SQUIRE PATTON BOGGS

China Passes New Data Privacy and Security Laws

Asia Pacific – 27 August 2021

The People's Republic of China (China), has been active lately in passing several new laws and regulations relating to data privacy and security. Here are two of the recent laws that tend to focus more on those handling national security data and/or public interest (aka Critical Information Infrastructure or Important Data).

Data Security Law

On June 10, 2021, The National People's Congress Standing Committee of the People's Republic of China passed the Data Security Law (DSL). The key focus of the DSL is the protection and security of critical data relating to national security and the public interest. The most significant element of the law is the so-called data classification system whereby the government will classify different types of data based on its level of importance and then publish a protection/security standard for each class of data. DSL also sets out certain general security obligations for data processors at large. Given the law is broad in nature, the immediate impact for companies may be limited. We expect to see implementing guidelines and standards to follow.

It is our expectation at present that DSL will have more impact on companies that possess data relating to national security and the public interest, including those with a large volume of personal data, critical infrastructure and critical industries, such as financial, medical and key technologies. We recommend that each company evaluate the type of data it processes and work with legal counsel to determine the level of requirements applicable. The DSL will take effect from September 1, 2021.

Security Protection Regulations on Critical Information Infrastructure

On August 17, 2021, the State Council of the People's Republic of China released the Security Protection Regulations on Critical Information Infrastructure (the CII Regulation). The CII Regulation is an implementing rule of the Cybersecurity Law (CSL). It applies only to Critical Information Infrastructure (CII), which refers to the network and IT system that are critical to national security and public interest, but may also have implications for companies that supply or service such networks and systems. Operators of CII are subject to much stricter rules in terms of data security and cross-border data transfer. Compared with CSL, the CII Regulation does not introduce any material new development in this regard.

There are no rules or public guidelines as to what network or IT systems are viewed as CII. The relevant government authority is supposed to evaluate and make decisions on a case-by-case basis, and a company, if determined to be a CII operator, will be informed of such decision. Nevertheless, we recommend companies conduct a self-evaluation from the following two aspects: (1) the nature of its businesses, and the type of data it processes, to evaluate the potential risk of being deemed to be a CII operator, and (2) if any of its customers may be deemed to be a CII operator, as the procurement of CII operators may be subject to a security assessment. The CII Regulations will take effect from September 1, 2021.

We further note that China's new Personal Information Protection Law, a draft of which we previously summarized, has just been passed. You can now read the update on its final version.

Contact

Lindsay Zhu
Partner, Shanghai
T +86 21 6103 6303
E lindsay.zhu@squirepb.com

About Us

Our China team works closely with our Data Privacy, Cybersecurity & Digital Assets team, which has more than 20 years of experience in data protection. We cover the full scope of privacy and cyber services, including proactive compliance work and risk assessments, incident preparation and response, post-incident remediation and crisis management, as well as privacy and cybersecurity litigation strategy. We also work with local firms to engage with local regulators and defend our clients.