Top 5 China Data Privacy Guidelines

www.asia-advisers.com

Asia Advisers

+86 157 1017 5083
info@asia-advisers.com
www.asia-advisers.com

Asia Advisers

Top 5 China Data Privacy Guidelines

www.asia-advisers.com

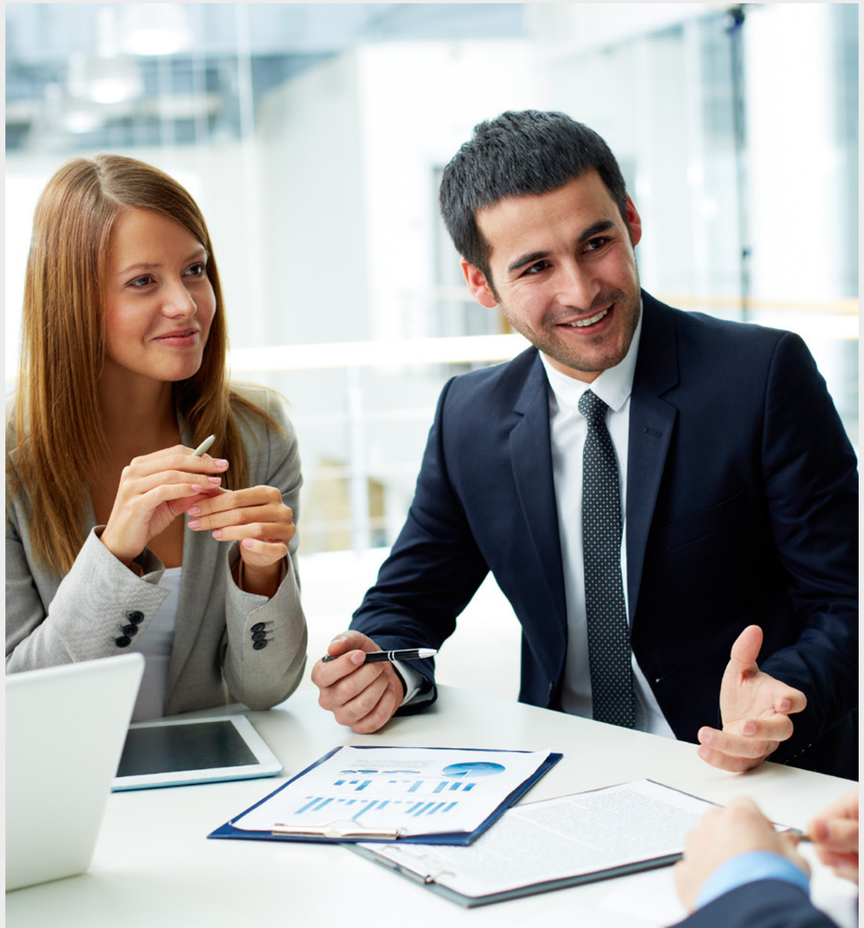
Now more than ever, as companies prepare for China's newest privacy regulation—the Personal Information Protection Law (PIPL), slated to take effect in early 2022—stakeholders must make sure they have all their proverbial ducks in a row.

Operating a business in China is complex but rewarding. It requires an awareness of local data privacy law and a series of practical solutions to ensure compliance.

+86 157 1017 5083
info@asia-advisers.com

Asia Advisers

The first step is to review the top 5 data privacy guidelines in China:



www.asia-advisers.com

01 Ensure the protection of any sensitive personal information.

The current draft PIPL defines "sensitive personal information" as any data that can affect consumers' safety or property in the event it is disclosed or used illegally. This includes information such as race, ethnicity, religion, medical or financial records, location details, and even phone numbers and email addresses.

The scope is broad, yet all the above information should be protected under Chinese law. This means your company may want to design a unique, differentiated privacy notice interface that allows consumers to provide their explicit consent for every purpose you may have for processing their information.

02 Implement encryption and de-identification measures.

As described above, consent is key to data privacy in China—and so too are encryption and de-identification measures that safeguard user information. To protect consumers' privacy, you might deploy encryption measures for your server, network, and computers to reduce your risk of a potential security breach.

In this same vein, applying de-identification measures can help you decrease the sensitivity of your consumer data, or even anonymize it. Ultimately, both encryption and de-identification can help to ensure compliance with the upcoming PIPL.

Asia Advisers

03 Understand “privacy by design” vs. “privacy by default.”

Does your team understand the difference between “privacy by design” and “privacy by default”? Some context: When making design decisions, companies must consider data privacy from the very beginning. This means the default setting of all apps and systems should emphasize personal information protection.

What might this look like? While many companies collect consumer data by default but allow consumers to opt-out down the road (say, by allowing them to “unsubscribe” from an email list), this shouldn’t be the standard. Instead, consumers should have to give their express permission to have any of their data processed in the first place.

04 Regularly audit your personal information processing activities.

To keep from violating China data privacy regulations—including the upcoming PIPL—you’ll want to consistently audit your company’s personal information processing activities and protection measures. You can ensure compliance by maintaining all risk assessment reports and processing records for less than three years.

This includes everything from how you leverage your automated decision-making to the channels through which your teams share personal information outside of China. In the event of a breach, please note that you will need to notify the authorities immediately and rectify the situation in compliance with the PIPL.

05 Closely monitor your staffing and training.

When it comes to data privacy, staffing and training are critical. For the former, all companies operating in China must employ a designated general information security team, a privacy rep, or a data protection officer (DPO) to protect consumers’ personal information.

Per Article 51 of the PIPL, even businesses based outside of China must have a unique agency or representative located in China to protect consumer information. The draft PIPL also asserts that companies must conduct regular security and privacy training for all staff members, focusing on personal information protection.