January 2, 2018

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.
An ALM Publication

Cross-Border Data Transfers: CSL vs. GDPR

Helping in-house counsel with GDPR exposure to prepare for the data-transfer requirements of China's Cybersecurity Law (CSL).

By Xiaoyan Zhang

As multinational companies wrap up compliance preps for the EU's General Data Protection Regulation (GDPR), China's Cybersecurity Law (CSL) takes center stage presenting new challenges. Although CSL took effect on June 1, 2017, the compliance deadline for the most controversial cross-border data transfer requirement is deferred until Dec. 31, 2018. Companies deemed "network operators" are required to conduct a security assessment if they transfer personal information or important data collected or generated in China to a foreign party. While CSL's security assessment regime remains under development and the draft bears superficial resemblance to GDPR, the Chinese legislative and enforcement styles create confusion, and sometimes false hopes, for western companies. This article sheds light for in-house counsel with GDPR exposure on how to prepare for CSL's data transfer requirement.

The Data Transfer Requirements under CSL and GDPR

Article 37 of CSL initially requires that operators of critical information infrastructure (CII) store personal information and important data collected or generated in China within the territory of China, and conduct a security assessment if such data needs to be provided to a foreign party. Article 2 of the draft Measures later issued by the Cyberspace Administration of China (CAC) expanded the assessment requirement from CII operators to "network operators."

CII operators refer to companies in critical sectors such as radio, television, energy, transportation, water conservancy, finance, and others that "will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses function or encounters data leakage." The much broader category, "network operators," refers to "owners, operators, and service providers of computer networks."

Xiaoyan Zhang , Reed Smith counsel

In parallel, China's National Information Security Standardization Technical Committee (NISSTC), a standard-setting committee jointly supervised by the Standardization Administration of China (SAC) and the CAC, is preparing the security assessment Standard, which, though not legally

binding, will provide practical guidance on how to conduct security assessment. Neither the Measures nor Standard have been finalized as of today.

Article 44 of GDPR generally prohibits transfer of personal data to non-EEA recipients unless: (i) the recipient country is deemed to provide an adequate level of data protection (Article 45); (ii) data exporters adopt "appropriate safeguards" (Article 46); or (iii) a derogation applies (Article 49).

CSL and GDPR Appear to Have Different Rationales

The CSL concerns data sovereignty, national security, and the big data-driven economy. China has been an open advocate of Internet and data sovereignty and discourages excess reliance on U.S. communication infrastructure. In a 2011 submission to the United Nations, China, along with Russia and several other nations, articulated desires to claim sovereignty over its citizens' data, and the rights to censor content and protect CII from foreign threats. The 2013 Snowden revelation led China to believe that it was a victim of NSA surveillance, and the first draft of CSL was released shortly after. Today, China accounts for more than 40 percent of the world's e-commerce transactions according to the McKinsey Global Institute. Maintaining control over its data is believed to be essential to preserving China's role in the global digital economy, and to support its big data-driven economy backed up by emerging technologies such as AI.

As a result, CSL is designed with an over-reaching scope coupled with a heavy regulatory focus that places the ultimate decision-making power at the discretion of the authorities.

In contrast, GDPR focuses on protecting individual rights while balancing the need of global trade. GDPR, together with its predecessor Directive, is based on a body of human rights laws including the 1948 Human Rights Declaration. Although neither statute articulates specific rationales behind the data transfer restriction, it is obvious that the main legislative purpose is to protect EU citizens' personal information from misuse, particularly when such information leaves the EU territory.

Mindful of the OECD principles, GDPR is not oblivious, however, to the practical needs of the global economy. It carefully balances the need to protect individual rights with the necessity of cross-border data flows by providing "adequacy" alternatives. Indeed, companies have been relying, and will continue to rely, on "appropriate safeguards" and "derogations" for compliance.

The ends determine the means. CSL and GDPR thus have more differences than similarities.

Unlike GDPR, CSL Captures Non-personal Information

GDPR only concerns personal data. CSL also subjects non-personal information to transfer assessment, namely, "important data," which is defined as data "closely related to national security, economic development and public interest."

The content of "important data" is sector-specific. The revised draft Standard gives a non-exhaustive list of exemplar information that may be deemed "important" for 28 sectors. For example, information concerning business entities such as name, address, account number, and operational data generated on the e-commerce platform for e-commerce; data concerning product sales, market research, and marketing plans for finance; stats of user behaviors and business trends for telecom. Sector regulators will have the ultimate discretion to determine what constitutes "important data." Notably, "important data" covers both original data collected or generated in China as well as data derived from the original.

CSL Applies Broadly to 'Network Operators'

GDPR applies to all controllers or processors that need to transfer personal data. At first glance, CSL appears narrower in scope by only concerning "network operators." However, since "network operators" are understood in practice to capture any

companies providing services or operating business through computer networks including company intranets, the term is equivalent to the controllers or processors under GDPR in scope. This is not surprising, as data localization regulation in most jurisdictions does not typically tie to a particular set of business operators. A company, therefore, should not set aside its data transfer obligations by over-relying on the belief that it is probably not a network operator.

