China's new cybersecurity law effective as of 1 June 2017

May 12, 2017

On 1 June 2017, China's cybersecurity law will come into effect. As the first Chinese law focusing exclusively on cybersecurity, the law will introduce unprecedented regulation on data protection and data security practices. This includes mandatory domestic storage of data (data localisation), restrictions on cross-border data transmissions, and data security assessments that may lead to the sharing of confidential information with the Chinese authorities.

On 11 April 2017, a set of draft measures and guidelines were released, providing further insight into the practical implementation of the cybersecurity law. However, the draft measures also reveal the ongoing ambiguity of the law and possible implications. This includes unclear definitions that can be interpreted broadly, and, under the draft measures, the scope of some of the law's most far-reaching obligations appears to be much more expansive than under previous drafts of the law. Although a complete interpretation of its specific provisions remains difficult, the law could have major implications for almost all companies operating in China.

Based on the scope of the legislation, we have several recommendations, including: assessing whether your business is impacted by this new legislation; reviewing your technology and data arrangements; and considering how to comply with these new and untested requirements. We stress that this legislation could also affect companies located outside of China when data belonging or relating to those companies is in the possession of customers or suppliers with a presence in China.

Introduction

On 1 June 2017, China's cybersecurity law will come into effect. As discussed in the September 2015, August 2016 and December 2016 editions of In context, the new law introduces a framework for China's cybersecurity regime. The law can be seen against the background of the Chinese government's recent tightening of control over matters relevant to national security. Although its exact scope and implications are still relatively unclear, it is now evident that the law will impose obligations with regard to local storage of data in China (data localisation), restrictions on cross-border data transmission, and security assessments that will be conducted by companies themselves or by Chinese authorities. In addition, the law requires companies to implement compliance and governance policies relating to data protection and cybersecurity.

On 11 April 2017, the Cybersecurity Administration of China released a set of draft measures and guidelines (*Security Assessment Measures regarding the Export of Personal Information and Important Data*) which provide insight into the practical implementation of the cybersecurity law. The draft offers some guidance on several aspects of the law, but also creates more uncertainty, as it broadens the scope of specific requirements. As such, it remains uncertain how some of the more ambiguous obligations and definitions in the law will be interpreted in the future. In any case, the draft measures show that the immediate future of Chinese cybersecurity regulation for companies operating in China remains vague.

Scope: network operators and critical information infrastructure operators

The cybersecurity law imposes its most significant obligations on two categories of entities: "network operators" and operators of "critical information infrastructure." Although many had hoped that the draft measures would further clarify the definitions of these entities, this has not been the case. Although further elaboration of these definitions is expected at a later stage, some clarity has been provided, as outlined below.

Under the cybersecurity law, "network operators" are defined as "network owners, administrators or service providers". This definition leaves much room for interpretation and potentially covers any entity that uses the internet or other networks in its operations. This means that almost all companies currently operating in China would fall under its scope. Consequently, any company with a presence in China should assume that they will be subject to the corresponding obligations. These include:

- formulating internal security management systems and operating rules
- appointing designated officers responsible for network security
- adopting technological measures to prevent and mitigate computer viruses and network attacks and intrusions
- monitoring network operations and incidents and storing these records for a period of six months
- adopting measures relating to data classification, back-ups and encryption.

As for operators of "critical information infrastructures", the definition seems narrower than "network operator". The cybersecurity law states that the exact definition of "critical information infrastructures" has yet to be formulated by the State Council, but specifies several industries covered under the definition, such as "public communication and information services, power, transportation, water, finance and public services". In addition, any information infrastructure which, "if destroyed, loses function or leaks data, might seriously endanger national security, national welfare and the people's livelihood, or the public interest", also falls within the scope of the definition. As for the requirements for operators of "critical information infrastructures," as a start, they have to comply with the obligations of "network operators" as outlined above. In addition, more rigorous requirements apply, such as obligations to:

- set up specialised security management departments and conduct security background checks on responsible officers in critical positions
- periodically conduct network security education, technical training and skills evaluations for employees
- carry out disaster recovery backups of important systems and databases

- formulate emergency response plans for network security incidents, and periodically organise drills
- be subject to state security assessments by governmental authorities when purchasing products "impacting national security"
- annually engage a third party to conduct a security and risk assessment and to submit the results to the authorities
- provide network security information to authorities and "research institutions".

Data localisation

One of the most significant requirements under the cybersecurity law is the domestic storage of data (data localisation) within the People's Republic of China, which for this purpose is likely intended to exclude Hong Kong, Taiwan and Macau. Under the initial drafts of the cybersecurity law, and as previously reported by In context, the data localisation requirement was limited to operators of "critical information infrastructure" only. However, the draft measures now seem to indicate that the requirement has been extended to all "network operators." The scope of the data localisation requirement thus appears to be much wider than previously indicated and, as a result, compliance with the data localisation requirement may be imposed on virtually every company operating in China. This change might be an indicator that data localisation is now to be viewed as a more general, leading principle under the cybersecurity law and an additional important tool for the restriction of cross-border data transmission (see also next paragraph).

Regulated transmission of data and mandatory security assessments

Equally important as the data localisation requirement are the regulations imposed on cross-border transmissions of data. Under the cybersecurity law and the recent draft measures, such transmission is subject to specific self-assessment regulation and, in specific cases, a security assessment by the authorities.

