



GO WITH THE FLOW

Cross-border data transfer: a China perspective

Before China enacted its new Cybersecurity Law on 7th November, 2016, cross-border data transfer was largely unregulated by the government. While many Chinese laws and regulations governed the collection, use and storage (including localisation) of data, no binding laws or regulations contained generally applicable legal requirements or constraints on the transfer of data across Chinese borders. **Yan Luo** of **Covington & Burling LLP** explains the changes proposed by the law and discusses potential data transfer compliance strategies that companies can adopt to comply with the new Chinese data transfer requirements.

Cybersecurity Law: before and after

Once the Cybersecurity Law (the Law)¹ takes effect on 1st June, 2017, the regulatory landscape for cross-border data transfer will change completely: China will become another important jurisdiction to watch in the international data transfer space.

Before the Law was officially promulgated, China had already started efforts to consolidate its jurisdiction over data by imposing data localisation requirements in many industry-specific regulations.² However, there existed no comprehensive framework for regulating cross-border data flow.

A voluntary, non-binding national standard was issued in 2012 – the *Guidelines for Personal Information Protection within Public and Commercial Services Information Systems* (GB/Z 28828-2012) (*Guidelines*).³ The *Guidelines* provided that “absent express consent of the personal information subject, or explicit legal or regulatory permission, or absent the approval of the competent government agencies, the administrator of personal information shall not transfer personal information to an overseas recipient of personal information, including an individual located overseas or an organization or institution registered overseas.” The *Guidelines*, however, lack the force of law and did not gain traction in practice.

Article 37 of the Law, for the first time expressly requires that operators of Critical Information Infrastructure (CII) store within China “citizens’ personal information and important data” collected or generated in the course of operations within the country.⁴ If transfers of data offshore are necessary for operational reasons, a security assessment must be conducted by designated agencies, unless otherwise regulated by laws and regulations.⁵

The Law defines CII broadly as “infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest”. Specific reference is made to ‘key sectors’ such as telecommunications, financial services, transportation and e-government.⁶ This definition is sufficiently broad to potentially cover many sectors and industries. The Cyberspace Administration of China (CAC), the agency tasked with implementing the scheme, is expected to issue an implementing regula-

tion in the next six months to offer more guidance on the scope of CII.

Data localisation vs data transfer

The CAC indicated in press reports that to protect China’s CII, personal information of Chinese citizens and “important data” collected and generated by CII operators should in principle be stored onshore.⁷ Transferring data offshore can only be done if “absolutely necessary” and must “follow rules”.⁸ To ensure “orderly” cross-border data transfer, when deciding whether to approve a data transfer requirement, the agency will primarily consider whether at the destination, Chinese data is properly safeguarded post-transfer.⁹

The CAC is expected to issue an implementing regulation that governs the security assessment prescribed by Article 37. While awaiting the formal issuance of the implementing regulation, we examine below potential requirements for the transfer of two different groups of data: personal information of Chinese citizens and ‘important data’.

Cross-border transfer of personal information of Chinese citizens

The CAC is yet to provide any details on how it plans to evaluate whether foreign countries, organisations or individuals are “willing and capable of” safeguarding Chinese citizens’ personal information.¹⁰ There is also no indication that the CAC will, in the near future, recognise that any specific countries can afford an adequate level of protection and thus automatically allow the transfer of data to such countries.

Without recognition of other countries’ data protection regimes, the CAC is likely to devise a data transfer mechanism that relies on CII operators’ commitments or binding contractual obligations to ensure that personal information is sufficiently protected outside of China. Although there is currently a lack of specifics, it is possible that at least some elements of this mechanism will be comparable to the European Union’s (EU’s) *Model Contracts and Binding Corporate Rules* (BCR) or Asia-Pacific Economic Cooperation’s (APEC’s) *Cross Border Privacy Rules* (CBPR) system.

The CAC has also not provided any details on what contractual arrangements or company internal rules and procedures can satisfy the agency’s requirements if companies are required to robustly protect Chinese citizens’ personal information outside of China. One potential benchmark is the *Information Security*

¹ *Cybersecurity Law of the People’s Republic of China*, effective 1st June, 2017.

² Stratford, Tim & Luo, Yan, *3 Ways Cybersecurity Law In China Is About To Change*, Law360, 2nd May, 2016, <<https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-to-change>>

³ *Guidelines for Personal Information Protection within Public and Commercial Services Information Systems* (GB/Z 28828-2012), jointly released by the General Administration of Quality Supervision, Inspection, and Quarantine and the Standardization Administration of China, 5th November, 2012, effective 1st February, 2013.

⁴ Article 37 of the Law.

⁵ Data transfer requirements imposed by other laws and regulations will be ‘grandfathered’ by the Law. However, requirements imposed by department rules and local regulations are beyond the scope of this article.

⁶ Article 31 of the Law.

