Policy/regulatory brief, December 2020

Three recommended priority action areas in Cybersecurity compliance

Introduction and background

As Chinese policymakers strive to strengthen China's digital economy while safeguarding national security and reinforcing China's global influence, cybersecurity has emerged at the forefront of government priorities in recent years. The Coronavirus outbreak, by forcing companies and individuals to rely on online tools, further highlighted the need for enhanced digital security.

As a result, 2020 was a crucial year for cybersecurity in China. Key regulations, such as the draft *Personal Information Protection Law* and the "*Guiding Opinions on Multi-level Protection Scheme (MLPS 2.0) and Critical Information Infrastructure Operators*", were issued this year. Not only did Chinese leaders decide on new rules: They also made sure to finally enforce existing ones. Enforcement of the Cybersecurity Law took off in 2020. Personal Information Protection enforcement experienced a similar momentum.

This increased focus on cybersecurity has repercussions. China-subsidiaries of Swiss companies that have been so far following and discussing the general CSL evolution without taking specific action, now need to review their compliance set-up. Based on Sinolytics' hands-on regulatory consulting experience, we recommend action in three priority areas: MLPS self-assessment, personal information protection, and cross-border data transfer.

MLPS 2.0 self-assessment

What is it about

- MLPS 2.0 is not completely new, but most of the implementation guidelines were issued in 2019 and 2020, and few companies have so far done the necessary adjustments to remain compliant.
- According to these regulations, all "network operators" must self-assess their MLPS level, based on the degree of harm that would happen if the network system were compromised and data leaked. The definition as "network operators" applies to virtually all companies, and large MNCs usually operate several networks and therefore need to conduct several self-assessments.
- Based on the level obtained for each network, different requirements then apply. For those above level 2, companies must get an additional expert evaluation by a certified agency and conduct a compulsory filing with local public security bureaus. Level 3 companies must comply with 189 security requirements, as opposed to 122 for level 2 companies, and only 53 for level 1 companies.

What next

- While the Chinese government has given companies some time to prepare, this window of opportunity is now closing. Based on Sinolytics' consulting practice, Public Security Bureaus have already started to reach out to IT managers in foreign companies to check MLPS 2.0 compliance.

Key compliance documentation required

- MLPS 2.0 Self-assessment

Sinolytics' advice

- *To prepare for MLPS 2.0, companies should start by identifying the different networks they operate and conducting a self-assessment according to Chinese standards. If they find themselves above level 2, they should pay extra-attention to complying with all the appropriate requirements.*

Personal information protection

What is it about

- In the last few years, China has set up a strict privacy regime very similar in scope and approach to the EU's General Data Protection Regulation (GDPR). In both, companies that collect personal data

must disclose to the user what information they collect and how it will be used. They must also obtain user consent for collecting and sharing the data, for each purpose of data processing.

- Beyond the similarities, it is the many small differences between GDPR and Chinese regulations to which companies must pay extra attention. For instance, while companies have 30 days to respond to users' data access requests under GDPR, they only have 15 days under Chinese regulations.
- All these requirements are outlined in a dozen of regulations, including the "*Personal Information Security Specification*", which took effect in 2018 and was revised in 2020. Based on Sinolytics' regulatory database, companies are required to comply with more than 500 requirements, ranging from impact assessments to managerial requirements and consent notifications.

What next

- Data protection rules are already enforced. Administrative sanctions for non-respecting these rules increased tenfold between 2018 and 2019, and more than doubled again between 2019 and 2020. Companies also started using data protection rules in lawsuits: In 2019 and 2020, several courts cited the *Personal Information Security Specification* to rule against data protection violators.
- But this is only the beginning: 2021 will likely see a ramp up of enforcement. The new draft *Personal Information Protection Law*, issued in October 2020, centralizes data protection within the Cyberspace Administration of China (CAC), giving it more law enforcement power. It also increases the negative impact in case of violation: According to the law, mishandling of personal information can lead to a fine of up to 50 million RMB or up to 5% of a firm's annual revenues.

Key compliance documentation required

- Consent notification
- Security Impact Assessment / Third-party contracts

Sinolytics' advice

- *To prepare for compliance, companies should start by identifying data they collect and process and segmenting this data into "personal" and "personal sensitive" information. They should then identify the requirements that apply to their operations in China and adjust their practices accordingly.*

Cross-border data transfer

What is it about

- Though not already enforced, cross-border data transfer requirements are likely to be particularly thorny for companies. According to Chinese regulations, companies need to conduct security self-assessments before transferring the data, even if this data is sent between entities of the same group. They must also establish contracts with data receivers, and above a certain threshold, seek approval from the local Cyberspace Administration.
- The detailed procedure varies depending on the type of data that is being sent. Two types of data will face restrictions: "Personal information" and "important data", defined as data that, if leaked, may directly affect China's national security, economic security, social stability, or public health.

What next

- None of the cross-border data transfer regulations are in force today, and there seems to be a considerable debate within the Chinese government over how strict the requirements should be. However, the most recent drafts give clear indications about future implementation. Anticipating entry into force of the rules in 2021, companies should kick-start the internal compliance process.

Key compliance documentation required

- Security Self-assessment
- Data recipients' contracts

Sinolytics' advice

- *To prepare for cross-border data transfer compliance, companies should start by creating a systematic overview of cross-border data transfer flows from China to other countries (including Hong Kong), distinguishing between personal and important data. They should write contracts with the data recipients and prepare a security self-assessment based on existing Chinese standards.*

About us

Sinolytics is European research-based consultancy entirely focused on China with offices in Berlin, Zurich, and Beijing. Sinolytics consultants analyze complex China related questions at the intersection of policy and business. The policy analysis focuses on economic, industrial, S&T, trade and social policies and is complemented by regulatory topics such as cybersecurity, social credit system or environmental regulations. Sinolytics has also been working in areas such as licensing analysis, technology transfer partnerships or VC scouting. Founded in 2017, Sinolytics has built a strong track in contributing to informed decision-making of European companies and public sector agencies based on its problem solving and strategy development capabilities. The team is interdisciplinary, cross-cultural and includes economists, public policy, law and political science/IR experts with a shared foundation of native/proficient language expertise and hands-on practical experience in the Chinese market.

Camille Boullenois
Consultant
Camille.boullenois@sinolytics.de

Tiffany Wong
Consultant
Tiffany.wong@sinolytics.de

Dr. Jost Wübbeke
Director
Jost.wubbeke@sinolytics.de

Markus Herrmann Chen
Director
Markus.herrmann@sinolytics.ch