The Great Wall of Data Privacy: China Passes Comprehensive Data Privacy Law

On Aug. 20, 2021, the Standing Committee of China's National's People's Congress, the top legislative body of the People's Republic of China, adopted a national privacy law. The extensive law, named the Personal Information Protection Law (PIPL), will take effect on Nov. 1, 2021. With the passage of the PIPL, China is the third country with a competitive global economic presence to have a national privacy law, leaving the United States as the only nation in the top four global economic leaders without one.

PIPL, which has drawn comparisons to the European Union's General Data Protection Regulation (GDPR), is the first law in China that provides individuals with rights relating to their personal data. However, the law does build on China's new Cybersecurity Law, the Data Security Law (DSL), specifically relating to data transfer and storage restrictions. Some of the most important aspects of PIPL are detailed below.

Who does PIPL apply to?

PIPL applies to entities doing business in China, as well as entities conducting business wholly outside of China that process personal information belonging to natural persons within the territory of China (ring any GDPR bells?). Specifically, the PIPL applies to businesses outside of China where: 1) the purpose of processing it to provide products or services to domestic natural persons; 2) the purpose is to analyze and evaluate the activities of domestic natural persons; and 3) there are other circumstances provided by laws and administrative regulations. Of note, the law applies to both the public and private sector, but it ***does not apply*** to China's government.

What does PIPL do?

Much like GDPR, PIPL establishes certain privacy rights for Chinese consumers. Specifically, Chinese citizens will have the right to access, correct, know and delete their personal information, as well as a right to data portability, restrict processing and certain rights relating to automated decision-making. Chinese consumers will also be able to withdraw consent and lodge a complaint with regulators. Businesses are obligated to set up easy mechanisms for Chinese consumers to exercise such rights.

Transfer of personal information to entities outside of China, including the United States, will require entities to provide individuals with certain information about the transfer, and obtain separate consent for the transfer. Further, the business will have to adopt certain measures to ensure that the overseas entity can provide the same level of protection required under PIPL, and the business will also have to conduct a personal information protection impact assessment. In some circumstances, if businesses are considered Critical Information Infrastructure Operator (CII Operator), they may be required to store data in China and gain approval from the Cyberspace Administration of China (CAC) prior to transfer outside of the territory of China.

Also, like GDPR, PIPL requires businesses to justify their data processing via certain enumerated lawful bases, such as processing as necessary to perform a contract or to perform legal responsibilities or obligations. However, unlike GDPR, PIPL does not provide a "legitimate interest" provision as a lawful basis for processing personal data. PIPL has both "Personal Information" and "Sensitive Personal Information," the latter including things such as biometrics, religious beliefs, specific identities, medical information, financial accounts, location data and data for individuals under the age of 14. To process such information, businesses will need to have a specific purpose and sufficient necessity, take strict protective measures and have individual consent.

In addition to all the above, PIPL requires numerous additional obligations including, but not limited to, designating data protection officers (if applicable), preparing for and responding to data breaches, as well as complying with new regulations on facial recognition and biometric technologies.

What are the enforcement mechanisms?

The regulators of PIPL have a number of enforcement mechanisms at their disposal. Specifically, they can issue warnings, take corrective action, suspend services or issue a fine. The fines are significant, as they can be up to 50 million RMB (which equals over $7 million US) or 5% of a business' annual revenue for the prior fiscal year. Businesses that violate the law may also be recorded into the "credit files" of processing entities under China's social credit system. In addition, like GDPR, there is a private right of action for Chinese consumers.

What does this mean for your business?

PIPL is the newest legislation to hit the complicated data privacy landscape and involves the data of over one billion people. Companies that conduct business internationally, or that process data of individuals located within China, will want to ensure compliance with this new law. It is important to note that being GDPR compliant does not make a business compliant with PIPL. However, businesses that are already compliant with GDPR will have established a good framework to begin compliance processes for PIPL. Businesses subject to PIPL will want to work on compliance efforts now to ensure adequacy when the law becomes effective in a few short months, including updating your privacy policy and contracts to reflect PIPL specific requirements. It is likely that additional guidance will be published in the coming months outlining further compliance steps for businesses to follow, so we will continue to monitor any updates as they become available.

For more information regarding China's Personal Information Protection Law and to discuss compliance efforts businesses should be taking, contact Amber Lawyer, Jessica Copeland, Shannon Knapp or any attorney in the Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS