CHINA 華牌 BRAND®

CYBER AND DATA SECURITY IN CHINA

New Laws and Recommendations for Action

Dr. Hans Joachim Fuchs, Mareike Seeßelberg, Zihao Liao

CHINABRAND IP CONSULTING GMBH

Grashofstrasse 3 ▪ 80995 DE-Munich ▪ +49 89 32 12 12 800

info@chinabrand.de ▪ www.chinabrand.de

Grashofstraße 3, DE-80995 Munich

+49 89 321212800

www.chinabrand.de

Table of Content

Overview of New Laws and Regulations

The People's Republic of China feels threatened in its national security. Growing tensions between the U.S. and the country of the rising sun have resulted in the Asian nation's accelerated decoupling from the West, which is also the case for Europe. China, like the U.S., is deliberately decoupling not only supply chains and technologies, but also cross-border data flows, research, regulatory standards and the freedom of movement.

The political strategy aims to nationalize and comprehensively upgrade Chinese industry, to strengthen the domestic economy (domestic circle), reduce the market share of foreign companies or to drive them out of the Chinese market altogether. The Made in China 2025 strategic plan, although no longer prominently communicated, is still in effect and is now being vigorously implemented by various authorities as part of the *new Guiding Opinions on Expanding Investment in Strategic Emerging Industries*.

Digital technologies and data play a prominent role in this strategy. The Chinese government has established numerous data-related stimulus measures in high-tech sectors such as 5G infrastructure, data centers, the promotion of digital platforms and a digital currency. These actions are serving as market drivers in the various affected industries.

Increased policy activity is leading to higher regulatory dynamics that are now challenging foreign companies in China. On the one hand, they are forced to monitor economic policy and regulatory developments relevant to their business in a timely manner and to adapt their compliance activities. On the other hand, these companies must also rethink and, if necessary, adapt their business models and strategies for the Chinese market. Since the enactment of the Cybersecurity Law (CSL) in China on June 1, 2017, as a basis not only for cybersecurity but also for data protection, China's legislative activity on these two topics has steadily increased. Especially 2019 and 2020 have brought a flood of new regulations and standards.

However, not all of these regulations fit together harmoniously. This is primarily since it is a patchwork of regulations, ordinances and standards from various ministries and regional and national authorities. Three ministries are simultaneously responsible for cybersecurity in China: the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS).

Increased political and legislative activity in the areas of cyber security and data protection is challenging foreign companies as well as Chinese companies. Considering the potential for high penalties, compliance with the regulations should be given a high priority.

Also, Individuals now have the possibility to take civil action against data protection violations affecting them. This new possibility is based on the new PRC Civil Code, which came into effect on January 1, 2021, and an interpretation by the Supreme People's Court. For companies, this implies that they must no longer expect only fines but also claims for damages in the event of data protection violations.

Many of the regulations already mentioned above contain provisions that lead to a specific need for action on the part of companies operating in China. The *Multi-Level Protection Scheme 2.0 (MLPS 2.0)*, which will be discussed in more detail below, is particularly worth mentioning in this context. However, regulations on encryption technologies are also relevant for foreign companies operating in China.

The implications of the *Data Security Law (DSL)* and the *Personal Information Protection Law (PIPL)* should not be overlooked either. While both laws are not effective yet, the DSL will come into force on September 1, 2021 and the PIPL also is expected to come into legal effect before year-end 2021. These two laws (especially the PIPL) contain comparatively similar regulations to the GDPR on the protection of personal data, which are regulations that could restrict the transfer of data abroad.

Overview of the most important laws, regulations and standards in the PRC:

Applicable Laws, Regulations and Standards			
Name	**Level**	**In Effect Since**	**Relevant Articles**
Criminal Law	Law	4.11.2017	Article 253(1) [1]
General Rules of the Civil Law	Law	1.10.2017	Article 111 [2]
Civil Code	Law	1.1.2021	Article 111, 134 ff.
State Security Law	Law	1.7.2015	Article 25 [3]
Cybersecurity Law	Law	1.6.2017	Article 37 [4]
Data Security Law	Law	1.09.2021	Complete
Encryption Law	Law	1.1.2020	Complete
Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection	Law	28.12.2012	Article 2, Article 3 [5]

[1] Article 253(1) When persons sell or provide personal information of citizens to others in violation of relevant national provisions, and the circumstances are serious, the sentence can be fixed-term imprisonment of no more than 3 years or criminal detention, in combination of fines, or the sentence can be fines alone; if the circumstances are particularly serious, the sentence shall be fixed-term imprisonment from 3 to 7 years, in combination of fines.

