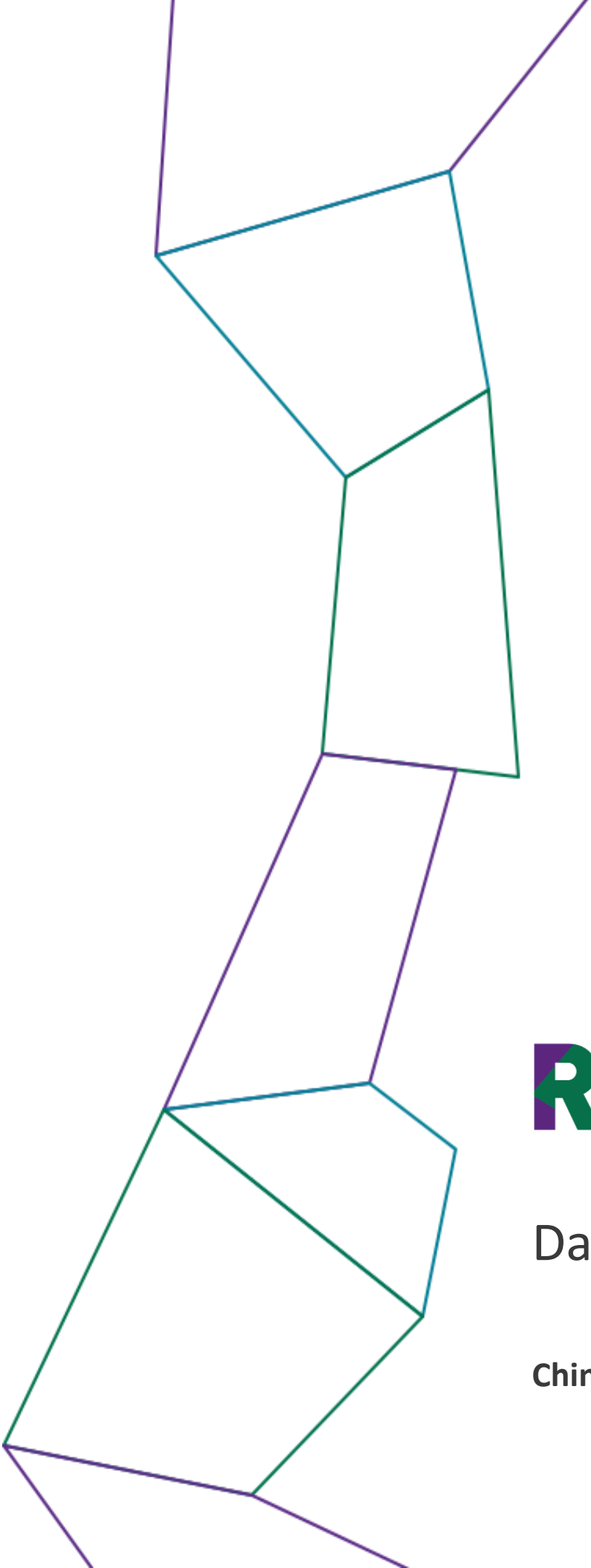

ROUSE

Data Privacy Q&A

China

DATA PRIVACY Q&A: CHINA

Is there a data privacy law in your jurisdiction? If yes, is it implemented? If no, what laws are relied on?

Yes. China's Personal Information Protection Law ("PIPL") was passed on 20 August 2021 and went into force on 1 November 2021. The PIPL is China's first omnibus law regulating personal information protection.

What significant legal instruments relating to data protection are currently pending? If any, what are the timelines?

A number of implementing regulations for the PIPL are in the process of legislation. They include, among others, the third version of *Measures for the Security Assessment of Outbound Data (Exposure Draft)* ("Measures") which was released on 29 October 2021 by the Cyberspace Administration (CAC) for public comments. The CAC, as China's principal cybersecurity enforcement agency, dictates in the Measures specific circumstances in which security assessments are required. While the legislative timeline is unclear, the Measures will likely be enacted in 2022. The CAC is also expected to issue standard contractual clauses for cross-border transfer of data.

Who does the China Protection Law apply to?

The PIPL has extra-territorial effect. It can apply to the processing of personal information of natural persons located in China irrespective of the location of the processing making it crucial for both entities doing business in or with China to consider whether they fall within scope of the PIPL. For entities engaged in personal information processing activities outside China, the PIPL will apply if:

- The purpose of processing personal information is to provide products or services to natural persons in China
- Where analysing or assessing activities of natural persons inside China
- Other circumstances provided in laws or administrative regulations

Who are the relevant regulatory and enforcement authorities in China with regards to Personal Data protection?

The CAC serves as the main authority overseeing personal information protection. That said, other government agencies such as the Ministry of Public Security, which leads broader data security efforts, Ministry of Industry and Information Technology, and Ministry of Science and Technology, can also enforce the PIPL.

How is Personal Data defined in China?

