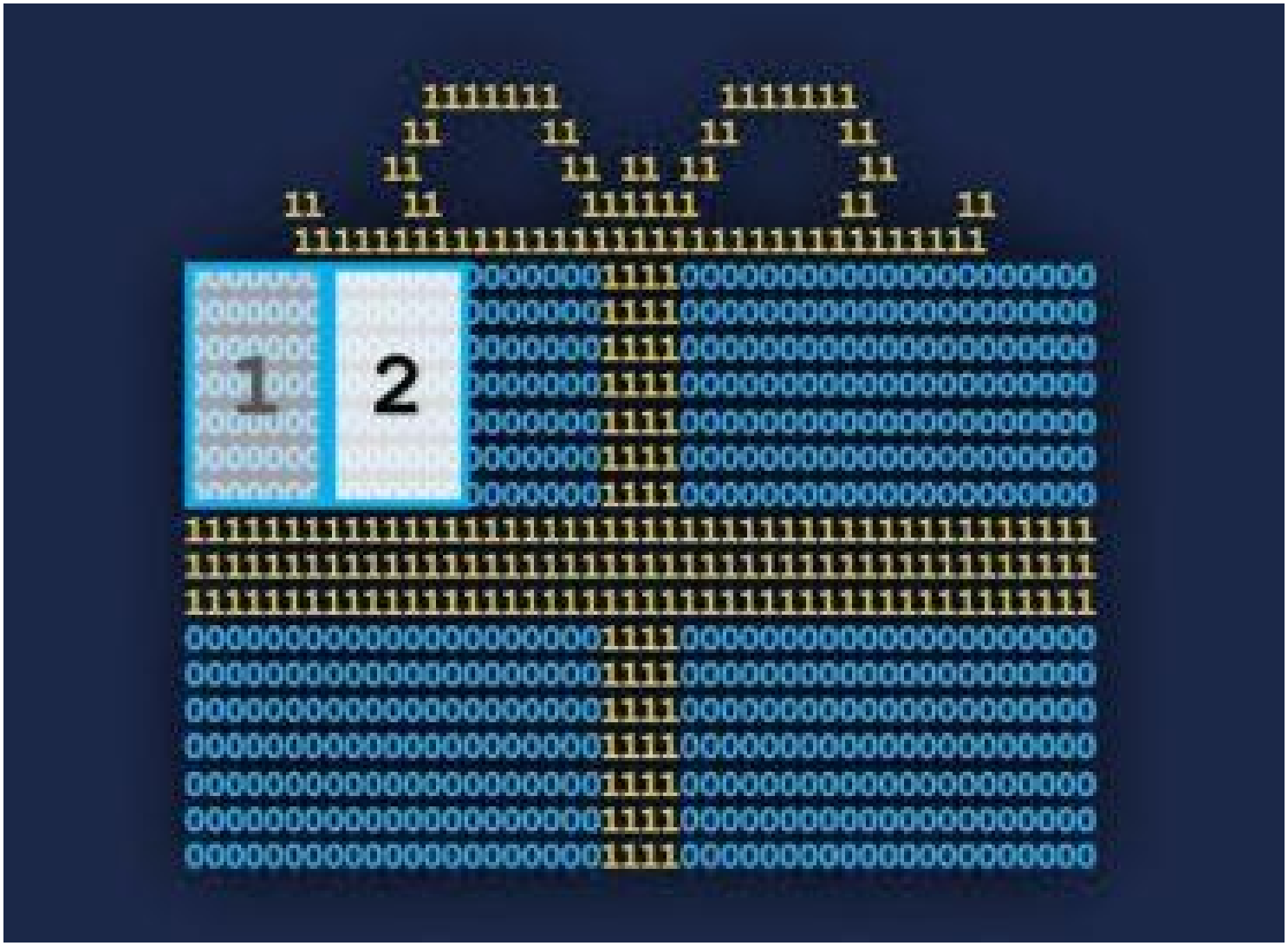
ROPES & GRAY
RopesDataPhiles
Practical Data, Privacy & Cybersecurity Tips from Ropes & Gray

What China's New Data Laws Could Mean for 2022

By Fran Faircloth & Brendan Kearney on December 15, 2021



2021 was a busy year for data protection law in China. On June 10, 2021, the Standing Committee of the National People's Congress of the People's Republic of China adopted the **Data Security Law** (DSL), which went into effect on September 1, 2021. On August 20, 2021, the Standing

Committee of the National People's Congress enacted the **Personal Information Protection Law** (PIPL), which went into effect just last month, in November 2021. The DSL applies broadly to processing of all data, not just personal information or electronic data and expands on the provisions from China's Cybersecurity Law, which was enacted in 2016. In contrast, the PIPL applies only to the processing of personal information and has been compared to Europe's General Data Protection Regulation (GDPR), although that comparison may obscure the contours of China's law more than it enlightens.