[2] Article 111 Natural persons' personal information shall be protected by law. Any organizations and individuals who need to obtain personal information of others shall obtain the information according to law and shall ensure the information safety. It is not allowed to illegally collect, use, process or transfer the personal information of others. It is illegal to buy and sell, supply or publish the personal information of others.

[3] Article 25 The State shall develop network and information security assurance system, enhance network and information security assurance capabilities, strengthen innovative research and development and application of network and information technologies and realize the security and controllability of network and information core technologies, critical infrastructure and information systems and data in key areas; the State shall also enhance network management, prevent, deter and punish network criminal acts such as cyber-attacks, network intrusion, network theft and illegal spread of harmful information in order to safeguard the sovereignty, security and development interests of the state cyberspace.

[4] Article 37 The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail.

[5] Article 2 Network service providers and other enterprises and public institutions that collect or use citizens' personal electronic information in the their business activities shall follow the principles of lawfulness, reasonableness and necessity, explicitly state the purpose, method and scope of collection and use of the information, obtain the consent of the one whose information is collected, and shall not collect or use information in a manner that violates the provisions of laws and regulations, or the agreement of the parties. Network information providers and other enterprises and public institutions that collect or use citizens' personal electronic information shall make in public their rules for the collection and use. Article 3 Network service providers and other enterprises, public institutions and their employees must strictly keep confidential of citizens' personal electronic information collected during their business activities and may not disclose, falsify, damage, sell or illegally provide such information to others.

Provisions on Protecting the Personal Information of Telecommunications and Internet Users [6]	Departmental Rule	1.9.2013	Complete
Provisions on the Cyber Protection of Children's Personal Information [7]	Departmental Rule	1.10.2019	Complete
Guidelines for Internet Personal Information Security Protection [8]	Departmental regulatory document	10.4.2019	Complete
Information Security Technology—Guideline for Personal Information Protection within Information System for Public and Commercial Services (GB/Z 28828-2012)	National technical guide	1.2.2013	Complete
Information Security Technology—Personal Information Security Specification (GB/T 35273—2017)	Voluntary Standard	1.10.2020	Complete
Information Security Technology—Baseline for Classified Protection of Cybersecurity (GB / T 22239-2019)	Voluntary Standard	1.12.2019	Complete
Information Security Technology—Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB / T 25070-2019)	Voluntary Standard	1.12.2019	Complete
Information Security Technology—Evaluation Requirements for Classified Protection of Cybersecurity (GB / T 28448-2019)	Voluntary Standard	1.12.2019	Complete
Entwürfe			
Name	**Level**	**Date of Release**	**Relevant Articles**
Personal Information Protection Law	Law	21.10.2020	Complete
Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment)	Departmental regulatory document	11.4.2017	Complete
Administrative Measures on Data Security (Draft for Comment)	Departmental regulatory document	28.5.2019	Complete

6 Decree of the Ministry of Industry and Information Technology No. 24

7 Order of the Cyberspace Administration of China No.4

8 Issued by the Ministry of Public Security and Beijing Internet Industry Association

Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment)	Departmental regulatory document	13.6.2019	Complete
Regulations on the Multi-Level Protection Scheme for Cybersecurity (Draft for Comment)	Departmental Rule	27.6.2018	Complete
Measures for Cybersecurity Review	Departmental Rule	21.5.2019	Complete
Implementation Opinions on Carrying out the Testing and certification Work of Commercial Cryptographic Products (Draft for Comment)	Departmental Rule	20.2.2020	Complete
Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment)	National Standard	30.8.2017	Complete
Information Security Technology - Security Impact Assessment Guide of Personal Information (Draft for Comment)	National Standard	11.6.2018	Complete
Information Security Technology - Guidelines for Personal Information Notices and Consent (Draft for Comment)	National Standard	20.1.2020	Complete

Individual relevant laws and regulations are discussed in more detail below. The aim of this white paper is to enable companies to assess how they are affected by relevant laws in the area of cyber security and data protection and to outline the further procedure required for compliance. The focus is primarily on regulations that affect companies which are not operators of critical infrastructure.

