge if they are also subject to GDPR (General Data Protection Regulation) in Europe and CPRA (California Privacy Rights Act) requirements, not to mention other local cyber laws of other countries such as Brazil (LGPD) and South Africa (POPI).

COMPARISON OF PIPL WITH GDPR AND CPRA[6]

Provisions	PIPL	GDPR	CPRA
Right to stop processing	Right to limit or refuse processing of personal information, with some exceptions; right to withdraw consent.	Right to withdraw consent or otherwise stop processing of EU personal information.	Right to opt out of selling/sharing personal information; must include opt-out link on website.
Right to stop automated decision-making	Right to explanation and right to refuse solely automated decisions with significant impact.	Right to require a human to make decisions that have a legal effect.	Regulations to govern access and opt-out rights for automated decision-making technology.
Right to stop third-party transfer	Requirement to obtain explicit consent before transfer to third parties.	Right to withdraw consent for data transfers involving second purposes of special categories of data.	Right to opt out of selling/ sharing personal information to third parties.
Right to equal services and price	Partial. Cannot refuse to provide goods and services if individual refuses to consent (unless necessary).	At most, implicitly required.	Explicitly required.
Regulator enforcement penalties	Ceiling of 5% of annual revenues or RMB 50m ($7.8m), plus potentially unlimited penalties to businesses and individuals.	Ceiling of 4% of global annual revenues.	No ceiling—$7,500 per violation.

[6] https://www.mondaq.com/china/data-protection/1122748/the-comparison-between-china39s-pipl-and-eu39s-gdpr-practitioners39-perspective
https://wirewheel.io/ccpa-and-cpra-california-data-privacy-law-guide/

Recommendations

To align the business with the stringent triple cyber laws from China and the rest of the cyber regulations around the globe, organisations are undertaking a rigorous reorganisation. The following recommendations may help making this process more efficient.

- Localise data for the Chinese market, including Chinese nationals outside the country (Employees / Customers)
- Conduct a cost and benefit analysis on investment returns for the Chinese market
- Assess and evaluate vendors within the supply chain to mitigate risks of servicing Chinese client bases
- Transfer parts of these risks via insurance solutions such as cyber insurance, director's and officers' insurance and professional indemnity (errors & omissions) insurance.

STEPS IN THE PROCESS

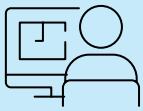
Step 1

Identify exposure

Assess whether the organisation is currently handling Chinese residents' information. If so, assess and have these processes documented. It is important to address the legal basis for these activities and the location of the documentation, along with the date-use life cycle (e.g. data retention period, data disposal...etc). Is the organisation a Critical Information Infrastructure (CII) Operator or does it hold records large enough to face additional compliance requirements?

Should these be addressed within the organisation's risk register or namely, a top cyber priority?

Step 2



Gap Analysis & Impact Assessments

Upon addressing and fulfilling the compliance protocols, are risk mitigation and risk transfer (insurance) measures in place when certain scenarios arise, such as a cyber breach, cross-border data transfer accident or ill trained data protection officers? What is the quantum of potential fines & penalties or losses the organisation may face?

Step 3

Enhancing existing IT frameworks and infrastructure

Establish new roles and responsibilities dedicated to privacy management, refine policies & procedures, formulate processes on dealing with personal information protection and impact assessment frameworks, keep an audit trail supported by technology solutions.

Step 4

Risk Transfer Solutions

As no system or process is 100% foolproof and no organisation can guarantee that no human errors may happen in the company, businesses need to make up for the potential shortfall, which will be borne by the organisation right from their balance sheet.

The utilisation of cyber insurance and other related insurances such as professional indemnity (errors & omissions) and directors' & officers' insurance can act as the financial buffer to make up for the organisation's shortfall should these events occur, and at times, preserve the viability of the business.

YOU CAN READ MORE ABOUT RISK TRANSFER SOLUTION - CYBER INSURANCE HERE

For further information, please contact us at enquiry.asia@lockton.com.

UNCOMMONLY INDEPENDENT