Consistent with the course of Chinese administrative law, the laws' key terms, analyses, and processes will continue to be fleshed out and perhaps materially enhanced or diminished in a series of regulations, measures, standards, and guidance documents. The latest draft measures on cross-border transfers, which are being closely watched by organizations contemplating cross border data transfers, were published at the end of October, and comments were accepted through November. We expect China to continue finalizing the laws' terms and measures in 2022.

Earlier this fall, Ropes & Gray LLP's **Katherine Wang** and **David Chen** joined **Mingli Shi**, Senior Associate Attorney for Global Privacy at Qualcomm, to discuss the practical implications of this complex legal evolution for businesses with operations in China. During the transition, they noted, companies should be moving toward compliance with the core requirements of the new regime with plans to fill in the gaps as China releases further details.

Ms. Wang explained how the new laws could significantly influence international businesses by requiring on-shore storage of large collections of personal or health data as well as data collected or generated by Critical Information Infrastructure Operators, a category of key entities that is still being defined. Much of the data that must be stored in China also must pass a cybersecurity review before possible export.

She explained how companies' obligations depend on the categories of data they process, ranging from personal data to "important data" (another evolving category) to sector-specific data, like human genetic resources (HGR) data. Other requirements arise from the classification of the entity holding the data, i.e., whether a company is involved in Critical Information Infrastructure (CII). A further consideration is a company's legal basis for processing the data, which recently expanded from a consent-based regime under the Cybersecurity Law to a broader set of possible bases under the Personal Information Protection Law (PIPL).

Both Ms. Wang and Mr. Chen noted that, while the PIPL uses some of the concepts from the GDPR, the laws are significantly different. Whereas the GDPR stems from a commitment to universal human rights, PIPL stems more from an assertion of Chinese national sovereignty and the ability of the state to control data through its law, as opposed to accepting the laws of other nations or the practices of global technology companies as de facto requirements. These differences become all the more apparent as the laws are examined in detail. For instance, there is no "legitimate interests" basis for processing under PIPL as there is under the GDPR, which means companies operating in both geographies may have to reassess their bases for processing certain personal information. Ms. Shi noted that though consent is not favored in Europe, consent is recommended under the PIPL, but without firm guidance on the details of the required consent and situations when a data subject withdraws consent. "Separate consent" is required under PIPL for cross-border transfers, though it is not yet clear how it should be obtained, Mr. Chen said. Some companies are considering separate consent forms or checkboxes, he noted, though there is a question whether separate consent is required if consent was not the legal basis for processing the data in the first place.

The PIPL's avenues for approved cross-border transfers raise another set of questions, Mr. Chen and Ms. Shi explained. Under the draft measures published late last month and now pending comments, for several categories – CIIOs that collect personal information or important data and companies that process have the personal data of at least 1 million people or who are transferring the personal data of 100,000 people – the only option is a security assessment by the Cyberspace Administration of China. Companies that do not require a security assessment will likely be able to rely on standard contracts, Mr. Chen said, though China's standard clauses have not been published, and may be much different from those that enable GDPR compliance for cross-border transfers. Intensifying these questions is the extraterritorial reach of the PIPL and the penalties for violating the law: fines of up to CNY 50 million or 5% of revenue from the previous year.

While the new laws' requirements give multi-national companies plenty to contend with now, more challenges loom over the long term. As China builds out its legal framework around data, Mr. Chen said, friction with the United States will likely persist, making cross-border transfers and **investments more complicated**. Companies will find it more and more difficult to operate on a worldwide basis with respect to data, prompting tough choices about operations in China.

Other countries in Asia are taking different approaches to data security. China’s approach may eventually dominate based on its economic influence, but only time will tell whether conflict or coherence is the continent’s data destiny. Companies should keep an eye out for further guidance from the China’s data-related agencies and Ropes & Gray LLP regarding the practical details of compliance in the months ahead.

RopesDataPhiles