The white paper is based on currently available laws and regulations as well as draft laws, regulations related to cyber security and data protection which have not yet come into effect.

Cyber Security Law (CSL)

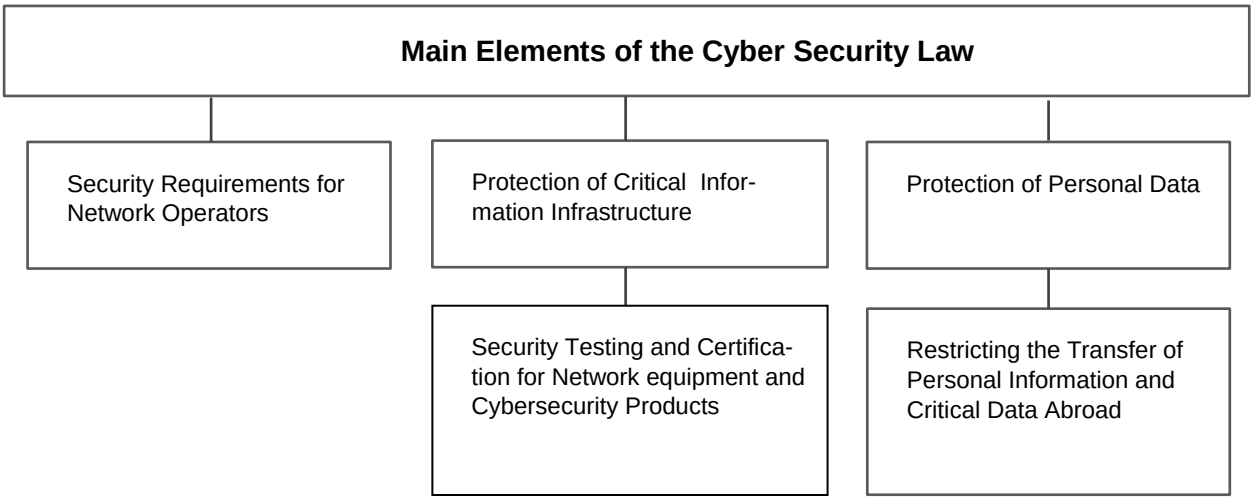
The *Cyber Security Law of the People's Republic of China (CSL)* is the basis for China's current legislation on network security and data protection.

The law provides strict regulations and liability for so-called "network operators" and even stricter regulations for those organizations operating so-called "critical infrastructure." "Network operators" are owners, operators, and users of a network, as well as network service providers. A "network" is defined as a system consisting of computers or other information terminals and related equipment that collects, stores, transmits, exchanges and processes information according to certain rules and procedures. This means that any company in China that operates a computer network or even a website is a network operator as defined above.

According to the *CSL*, operators of critical information infrastructure are primarily organizations in the transportation, energy, and financial sectors, as well as in the areas of public communications and information, hydraulic engineering, and e-governance. Furthermore, all organizations with information systems that are likely to have serious consequences for the state and public safety in the event of a disruption are also operators of critical information infrastructure. The Council of State is responsible for determining which organizations are affected. A further specification of the definition of CIIOs can be found in the Regulation for the Security Protection of Critical Information Infrastructure (draft). All of the above definitions must always be considered in the context of other relevant regulations on cybersecurity and data protection. In the latter, further elaborations on the definitions can be found in many cases.

Along with other subject areas, the *CSL* covers the topics of personal data protection, network security, protection of critical information infrastructure, data localization, risk assessment for data transfers abroad, and security auditing of network products and services.

The main elements of the Cyber Security Law can be outlined as followed:



The CSL is the basic framework for the subsequent regulations, which concretize the rather general requirements of the CSL and thereby make them implementable.

The most important regulations for companies are the:

- Multi-Level Protection Scheme
- Protection of Personal Data
- Use of Network Products and
- Encryption Technologies

Generally, a distinction can be made between regulations on data protection and regulations on network security in the CSL.