The PIPL defines personal information as all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons located in China. Personal information does not include anonymized information that cannot identify a specific natural person.

Is there a distinction between Personal Data and Sensitive Data under the law?

Yes, the PIPL defines sensitive personal information as personal information that when disclosed or illegally used, may cause harm to the dignity of natural persons. Sensitive personal information includes, among others, information on biometric characteristics, religious beliefs, personal identity information (such as ID card, passport, driver's license, work permit, social security card, residence permit, etc.), medical health, financial accounts, individual location tracking and personal information of minors under the age of 14.

Under the PIPL, sensitive personal information processing requires a specific purpose, specific need, and stricter protective measures. The relevant individual's separate consent must be obtained, and written consent is required if stipulated in other laws/regulations.

Personal information handling entities[1] are also obligated to inform the relevant individuals of the necessity of processing sensitive personal information and the impact(s) on their rights and interests. Personal information of minors require the consent of the parent/guardian.

What are the legal bases of processing personal data in China?

Below are the legal bases for processing personal information under the PIPL:

- Obtaining individuals' consent
- Where necessary to perform a contract to which the individual is a party, or to implement human resources management
- Where necessary to fulfil statutory duties and responsibilities or statutory obligations
- Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property under emergency conditions
- Handling personal information within a reasonable scope for purposes of news reporting and other activities serving the public interest
- Handling personal information disclosed by persons themselves or otherwise already lawfully disclosed
- Where permitted by other laws and administrative regulations

[1] Handling, also referred to as processing, includes collection, storage, use, alteration, transmission, provision, and deletion of personal information. A personal information handler, as organizations/individuals that determine the purposes/means of personal information processing, is similar to the GDPR's data controller.

What is the consent requirement in China?

When consent serves as the legal basis for personal information processing, the individual must be fully informed and consent must be voluntarily and express. Where there is a change in the purpose of personal information handling, the handling method, or the categories of handled personal information, new consent regarding the change must be obtained.

What rights do individuals enjoy under the PIPL?

The PIPL is significant in that it provides individuals with a wider and stronger range of rights such as the below:

- Right to know and right to make decisions relating to their personal information; right to limit or object to the handling of their personal information by others (unless laws or administrative regulations stipulate otherwise)
- Right to access and copy their personal information from personal information handlers, and when such request to access and copy personal information are made, the personal information handler must respond in a timely manner
- Right to request correction and supplementing of personal information to which personal information handlers must respond in a timely manner
- Right to have personal information handlers proactively delete personal information in the following instances: (1) processing under the stated purpose has been achieved/is impossible to achieve, or the personal information is no longer necessary; (2) the products or services for which personal information was handled is no longer provided, or the retention period has expired; (3) consent has been revoked; (4) personal information handling violates laws, administrative regulations, or agreements; or (5) as provided in other laws or regulations.

What restrictions are there for cross-border transfer of personal data?

Entities handling personal information, due to business or other needs, can transfer personal information outside China if it (1) adopts necessary measures to ensure that offshore recipient of the personal information matches the level of personal information protection as provided in the PIPL; and (2) fulfils the following requirements:

- Obtain relevant individuals' separate informed consent. In practice, entities may obtain separate consent through an interactive notification interface requesting consent, such as a separate pop-up box. "Separate consent" in the PIPL context is understood to require "one processing, one notification, and one consent" so that consent specifically corresponds to only the notified and consented personal information processing scenarios, and aims to prevent arbitrary collection, excessive processing and other illegal situations. That said, it remains uncertain whether personal data collected based on the exceptions of "individual's consent" still requires "separate consent" for cross-border transfers. Forthcoming implementing regulations and/or legal interpretations is expected to provide further guidance on this issue.
- Conduct a personal information protection impact assessment prior to the offshore transfer of personal information
- Satisfy one of the following conditions:

1. Pass a security assessment organized by state cybersecurity authorities
2. Undergo personal information protection certification conducted by a specialized body to be named by state cybersecurity authorities
3. Enter into a contract with the overseas recipient using the standard contract formulated by the CAC, specifying the rights and obligations of both parties
4. Fulfil requirements under other laws or administrative regulations or by the state cybersecurity authorities

Is there a data localization requirement under the PIPL?

The PIPL requires storage of personal information in China in the following circumstances:

- Personal information processed by government agencies
- Personal information collected or produced in China by critical information infrastructure operators
- Personal information collected or produced by handlers processing personal information that reaches a threshold to be later prescribed by the CAC

What liabilities/penalties would non-compliance with the PIPL result in?

Non-compliant entities will face fines ranging from RMB 1 million to RMB 50 million or 5% of the preceding year's revenue, as well as other operational sanctions such as suspension of business activities or even being banned from operating in China.

CONTACT US

Sunny Su
Senior Associate

E: ssu@lushenglawyers.com
T: +86 10 8632 4100

Chris Vale
Director

E: cvale@rouse.com
T: +852 3412 4001