SQUIRE PATTON BOGGS

China's Didi Fined Over US$1 Billion by Chinese Data Regulators

Asia Pacific – August 2022

On Thursday, July 21, the Cyberspace Administration of China fined Didi, China's largest ride service, ¥8 billion (approximately US$1.2 billion) for violations of the country's data privacy, data security and cybersecurity laws.

The fine reportedly amounts to more than 4% of its total revenue for last year. It also fined the company's chairman, Cheng Wei, and president, Jean Liu, ¥1 million (approximately US$150,000) each as being responsible for the company's violations. Regulators claimed Didi, since July 2015, collected nearly 12 million screenshots, 107 million pieces of passenger facial recognition data and more that 167 million records of location data, as well as other information, causing serious national security risks to the country's critical information infrastructure and data security. Didi has posted on its social media account that it has "sincerely" accepted the decision. It is reported that the government will now ease restrictions it had placed on Didi, including in the adding of new users and having apps removed from online stores in China.

It should be noted that Didi initially listed on the New York Stock Exchange in June 2021, a move that was not well-met by Chinese regulators, which launched a probe two days after the listing – a probe that included raids on the company's facilities. China subsequently issued several regulations to quickly close the loopholes of the cybersecurity/data protection legal regime, such as the Cybersecurity Review Measures, which require internet platforms holding more than one million Chinese individuals' data to pass a cybersecurity review before being listed overseas. Didi subsequently delisted in June 2022. It is reported that this resolution may now pave the way for Didi to list in Hong Kong (note – the Hong Kong Stock Exchange is not considered "foreign").

This matter shows the importance of knowing what data you are collecting in China and ensuring compliance with local laws, many of which are new (such as China's far-reaching Personal Information Protection Law and Data Security Law implemented in the fall of last year). Not only can the fines and penalties be substantial, but the disruption of services during any investigation can be just as serious. This is especially true if the data collected may be determined as important for national, political or economic security.

Authors

Scott Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

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

About Us

Our China data privacy team assists regional and multinational companies in dealing with cross-border data protection and transfer, governance and compliance, as well as localization. Our clients are from various industries, including high-tech, traditional manufacturing, services, transportation and infrastructure, investment funds, energy and power, telecommunications, and banking and financial services. They have worked with our regional data team to advise hundreds of clients on various evolving privacy and security requirements.

52238/07/22