Data Protection

The *CSL* contains a number of regulations relating to the collection, storage and processing of personal information. It also regulates the transfer of critical data and personal information abroad. The term "personal information" refers to various information, in electronic or other form, about a natural person that, alone or in combination with other information, enables the identification of the individual, such as the name, date of birth, ID number, biometric information, address, telephone numbers and e-mail addresses.

The applicable *voluntary standard Personal Information Security Specification* further defines the term "sensitive personal information" as information that, if disclosed, would compromise the individual's security, damage the individual's reputation, or result in discriminatory treatment - for example, ID numbers, personal biometric information, bank accounts, communications credentials, property information, and credit information.

Other relevant terms defined by the Specification are "subject of personal data," the natural person who can be identified by the relevant personal data, and "data controller," the organization or individual that controls the relevant personal data and determines the purpose and nature of the data processing.

The protection of personal data, as regulated by the *CSL*, the *Civil Code* and other regulations, is subject to the following basic principles, which are similar to the *GDPR* in many respects:

- Integrity and Confidentiality
- Good Faith
- Transparency
- Purpose Limitation
- Data Minimization
- Accuracy

Data subjects in China, similar to the *GDPR,* have the right to be informed about the data collection as well as the nature of the data processing, the right to query the data stored about them, to correct errors, to request the deletion of the data, and the right to refuse the processing of the data.

In the event of violations of data privacy regulations by network operators, the responsible authorities can demand that companies remedy security vulnerabilities, confiscate illegal revenues, and impose fines.

Private individuals can take civil action against data protection violations and claim damages. The misuse or illegal sale of data is also relevant under criminal law: since the last amendment to the Criminal Code, the active sale or offering of collected personal data can be punished with a prison sentence of up to seven years. Companies can also be perpetrators, and the responsible person in the company is liable accordingly.

The *CSL* also addresses the issue of transferring data outside of China. However, the *CSL* only restricts the transfer of certain important and personal data by operators of *CIIOs*. Critical information infrastructure operators are not allowed to transfer personal information or important data collected in China to servers or to recipients overseas without prior security inspection by Chinese authorities. For the definition of important data, please refer to the *Guideline for Identifying Important Data*, found in the Appendix of the Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comment) standard, which includes, in addition to a definition, a list of examples of important data, as well as guidance on how to identify important data. According to this standard, critical data is data collected or generated in China by companies, organizations or individuals that is not a state secret but is closely related to national security, economic development and the public interest, and which may lead to the consequences listed below in the event of leakage, loss, misuse, falsification or deletion, or after combination, integration or further analysis:

1. Threat to national security, defense interests, and international relations;
2. Violation of state property, public interests and legal interests of private persons;
3. Impact on national prevention and action against economic and military spies, political influence, and organized crime;
4. Impact on legal prosecution of illegal behavior by authorities;
5. Interference with the lawful conduct of surveillance, management, inspection, and verification by government departments and obstruction of government departments in the performance of their duties;
6. Compromising the security of basic infrastructure, critical information infrastructure, or government information systems;
7. Impact on or threat to economic order or financial security;
8. Possibility of exploitation and analysis of state secrets or sensitive information;
9. Impact on or endangerment of national politics, territory, military affairs, business, culture, society, science, information, economics, resources, nuclear facilities, and other matters of national security.

The *Measures for Security Assessment for Cross-Border Transfer of Personal Data and Important Data (Draft)* also defines important data as: Data closely related to national security, economic development, and the public interests of society.

For example, documents related to a company's energy security systems would fall under the definition of important data. But the vast amounts of data Alibaba has collected, of which not all is personally identifiable, also would fall into this category. However, none of the above documents are officially valid. They therefore serve more as guidance as long as no legally effective definition exists.

Depending on further implementing regulations to the *CSL*, or further legislation, the restriction of transferring data abroad could also apply to simple network operators in the near future. Such restrictions would be a major obstacle for foreign companies, as the transfer of personal data to the headquarters of the company is a standard in many industries and the transfer of data across borders is an integral part of everyday business. For more details on the current developments in the field of data transfer, please refer to the chapters on *DSL* and *PIPL*.

