Cybersecurity and Data Protection: What matters when doing business with and in China

15.10.2021 The Chinese government is making it more difficult to do business in and with China with new laws on Cyber Security (MLPS 2.0), data protection and international data transfer. The most important laws, case studies and checklists for doing business in and with China.

Pict: skeeze / Pixabay

1. The current situation

More and more countries are trying to retain sovereignty over domestically generated data and protect it outside the country. China plays a prominent role in this. The country, which is important for the German economy, is restricting the processing of data and cross-border data traffic with several new laws. In addition to the protection of data, they also deal with the security of internal company IT systems and IT management. The regulations limit the handling of data and pose completely new risks for Western companies doing business in China, which must be identified, evaluated and minimized as part of IT compliance.

2. Specificities of the Chinese data protection regime

In China, the Cybersecurity Law (CSL) , the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) are the most important. Information Protection Law (PIPL) ⅼ are decisive for data protection. The basis for all data protection measures from the above-mentioned laws is the Multi-Level Protection Scheme (MLPS 2.0), which obliges all companies registered in China to have their IT systems security certified by the local authorities.

What is striking about the new laws is that, unlike what we know from the GDPR, they deal not only with the protection of personal data, but also so-called important data. Important data is data collected or generated in China that is not a state secret, but is closely related to national security, economic development and public interest and puts them at risk in the event of leakage, loss, misuse, falsification or deletion. While the categories of data that specifically fall under important data have not yet been clearly defined by law, many will include the economic
development and the public interest. The publication of official definitions is expected later this year.

Relevant data protection authorities in China

Three different authorities are responsible for data security, data protection and cybersecurity: the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). The implementation and enforcement of the regulations are handled by the local offices of the ministries, mainly the public security authorities and the local cyberspace administrations.

In the area of personal data protection, there are also some relevant specifics that need to be taken into account. It is not possible to simply transfer a GDPR-compliant data protection system to China. Adjustments must be made in order to make the system legally compliant in China.

A relevant difference is, for example, the legal basis for processing personal data. While the GDPR mentions a legitimate interest in data processing as a legal basis, the PIPL does not recognise legitimate interest as a legal basis for data processing.
Data processing operations in international companies therefore require a different legal basis in China - for example, the consent of individuals, a contract or compliance with legal regulations as a permissible basis for data processing.

3. Different regional requirements

China has strengthened the preventive mechanisms for data security as well as its control. The Data Security Law stipulates that a categorization of data into different groups with different security measures must take place. In addition to important and personal data, there will be other categories of data depending on the region and also industry. The Chinese legislator plans to give the competence and obligation to create corresponding lists for the categorization of data to the provinces or to associations of certain industries.

Additional categories will be added to the categories of data that were previously relevant for companies (for example, confidential, for inspection, personal, public, etc.). It is expected that the responsible authorities will publish corresponding regulations on data categorisation by the time the DSL comes into force on 1 September 2021. This means that for companies that have multiple branches in China, different regulations may apply to their data in different provinces.

4. Cross-border data traffic

The laws already in force restrict the cross-border data traffic of critical information infrastructure operators (CIIOs). Personal and important data are affected. However, there are already draft regulations that extend the restrictions on data transfers from CIIOs to all companies.

Example of the automotive industry: On May 12, 2021, the Cyberspace Administration China issued a draft to regulate data protection in the automotive industry. This is a first draft to regulate the handling of personal and important data by the automotive industry. It defines for the industry what constitutes important data and limits its processing to a necessary minimum. As far as possible, the important data should be processed in the car and not transferred. The processing of sensitive personal data will be prohibited, with a few exceptions. The transfer of data abroad will only be possible after a security check by the CAC and under further security conditions. The general rule is that data must be stored in China. Further regulations for other industries will follow soon.

When this comes into force, companies must adapt their data flows at short notice, obtain the relevant approvals for data transfer, prepare impact risk assessments and document their data transfers. The risk of violating regulations in the process can be minimized by a data management system introduced at an early stage, which makes it possible to flexibly control and document data flows. This allows a company to react promptly to changes in legal requirements.

Companies should find out at an early stage which local authorities are responsible for authorisations and whether they process and transfer categories of data for which an authorisation might be necessary before the cross-border data transfer. At the same time, a documented risk assessment system should be implemented that complies with the legal requirements.
The documentation of the data flows should be uniform and clear. It is particularly relevant here to specify the type of data processed and transferred on the basis of the specified data categories, so that in the event of an official inspection, complete tracking of the data processing activities is possible.

5. Multi-level Protection Scheme

There is an urgent need to implement the Multi-Level Protection Scheme (MLPS) for in-house IT systems as required by law (webinar on implementing MLPS 2.0: https://www.youtube.com/watch? v=5BaZkfkvAb8). Companies that fail to have their systems certified by the authorities risk a hefty fine and public display (blacklisting) on the Corporate Social Credit System (CSCS) (https://www.creditchina.gov.cn/), resulting in sanctions. The MLPS assigns a security level to each IT system, which then determines what measures are legally required to be taken to ensure system security. The adaptation of IT security measures (hardware, software and IT management) to the level required by the MLPS is mandatory, and the implementation of the MLPS is audited by the Public Security Authority.

