VDMA Information Sheet
China's Cyber Security Law (CSL)

China's Cyber Security Law came into effect on June 1, 2017 and formulates requirements and rules for the field of cybersecurity, focusing more on the protection of personal information and standardizing the collection and usage of data. Companies should not only pay attention to data security, but also increasingly focus on protecting the privacy of individuals. In this respect, the law is quite similar to efforts made by other countries which aim to ensure network security and the protection of personal and business data. However, the law also contains numerous broad statements that use unclear phrasing, such as "sensitive data" or "critical infrastructure". Furthermore, the term "network operator" has also not yet been clearly defined. This creates uncertainties for international companies operating in China. Financial institutions active in China are therefore expecting that they will be affected by this uncertainty.

The cybersecurity law was prepared by the Central Leading Group of Cyberspace Affairs, founded in 2013, and the associated National Information Security Standardisation Technical Committee (TC 260), which will also be responsible for drafting the relevant implementation regulations or administrative regulations. The law formulates verification and security measures in the event that a company's activities fall into the categories described within the law. Generally speaking, this will have to be accompanied by the disclosure of relevant information to the local authorities, such as source codes or encryption data. The law also describes higher requirements for the protection of key information and infrastructure.

In mid-September 2017, the European Chamber of Commerce in China published their first criticism of the law, citing numerous unclear phrasings and too much room for interpretation. The letter underscores the concern that the implementation of the law could intentionally or unintentionally lead to disadvantages for international or foreign-invested companies in China. In the meantime, initial drafts of administrative regulations for cross-border data transfer have been published by the technical committee and commented on by the Europeans. From the point of view of the European Chamber of Commerce in China, the new statements do not clarify the facts. On the contrary, some additional terms have been introduced that make a clear definition of the respective terms more difficult (e.g. “sensitive information” vs. “state secret”).

Important cornerstones of the cybersecurity law

- **Network operators:** Depending on the interpretation, this may include all companies in China that use or operate data-processing systems in China. The affected companies must then fulfill certain defined standards to ensure security.

- **“Critical infrastructure”:** Affected companies must fulfill even higher requirements than network operators (e.g. security contracts with suppliers, security assessment for a part of the workforce). The definition includes any threat to the Chinese economy, national security or the “public interest”.

- **“Local data storage”:** Network operators must store all “important business data” exclusively in China in future. The export of data can only take place once a security review has been successfully passed. Furthermore, encryption technology can only be used after approval/certification by the authorities.

Impact on the German mechanical engineering sector

The newly presented provisions can, depending on the interpretation of the law, potentially impede imports and close off the market. There is also the possibility that monitoring and maintenance processes may not be organized outside China in the future. Data exchange with entities outside of China may also be restricted or prohibited. Necessary data localization will cause higher costs. The protection of intellectual property could also be undermined. Electronic supply parts subject to authorization may need to be exclusively procured on the domestic market. Many provisions in the new law leave room for interpretation that can theoretically be applied to foreign companies. This will make the business environment in China more uncertain.

For the German capital goods industry, the obligation to save or store data generated in China exclusively in China could trigger additional investment in their Chinese business activities. In addition, there is the potential risk of an inadvertent drain on know-how as a result of the safety approvals or correspondingly mandated certifications.

China is aiming to become a key and technologically sophisticated player on the international markets by 2025 and to implement this position with its own, domestically produced innovations. In an environment where state-owned companies and the state itself still have a very large influence on economic activities, this could open the door to an involuntary transfer of know-how.

The urge of the Chinese administration to regulate the Internet in order to safeguard national interests and Internet security remains unabated. In this context, it was reported in the summer of 2017 that the authorities were actively approaching telecommunications providers (e.g. China Telecom, China Mobile) and obtaining information on who uses these services. So far, there are no restrictions on the use of VPN connections. However, it must be expected that only licensed domestic providers will be used on the Chinese market in the future. This could force medium-sized German mechanical engineering companies operating in China to research alternative solutions and adopt further measures to ensure the confidentiality of data communication.

Important questions for companies operating in China

- Possible impacts as “network provider”?
- Do our own products/services fall under “critical infrastructure”?
- Are any products from my supply chain potentially affected?
- Is the data generated in China currently stored in China?
- Is cross-border data traffic necessary as part of the business model?
- If so, how can this be secured in the future (e.g. through (licensed) VPN connections)?
- What is the risk potential for an involuntary knowledge transfers?
- What investments must be made to meet the requirements?
- Is the current IT system compatible?

VDMA, together with its Chinese offices in Beijing and Shanghai, will closely monitor further developments and inform its members accordingly should additional information be gained or new information be published by the authorities. The following VDMA specialists have been involved in this issue due to the various aspects and the possible diverse impacts in the fields of market access, standardization and data protection or security.

An English translation is attached to this leaflet.

Dated: November 24, 2017

Contacts:

Oliver Wack
VDMA Foreign Trade
East Asia Unit
Phone: +49 69 6603-1444
Fax: +49 69 6603-2444
Email: oliver.wack@vdma.org

Steffen Zimmermann
VDMA Product and Know-How Protection
Data Security
Phone: +49 69 6603-1978
Fax: +49 69 6603-2438
Email: steffen.zimmermann@vdma.org

Hermann Wegner
VDMA Technology, Environment and Sustainability
Technical Market Access
Phone: +49 69 6603-1899
Fax: +49 69 6603-2899
Email: hermann.wegner@vdma.org

Daniel van Geerenstein
VDMA Legal Department
Phone: +49 69 6603-1359
Fax: +49 69 6603-2359
Email: daniel.vangeerenstein@vdma.org