At the moment, there is no centralized authority to oversee the implementation of the *CSL* regulations. Involved authorities include the Cyberspace Administration China (CAC), the Ministry of Industry and Information Technology, and the Public Security Bureau.

Companies should inform themselves about which regulations apply to themselves and whether their current data protection system complies with the legal requirements. If this is not the case, the systems must be adapted in a timely manner.

Network Security

The *CSL* includes basic network security regulations. There are regulations for operators of CIIOs and manufacturers of cybersecurity-related products to distribute, or acquire, network equipment, cybersecurity products, and services. Since the enactment of the law, critical network equipment and cybersecurity-related products must be certified by qualified entities prior to distribution.

Further, critical information infrastructure operators purchasing network products and services must undergo security screening.

The certification of cybersecurity products and services, in particular, but also the security review, is a concern for foreign companies. There is a fear that source codes of computer programs will have to be released, i.e., IP-protected material. The worry regarding IP theft is therefore considerably high.

Whether this fear is justified remains to be seen. In any case, cooperation with the Chinese authorities in the event of a security investigation is important in order to avoid negative consequences for the company. The *cryptography law* is also relevant in this area and will be discussed in a later chapter.

Since mid-2018, companies have increasingly been audited for their compliance to cybersecurity regulations and fined accordingly, mostly after systems were hacked and data was leaked. In 2018, the Provisions on Internet Security Supervision and Inspection by Public Security Organs came into effect, allowing Public Security Bureaus (PSBs) to inspect companies for their *CSL* compliance in the future. Inspections can be carried out both on-site and remotely - i.e. via the Internet. For example, PSB will check whether a data protection officer has been appointed, whether suitable technical protection measures are in place, whether data is being passed on illegally, and whether IT systems are safe from attack. This gives the PSB potential access to a large amount of highly sensitive company data. The requirement to submit information for sampling significantly increases the risk of a security breach or information loss for companies.

Another relevant part of the network security regulations is the *Multi-Level Protection Scheme (MLPS).* This is not a separate law, but rather a part of the *CSL* that is specified by additional regulations and has been increasingly enforced in recent years. In the following chapter, we will give more information on the *MLPS*.

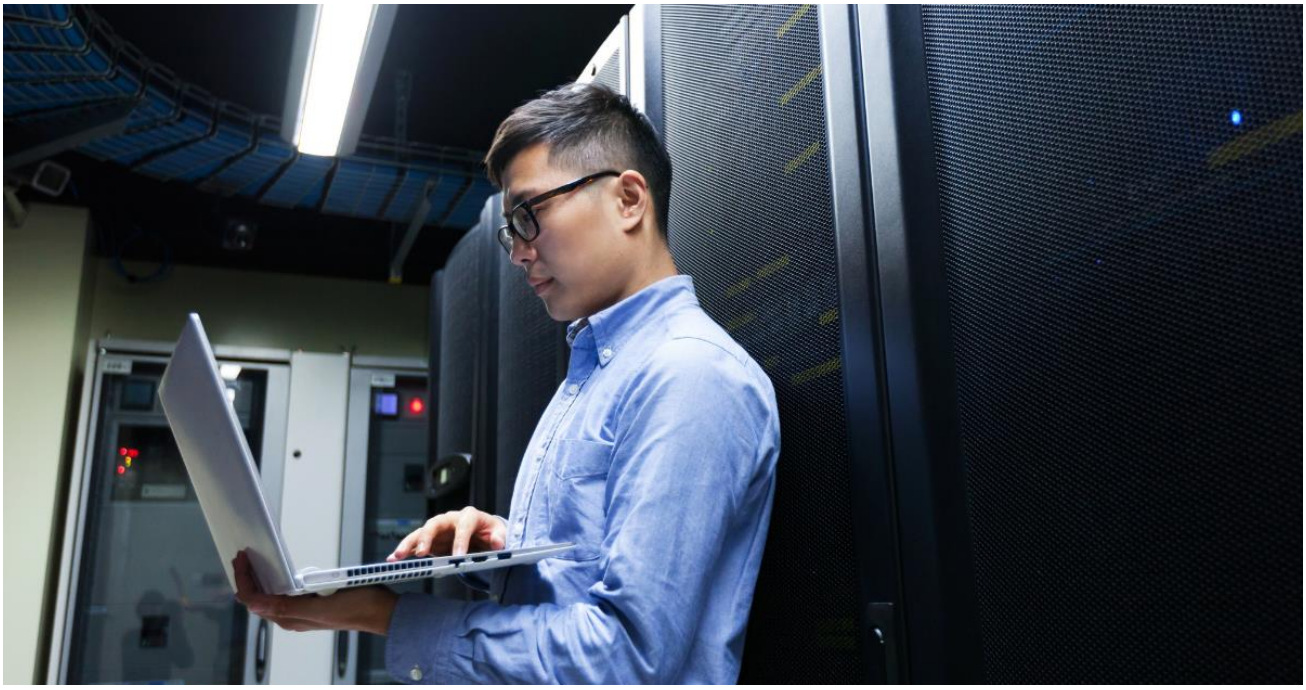
Multi-Level Protection Scheme (MLPS 2.0)