⁷ *CAC Is Enacting Regulations on the Evaluation of Cross Border Transfer*, New Beijing Paper, 8th December, 2016, <<http://www.bjnews.com.cn/feature/2016/12/28/428788.html?from=timeline&isappinstalled=0>>

⁸ *Ibid*

⁹ *Ibid*

¹⁰ *Ibid*

¹¹ *Information Security Technology – Personal Information Security Specification (Draft)*, National Information Security Standardization Technical Committee, 20th December, 2016, <http://www.tc260.org.cn/zjfb.jsp?norm_id=20160628214349&recode_id=21042&idea_id=20161221094921&t=0.20651056670257484>

Technology – Personal Information Security Specification (the Standard), a new national standard proposed by the CAC.¹¹ The *Standard* establishes a comprehensive data protection framework for regulating the collection, storage, use, transfer (within China) and disclosure of personal information, and adopts eight principles identical to the Organization for Economic Co-operation and Development's (OECD's) privacy principles.¹² Although not legally binding, such a national standard can provide companies with useful insight into what Chinese regulators may consider to be best practice in protecting personal information. If a company were to ensure that its handling of personal information outside of China also meets requirements articulated in the *Standard*, it could be easier to argue that the protection of Chinese citizens' personal information is adequate, wherever data is processed.

Cross-border transfer of 'important data'

Cross-border transfer of 'important data' will, however, be evaluated differently. The CAC has yet to fully define 'important data', although it is commonly understood as data relating to China's national security, which by itself is a sweeping concept under China's National Security Law.¹³

Chinese laws and regulations in two other areas could offer some clues regarding how the agencies may interpret this term, even though it is difficult to determine categorically which data falls within its scope. Any near-term assessment of the coverage of 'important data' will have to be made on a case-by-case basis.

The first law is China's Law on Guarding State Secrets (State Secrets Law).¹⁴ Under this law and its implementing regulations, 'state secrets' are prohibited from leaving China.¹⁵ The State Secrets Law offers a non-exclusive list of categories deemed 'state secrets', including, for example, information involving national defence construction and activities of the armed forces, diplomatic and foreign affairs activities, and activities related to national security investigations.¹⁶ Examples of information that the government in the past considered as 'state secrets' include certain government statistics, geographical data about infrastructure, certain law enforcement activities and certain information on natural resources.

The second set of rules relates to China's export control regime. Similar to many other countries, China maintains a system that controls the export of munitions, military products and other dual-use goods and


technologies. Transfer of data related to products and technologies that are covered by the export control regime is expected to be banned or be subject to heightened scrutiny.

Global data transfer compliance strategies: how does China fit in?

With China joining the club of countries regulating cross-border data flows, more compliance challenges lie ahead for companies that may be covered by Article 37 of the Law.

Setting aside the transfer of 'important data', which is likely to be subject to a case-by-case assessment, companies that transfer Chinese citizens' data into and out of China on a regular basis can consider taking steps to comply with the potential Chinese requirements, even though we still lack official guidance from the agencies.

For example, it is important that companies first have a good understanding of their data collection and flows into and out of China. They can then assess whether there is a need to supplement existing data protection compliance programmes in certain aspects, in anticipation of the new Chinese requirements.

Beyond China, when considering implementing a global data transfer strategy, it is also advisable to take the potential Chinese requirements into account up front. Although we cannot exclude the possibility that there may be (significant) differences between the future Chinese transfer mechanism and other regimes, such a mechanism may well share certain principles and characteristics of 'modern' data transfer regimes such as the BCR and the CBPR. Therefore, companies can potentially deploy a single, global data governance process that satisfies regulatory requirements in China and other jurisdictions at the same time. Investing in advance is likely to be a better strategy than being forced to adopt convoluted data protection policies specifically for Chinese citizens if and when transferring Chinese data for offshore processing later becomes necessary. 

For nearly 100 years, Covington has been the preeminent law firm in dealing with the US Government. In the age of globalisation, Covington has expanded internationally to meet the challenges its clients face dealing with governments and regulatory regimes in key markets around the world.

Covington's Public Policy and Governmental Affairs Group (PPGA) draws on Covington's distinctively collaborative culture and unparalleled regulatory expertise and combines it with global reach. Our policy team of more than 50 members covers the globe, with extensive networks in key cities and regions, including: Washington, D.C., London, Brussels, the Middle East, Beijing, Shanghai, Seoul, Latin America and Africa.

¹² Luo, Yan, *China Releases Seven Cybersecurity and Data Protection National Standards*, *InsidePrivacy*, 21st December, 2016, <<https://www.insideprivacy.com/international/china/china-seeks-comment-on-seven-draft-cybersecurity-and-data-privacy-national-standards/>> ¹³ National Security Law, effective 1st July, 2015.

¹⁴ Law on Guarding State Secrets, effective 1st October, 2010.

¹⁵ Article 9 of the State Secrets Law defines a 'state secret' broadly as a "matter that relates to the national security and interests as determined under statutory procedures and to which access is vested in a limited range of persons during a given period of time."

¹⁶ *Ibid*