The cybersecurity law distinguishes "personal information" and "important data." Under both the cybersecurity law and the draft measures, "personal information" is defined, briefly, as information that, alone or jointly with other information, can be used to identify a natural person, including a natural person's name, date of birth, identification number, personal biometric data, address and phone number. The definition of "personal information" is particularly relevant because under the draft measures, if "personal information" is to be transferred outside of China, "network operators" must notify the data subject of the purpose, scope, content, recipients and destination of the transfer and obtain consent from the personal data subject. If consent has not been obtained, personal information cannot be transmitted outside China's borders.

A definition for "important data" is not included in the cybersecurity law itself, but the draft measures define it as "data closely related to national security, economic development and public interests" and further refer to national standards and guidelines.

According to the draft measures, if "network operators" need to export any data (either "personal information" or "important data") to a place outside of China for business reasons, a security assessment must be conducted. In principle, this security assessment should be conducted by "network operators" themselves; a self-assessment. This self-assessment must consider, among other factors:

- the necessity of the data transfer
- the amount, scope, type, sensitivity and, if applicable, consent in relation to the data
- security protection measures and capability level of the receiving party, and the cybersecurity environment of the destination country or region
- the possibility of the data being disclosed, damaged, tampered with, or abused after the cross-border transfer
- risks for national security, public interest and individual legitimate interests
- other important aspects.

In addition to the self-assessment, under specific circumstances the cross-border transfer of data has to be submitted to and assessed by the competent government authority. This government assessment considers similar factors to those listed above. A government assessment is needed if the cross-border data transfer fulfils specific additional criteria, such as:

- personal information involving over 500,000 individuals
- data size exceeding 1,000 GB
- data concerning nuclear facilities, biochemistry, national defence and military, demographics and health, large-scale project activities, marine environment or sensitive geographic information
- cybersecurity information about system vulnerabilities and security protection of "critical information infrastructures"
- any data exported by an operator of "critical information infrastructures"
- other circumstances that could potentially affect national security and public interest that the authorities deem should be assessed.

Finally, the draft measures provide that certain information is not allowed to leave China under any circumstances, making this data absolutely domestic. This prohibition regards:

- personal information for which no consent has been given or which may be contrary to the interests of the relevant individual
- data which, if transferred out of China, could impact national politics, the economy, science and technology, or national defence
- data which specific government authorities have deemed cannot leave China.

Reception from international business community in China

The publication of the draft measures, and particularly the broadened scope of some of its most significant requirements, have caused the international business community in China to repeat and renew its concern about the cybersecurity law. Criticism focuses on the lack of clarity over important terms, procedures and criteria, especially with regard to data localisation

and the procedural aspects of the security assessments. With the cybersecurity legislation itself already in place, any expansion of scope through implementing rules, such as these draft measures, could bring about significant uncertainties. These uncertainties might lead to compliance risks, increase difficulties for supervision and administration, and restrict the flourishing ICT market, particularly for multinational companies with global operations but also for Chinese companies expanding abroad.

Critics further argue that compared to the EU, where EU-approved standard contractual clauses suffice for export to a country or region not providing the adequate level of data protection, the assessment mechanism proposed under the draft measures is cumbersome. Such strict requirements may jeopardise business operations. More details are needed to clarify the ambiguities both in the law and in the draft measures, with regard to: key terms (such as "network operators", "critical information infrastructures" and "important data"); the responsibilities of the relevant industry departments and regulatory authorities; the relationship between self-assessments and security assessments conducted by the authorities; potential penalties for non-compliance; the possibility of appeal against unfavourable rulings; and any retroactive implementation of the legislation.

Recommendations

As the cybersecurity law will enter into force at the beginning of June 2017, we recommend that businesses operating in China assess if and how they might be impacted by this legislation, and if any additional preparatory or mitigating measures are necessary.

As a starting point, businesses should evaluate how they could fall within the scope of the new legislation. As previously noted, definitions under the cybersecurity law are not clear and remain in flux; however, if anything, the draft measures indicate that definitions should be interpreted broadly. We believe it is prudent to assume that any company that owns or operates computer systems, data networks or websites in China falls within the scope of "network operator." We note that the potential scope of the legislation is not limited to businesses themselves, but could also extend to their customers and suppliers located in China. In that respect, companies located outside of China could also be affected when data belonging or relating to them is in possession of business partners with a China presence.

In general, we recommend that companies review and update their internal compliance policies and instruct their designated compliance and data protection departments to closely monitor the ongoing development of data and cybersecurity legislation in China. In any case, policies regarding data storage, privacy obligations and the provision of information to the authorities should be revised (or formulated, as the case may be) and implemented. As the cybersecurity law could require companies to share information with Chinese government authorities, a close inspection of potentially sensitive and confidential information located in (and potentially transferred out of) China is paramount. Companies may want to consider exporting such sensitive and confidential information outside of China before the new legislation enters into force on 1 June 2017.

More technically, we recommend that companies examine their potential exposure under the cybersecurity law. This involves closely examining the ways in which data collected and generated in China is stored and transferred outside of China through data mapping and a review of data allocation and hosting services. It is possible that, to comply with the new measures, important changes will need to be made to companies' internal IT infrastructure. Although its full implications remain to be seen, the cybersecurity law might ultimately require companies to segregate their IT infrastructure to facilitate a separate China system. This could prove difficult if servers, databases and other IT systems are currently centrally hosted or otherwise shared on a global level.

Finally, it is vital that, going forward, companies closely monitor how the law will be enforced after it takes effect on 1 June 2017. Naturally, we will also follow all relevant developments and provide updates as soon as they are available.