The Multi-Level Protection Scheme 2.0 (MLPS), based on Art. 21 CSL, has been enforced since 2019. The regulatory system for data and cyber security stipulates that all companies must ensure that their network is free from interference, damage or unauthorized access, and that no data can be disclosed, stolen or falsified, according to the specifications of a multi-level protection system. The scope of the mandatory MLPS 2.0 is broad and, similar to the CSL, covers virtually all companies operating in China.

National standards were issued in May 2019 to promote implementation of the MLPS through more detailed technical requirements:

- *Basic Requirements for Multi-level Cybersecurity Protection* (GB / T 22239-2019)
- *Information Security Technology - Security Design Technical Requirements for Classified Cybersecurity Protection* (GB / T 25070-2019)
- *Information Security Technology - Assessment Requirements for Classified Cybersecurity Protection* (GB / T 28448-2019).

These key standards define the MLPS. Through these standards, companies, or network operators, network security companies and network security service providers, can implement all the steps of the MLPS. The MLPS primarily evaluates the technical aspects of network security as well as security management, such as management of security personnel, internal policies and procedures, system setup and maintenance.



The MLPS 2.0 distinguishes between 5 security levels for IT systems, from risk level 1, low, to risk level 5, very high. In a first step, companies must perform an approximate assessment of the risk level of the IT systems they use on the basis of the defined requirements catalog. Those IT systems of a company that achieve a classification of level 2 or higher in this preliminary assessment must

be checked by a qualified and certified expert and the risk level must be verified. The security levels of the individual IT systems then need to be filed with the public safety authority.

The next step is to go through the catalogs of requirements for the security of IT systems at specific risk levels and identify whether the IT systems already meet the required security level or whether adjustments need to be made. For systems of the second security level there are about 200 requirements, for systems of level 3 there are about 310 and for systems of level 4 there are 340 requirements that have to be considered.

8.1.4.8	Requirements: GB / T 22239-2019	Evaluation: GB / T 28448-2019
8.1.4.8.a	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据，重要业务数据和重要个人信息等 Cryptographic techniques should be used to ensure the confidentiality of important data during transmission, including but not limited to identification data, important business data and important personal information.	测评对象:业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等 测评实施包括以下内容: 1) 应核查系统设计文档,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性 2) 应通过嗅探等方式抓取传输过程中的数据包,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理 Object of evaluation: business applications, database management systems, middleware and system management software and system design documentation Evaluation implentation include: 1) Verification of system design documents, identification of data, important business data and important personal information, and whether cryptography is used to ensure confidentiality during transmission 2) Capturing packets in transit by sniffing and other methods to identify whether data, important business data and important personal information are encrypted in transit
8.1.4.8.b	应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据，重要业务数据和重要个人信息等 Cryptographic techniques should be used to ensure the confidentiality of important data during storage, including but not limited to identification data, important business data and important personal information.	测评对象:业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备中的重要配置数据 测评实施包括以下内容: 1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 3) 应测试验证是否对指定的数据进行加密处理 Object of evaluation: business applications, database management systems, middleware and system management software and system design documentation, data security protection system, operating systems in devices such as terminals and servers, critical configuration data in network devices and security appliances Evaluation implementation include: 1) It shall be verified whether cryptography is used to ensure confidentiality of identification data, important business data and important personal information during storage 2) It should be verified that technical measures (such as data security protection systems) are used to ensure the confidentiality of identification data, important business data and important personal information during storage 3) It should be tested to verify whether the specified data are encrypted