Companies that are not registered in China but provide product or service to consumers in China may fall under "network operators." The inquiry focuses on factors such as: (i) whether the Chinese language is used in the product or service offered; (ii) whether RMB is used as the currency for payment; and (iii) whether any logistics services are provided to consumers in China.

CSL Adopts a Two-tiered Assessment Framework

Tier one is self-assessment. Unlike GDPR, CSL mandates that network operators conduct a security self-assessment annually and under any of the following circumstances:

- If a cross-border data transfers occurs;
- If an operator of CII is transferring data across the border;
- If the nature (i.e., purpose, scope, recipient, and type) of a cross-border transfer is changed significantly, or a serious security incident has occurred;
- As required by sector regulators.

The revised draft Standard proposes that network operators establish a security self-assessment working group consisting of members from legal, policy, security, technology, and administration. The working group shall: (i) review and approve the data transfer plan prepared by the business team; (ii) conduct periodic audit of transfers; (iii) prepare a report after completing the self-assessment; and (iv) retain the report for at least two years for official inspection. If the self-assessment concludes that the desired transfer should be prohibited, remedial actions should be taken to lower the security risks of the transfer. Finally, network operators must report the self-assessment results to their sector regulator or CAC under certain circumstances, including, for example, when the quantity of data transferred within one year exceeds the threshold designated by the CAC and sector regulators.

Tier two is official assessment, which may be initiated by the CAC or sector regulators under three circumstances: (i) if data transfers receive a large of amount of complaints from users; (ii) if national industry associations deem a security assessment necessary; and (iii) other transfers deemed necessary for review by CAC or sector regulators.

Regulators are required to: (i) establish a working group to conduct the assessment by way of "remote testing" and "on-site inspection"; (ii) appoint an expert committee to review the assessment report prepared by the working group; and (iii) make a final determination upon the committee's recommendation whether the proposed data transfer shall be approved.

CSL Focuses on Risks Factors but Provides no Mechanisms for Compliance

The GDPR data transfer rule, although daunting on its surface, offers ample practical solutions for compliance. Companies may rely on any of the six "appropriate safeguards" and seven derogations. For example, binding corporate rules (BCRs) are commonly used by multinationals to transfer data to its group affiliates outside of the EEA. Standard data protection clauses are frequently used with foreign data processing vendors and other contracts. Qualified consent and the necessity of contract performance are considered acceptable derogations.

CSL, however, does not envision such practical outlets. The substantive criteria for security assessment entails an overreaching two pronged test. The first prong, whether the transfer is "lawful, legitimate, and necessary" is a threshold requirement.

Consent and emergency, for example, would render a transfer legitimate and lawful, and transfers for performing contracts would qualify as necessary.

The second prong evaluates the risks associated with the transfer by examining two elements: (i) the nature of the data being transferred including the type, quantity, scope, sensitivity, and techniques employed to desensitize the data; and (ii) the likelihood of security breaches involving the transferred data and the level of the impact of such incidents. The second "risks" element examines nearly 50 factors (some overreaching while others redundant) ranging from the data protection capabilities of the data transferor and recipient, to the legal and political environment of the recipient's country. This massive totality of circumstances test will be challenging to execute in practice absent binding precedents. Ultimately, it will remain the discretion of the CAC or sector regulators to determine whether the risks for the transfer are so grave that the request should be denied.

Despite any surface resemblances, the cross-border transfer tests under CSL and GDPR differ in at least three material ways. First, CSL envisions no affirmative mechanisms such as the BCRs and standard data protection clauses for a company to get approval. Private contract clauses are briefly addressed in connection with transferors' data protection capability, which accounts for a small subset of the entire risk factors. Second, none of the seven GDPR derogations is present in CSL. Qualified consent in the EU can legitimize a transfer, but consent in China only satisfies the first threshold "legitimacy" test. Similarly, when a transfer is necessary for the performance of a contract, it satisfies GDPR but again only meets the threshold test of "necessary" under CSL. Finally, no privacy shield equivalent is envisioned by CSL to legitimize a transfer with the U.S.

CSL Enforcement Focuses on Shutting Down Businesses and Individual Liability, not Fines

Violations of the data transfer provisions of GDPR are subject to hefty administrative fines up to EUR 20M, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The fines imposed by CSL for violation of data transfer provisions are relatively small: between RMB 50K and 500K (~USD 7,500-75K). However, companies may face shutdown of websites or revocation of business licenses in addition to the fines. Personnel directly in charge can be individually fined between RMB 10K and 100K (~USD 1,500-15K).

The Path to Compliance

Despite all the differences, the types of operations affected by GDPR and CSL are largely similar, which include, among others, global HR databases, and any global service offerings involving customers, employees, and third-party vendors. To prepare for compliance, the following similar general steps should be taken: (i) review existing and planned business operations; (ii) identify all circumstances where governed data are transferred cross-border; and (iii) ensure that for, each such transfer, the company has in place the approval that complies with the law.

For China, particular attention should be given to "important data," the book-keeping and reporting obligations of the self-assessment, and maintaining an open communication channel with the sector regulator.

Xiaoyan Zhang *is an attorney in the global IP, Tech & Data group of Reed Smith in San Francisco. She advises clients extensively on privacy and cybersecurity issues in Asia, particularly China's new Cybersecurity Law, as well as cross-border technology transactions with China.*