El

New laws and regulations in China

Cyber Security and Data Security in Business with China

05.07.2021 | Author / Editor: Mareike Seeßelberg / Peter Schmitz

In the area of Cyber Security and data protection, the pressure on foreign companies operating in or doing business with China continues to increase: a flood of new laws and regulations is increasingly restricting the handling of data and further limiting the already narrow entrepreneurial room for manoeuvre.

Cyber Security and data protection legislation has become more important in China, with many new regulations and standards introduced in 2019 and 2020.

(© BirgitKorber - stock.adobe.com)

The reason for the many changes lies in the growing geopolitical tensions. China feels threatened in its national security and wants to become more independent from foreign countries. To this end, the Chinese government is not only deliberately decoupling supply chains, technologies, R&D and standards, it is also restricting data flows - both within China and across borders.

Digital technologies and data play a key role in this policy shift, which is set out in the 14th Five-Year Plan. For example, the Chinese government has established numerous data-related stimulus measures in high-tech sectors such as 5G infrastructure, data centers, promotion of digital platforms and digital currency.

This has increased the importance of Cyber Security and data protection legislation, with

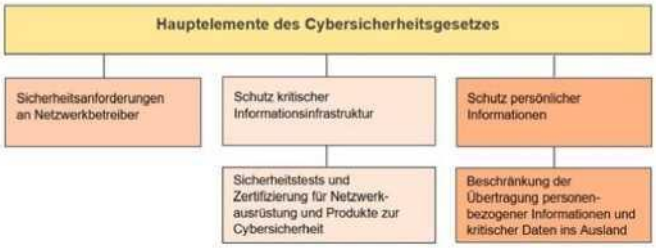
many new regulations and standards being introduced in 2019 and 2020 alone. Not all of them fit into a harmonious overall picture, as three different ministries are responsible for this complex of topics: the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). The many new regulations are correspondingly confusing for companies.

The Cyber Security Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) pose the greatest challenges. They severely restrict the handling and use of data and force companies to undergo security certification with the mandatory Multi-Level Protection Scheme 2.0 (MLPS 2.0).

Cyber Security Law (CSL)

The fundamental law for Cyber Security and data protection in China is the Cyber Security Law, which already came into force on 1 June 2017 and is now being implemented with vigour. Network operators and critical infrastructure operators are subject to a strict set of rules and are liable for non-compliance. According to this, networks are any systems of computers or other information terminals that collect, store, transmit, exchange and process information. This means that any company in China that operates a computer network or even a website is a network operator under the CSL.

In terms of content, the Act covers, among other things, the topics of personal data protection, network security, protection of critical information infrastructure, data localisation and risk assessment in the case of data transfers abroad, as well as security audits of network products and services.



The content of the Cyber Security Law (CSL) covers, among other things, personal data protection, network security, critical information infrastructure protection, data localization and risk assessment for data transfers abroad, and security auditing of network products and services.
(Image: Chinabrand)

The security check for the MLPS 2.0 certificate is divided into five steps.
(Image: Chinabrand)

Companies need to pay particular attention to personal data protection regulations, the use of network products and encryption technologies, and the implementation of MLPS 2.0.

Multi-Level Protection Scheme 2.0 (MLPS 2.0)

The MLPS 2.0 is mandatory for all businesses in China - Chinese and foreign. In doing so, the company must be certified by acompany a safety certificate issued by the local authorities. The prescribed steps for obtaining this certificate are divided into five steps. After the audit has been completed, the security audit that the own network is sufficiently protected, for example against possible unauthorized access by hackers.

First, the security level (1 - 5) of the company's relevant systems is determined: which information systems contain important data, which personal data? Are these internal systems or are there external access possibilities? The determined security level must be confirmed by the public security authority.

Subsequently, the security measures for the IT systems are adapted according to the legal requirements for the determined security level. For example, the MLPS 2.0 contains approx. 200 requirements for level 2 systems, for level 3 systems there are already approx. 310 requirements. Afterwards, a further check is carried out by a certified test centre, which issues a test report. In the final step, this report must be submitted to the public safety authority, which examines it and finally issues the safety certificate.

If an entrepreneur in China does not adhere to the requirements of the MLPS 2.0 or puts off the safety check, there is a risk of severe fines, a public blacklisting in the Corporate Social Credit System or - in serious cases - even the revocation of the business license.

Other new laws

The Encryption Law, which came into force on 1 January 2020, regulates the use and management of encryption technologies in China. In the area of commercial cryptography, there is an important change: the use of foreign encryption technologies is no longer explicitly prohibited. Commercial cryptographic products or technologies developed, used, sold, imported or exported by foreign companies are now on a par with domestic products or technologies - unless they are included in the list of critical network equipment.

The draft Data Security Law of July 2020 is also intended to increase data security in China. According to this law, data processing companies are obliged to set up a data security management system and to regularly adapt it to applicable regulations. The system must include technical and operational measures to ensure data security. Companies that process so-called important data must appoint a data protection officer and carry out regular data protection impact assessments of processing activities. The results must be reported to the responsible authority.

Explicit requirements for handling personal data are specified in the draft Personal Information Protection Law (PIPL) published in October 2020. Foreign companies must pay particular attention to the extraterritorial effects of this law and the regulations on the cross-border transfer of personal data. Once in force, the PIPL will apply not only to the handling of personal data within China, but also to certain activities outside the country. Foreign companies whose processing of personal data collected in China outside China actually or allegedly harms the interests of Chinese citizens or even endangers China's national security may be blacklisted or sanctioned. In addition, further transfer of data to that company would be restricted or completely prohibited.

Companies need to look closely

The biggest challenge currently facing European companies operating in China is the MLPS 2.0 enshrined in the CSL. Its implementation is a high priority for the Chinese government. Every company should carefully assess and register its own IT systems in order to avoid heavy fines and a negative rating in the Corporate Social Credit System. It is also essential that companies comply with the new requirements of the Cryptography Law, the Data Security Law and the Personal Information Protection Law when handling personal data.

About the author: Mareike Seeßelberg is a Senior Consultant at CHINABRAND IP CONSULTING in Munich. (ID:47469692)