Example of Requirements and Assessments

After the systems have been adapted, a check is made to ensure that the system is secure. This is performed by external, state-certified service providers. In a final step, a regulatory inspection is carried out. In general, the public security authority can carry out inspections at any time, but at least once, before confirming that the IT systems are secure, it will conduct a review of the systems, during which it will need access to the companies' networks and could potentially gain access to confidential data and information.

Depending on the risk level of the IT systems, such an inspection may be necessary on a regular basis, rather than just once.

5 steps of the implementation for the MLPS

We strongly recommend that all companies operating in China should move quickly in order to implement the MLPS 2.0 - even if it requires a significant investment of time, money and human resources as the enforcement of the system by the Chinese government is gathering pace. Those who fail to comply with the MLPS will have to face severe penalties, which include not only high

fines, but also a blacklisting in the *Corporate Social Credit System*.

Excursus: International Cooperation

In the future, the Chinese state will also increasingly pursue cybercrime and the theft of trade secrets via the Internet in cooperation with other countries. To this end, in July 2019, the Ministry of Public Security launched an operation called Cloud Sword, which focuses on international cooperation in combating transnational cybercrime.

The new program quickly showed results. In December 2019, Nepalese police arrested 122 Chinese citizens suspected of being involved in transnational cyber fraud. Additionally, to the Chinese police, their counterparts in Nigeria were involved as well in this process. As early as October 2019, Mongolian law enforcement authorities arrested 790 Chinese citizens suspected of telecom network fraud in four hotels in Ulaanbaatar, while seizing nearly 1,000 computers, thousands of cell phones and other tools. 759 suspects were sent back to China.

In Europe, the Chinese Ministry of Public Security cooperated together with the Spanish police. Through this cooperation, 229 Chinese individuals who were suspected of telecommunications fraud were arrested and repatriated to China. On the Ministry's high-priority agenda is also the international prosecution of trade secrets theft through cyber espionage. Attackers are targeting not only technical data, but also business lists of customers and suppliers. The program shows that China is also decoupling itself from law enforcement and going its own way.

Cryptography Law (CL)

China's Cryptography Law (CL) has been in effect since January 1, 2021. It aims to regulate the use and management of encryption technologies and facilitate the development of the cryptography industry. The law includes a list of commercial encryption technologies subject to special regulations when importing or exporting to/from China, also effective since January 1, 2021.

The law distinguishes between core, standard and commercial cryptography. Since core and standard cryptography are used to protect state secrets, they are not relevant for most foreign companies in China. Commercial cryptography can be used by citizens, legal entities and organizations to protect their data and systems

As a new development, the *CL* does not explicitly prohibit the use of foreign encryption technologies in China for commercial use. Back in 2017, the Chinese government decided to remove some restrictions for foreign companies in the area of encryption technology. For example, the need of special permits for the use equipment containing encryption technology or the use of encryption technology produced outside of China by foreign invested enterprises was eliminated.

Furthermore, at the end of 2019, the certification system for encryption technologies that had been in place until then was eased, meaning that only commercial encryption products that are on the list of critical network equipment and dedicated cybersecurity products need to be certified.

Commercial cryptographic products or technologies which are developed, used, sold, imported or exported by foreign companies will now be treated the same as domestic products or technologies. However, the importation of cryptographic products, unless they are publicly available consumer products, still requires an import license, specifying exactly who will use the product and for what purpose.

Cryptographic products sold and used in China must comply with a strict set of standards, which will be further defined by additional regulations. A license must also be applied in order to export cryptographic products. However, this will soon be replaced by a comprehensive import-license and export-control system based on international practice.

All companies that use commercial cryptography to protect their data are subject to monitoring and evaluation by the *State Cryptography Administration (SCA)*, which has the right to check whether cryptography products and technologies are used in compliance with the law. However, the *SCA* also refers directly to the *CSL* in Article 26: security testing and certification of commercial encryption technology is subject to CSL regulations and should be aligned with MLPS requirements to avoid repetitive testing and review.