Auditing of businesses for MLPS implementation is gaining momentum. In some cities, the CAC has already checked local companies for security gaps with penetration tests. If data protection-relevant gaps are found by the CAC, the companies concerned will be admonished and will have to remedy the corresponding security gap in a timely manner. Fines can also be imposed.

Case study: IT compliance project

An international group with a branch office in Shanghai for manufacturing and customer service on the Chinese market uses uniform company software throughout the group to manage its diverse data. The data of the Chinese subsidiary has so far been transferred to a server in Germany and also stored and processed in Germany. This includes production data, sales figures, project information and sales information as well as personal data such as customer and employee data. The Chinese production lines are equipped with sensors that permanently record operating data.

[18].w. [21]and sent to the German headquarters via a digital twin for the purpose of predictive maintenance.[11:41]
become

In a first step, all of the branch's data collected and processed in China was classified according to industry and province into the categories a) personal data, b) sensitive personal data, c) important data and d) other data categories. In order to be able to adapt the internal procedural rules in a timely manner, an external service provider was commissioned to continuously monitor the current Chinese legislation.
Since the rules of the GDPR are not sufficient in the Chinese market, the already implemented data protection processes and measures that are applied to the processing of personal data were adapted to the Chinese data protection law. In doing so, particular attention was paid to the company's information obligations.

The next step was to check the permissibility of data transfer abroad. For this purpose, it was checked which data of the company are important in the sense of the law and therefore may only be stored in China and for which data an approval must be obtained. For selected data, the storage obligations China were reviewed. It was important to answer the question of whether foreign partners to whom data is transferred meet the standards of Chinese data protection.

In order to be able to flexibly control and document the company's data flows and thus meet the strict documentation requirements, a new flexible data processing system was set up. In this context, risk impact assessments were also prepared for data transfers, which can currently still be carried out freely. Experienced experts from a local testing centre, with whom personal contacts already existed, were used to implement the MLPS certification. Thanks to the good connection to the testing authority, a smooth process could be ensured.

Checklist: Risks of missing IT compliance

- Lack of employee awareness in China leaves security vulnerabilities in the dark.
- Detection of vulnerabilities through pentesting by local authorities.
- High fines for lack of or poor implementation of data protection regulations, especially in the case of data leaks.
- Threat of entry (blacklisting) in the Corporate Social Credit System, damage to reputation.
- Temporary interruption of business operations.
- In extreme cases, revocation of the business license.
- Stop all data transfers abroad if unauthorised cross-border data transfers are detected.
- Use of hardware and software not permitted in China

6. Recommendations for action

IT compliance is now essential in China. The first step should be to implement the MLPS and adjust the security measures of the relevant IT systems. Only in this way can companies show the authorities that they are already in the process of meeting the new legal requirements for cyber and data security.

In addition, a flexible data management system should be set up or existing systems should be reviewed and, if necessary, adapted. If the company has several branches in China, different data categories must be created regionally and these must be managed separately. Since there will be different categories, flexible handling is necessary in data management. When exporting data, documentation requirements and risk assessments, there will be restrictions that need to be taken into account.

Companies must also ensure that they are promptly informed about the current status of rapidly changing legislation. Many of the relevant regulations and standards are only available in Chinese, so the current status of legislation should be provided by a Chinese employee or Chinese-speaking lawyer.

In addition to the IT compliance requirements brought about by tighter data protection in China, companies should also consider which data needs to be collected in China and which needs to be transferred to or from China across borders. What data flows are mandatory and how can they be guaranteed to flow in compliance with the law and without interruption? Although there are significant restrictions on data traffic, professional IT compliance will enable German companies to avoid major risks and disruptions in their business with China.

Mareike SeeßelbergO is a Senior Consultant, Zihao LiaoO is a Consultant at Chinabrand IP Consulting |$|.
(Authors: Sebastian Halm , Mareike Seeßelberg , Zihao Liao)

More articles on this topic:

China turns off the juice to Bitcoin miners ► (21.06.2021)
Pioneer market livestream shoppingpping: What online retailers can learn from China ► Q (30.03.2021)

Selected agencies and service providers in this field:

Display

websedit
web solutions

unitb consulting
As a digital agency, we work for well-known clients (e.g. Burda, BVG, Funke, HDI, RBB, ZDF), but also fascinating startups. We advise, design and implement complex projects on the internet and intranet.

Referred to in this post:

Persons: Zihao Liao Mareike Seeßelberg
Companies / Sites: china-briefing.com chinabrand.de gov.cn newamerica.org stanford.edu youtube.com
Tags: china data protection data security

Trackbacks / Comments

Trackback URL ► Permalink►

Write your opinion, experiences, suggestions with or about this topic. Your post will appear in this space. Your comment: ►

All g15.10.2021