Data Security Law (DSL)

The National People's Congress passed the new *Data Security Law (DSL)* on June 10, 2021. The aim of the law is not only the protection of data, but above all the promotion of data infrastructure and innovative use of data by industry, as well as the development of the digital economy. Provincial governments are encouraged to formulate plans for the further development of the digital economy. The foundation for a functioning, secure digital economy is both cybersecurity and data security.

The law introduces a system for classifying data: assessing the relevance of particular data for the economy and social development and evaluating the damage in a potential case of misuse. The authority to define "important data" is handed over to regional governments, which are to publish corresponding catalogs. This means that in the future, companies may have to check on a regional level whether the data processed in the respective region meets the definition of "important data".

The law repeatedly addresses centralized mechanisms, systems and certified services for data security assessments, data transaction management and data security emergency management. The establishment of these measures lies within the state. The details of such systems are not yet clear, and will most likely be specified in further regulations and standards only after the *DSL* has come into effect.

The *DSL* stipulates that data processing companies are obliged to set up a data security management system and to regularly adapt it to applicable regulations. This system should include technical and operational measures to ensure data security. Companies that process so-called "important data" will be required to appoint a data protection officer and to conduct regular data protection impact assessments of the processing activities. The results of these reviews must be reported to the responsible authority.

In principle, any type of data collection or data processing should be carried out legally and with legal methods. All laws and regulations governing the purpose and scope of data collection and processing must be observed. Organizations or companies that sell data sets should be required to verify where the data comes from and must document the verification and all transactions. Providers of online data processing will have to apply for a special business license.

It is worth noting that, according to the law, organizations and individuals outside China will also have legal obligations once they are involved in China-related data activities, should these violate the national security, public interest or other legal interests of Chinese citizens or organizations. Accordingly, being located outside of China does not necessarily mean being safe from the long arm of the Chinese *DSL*.

The law formulates some principles on cross-border transfer of data. Article 10 of the DSL states that "the State shall actively conduct international exchanges and cooperation in the area of data, participate in the formulation of international rules and standards for data security, and promote the safe and free flow of cross-border data." Nevertheless, the *DSL* also includes regulations that restrict the free flow of data in certain circumstances, such as data related to controlled items associated with the fulfillment of international obligations and the preservation of national security. (DSL

Art. 23). However, a concrete list of these data types does not exist yet. This is also a reference to the new *Export Control Law*, which is aimed not only at products and services, but also at data and at know-how.

Further regulations on data transfer outside China can be found in the *Administrative Measures on Data Security (Draft for Comment)*, *the Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment)* and *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment).*

While the draft *Administrative Measures on Data Security (Draft for Comment)* stipulate that network operators must carry out a risk assessment before transferring "important data" abroad, submit this to the responsible authority and then obtain approval, the *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment)* stipulate that network operators must first undergo a security assessment and obtain approval from the cyberspace authority before transferring personal data.

For example, further preconditions for the transfer should be a contract with the recipient of the data that prescribes an equally high level of data protection at the recipient's site and specifies responsibility for data security. Annual reports to the responsible authority by the network operator should enable the authorities to keep track of "exported" data. Furthermore, foreign organizations collecting data in China will be required to appoint a legal representative in China who will be responsible for ensuring compliance with data protection regulations in China.

The Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft for Comment) provide further details on how to conduct security assessments before transferring data abroad, while also including the list of examples of "important data" (see chapter on *CSL* Privacy) in various industries.

More relevant than the DSL in terms of personal data protection regulations is the draft Personal Information Protection Law, which is discussed in the following chapter.

Excursus: Unfair competition with data rights

Recently, the first decision on *unfair competition with data rights* on Internet platforms was published in China: Tencent, the leader of social media, owns the data and limited data rights of 900 million daily users of the app WeChat. It is known that Tencent shares much of this data with the Chinese government. Nevertheless, the group has filed unfair competition lawsuits against two cooperating Chinese technology companies.

The defendant companies offer social media management software that interacts with functions of WeChat. Users can utilize this software to individually automate and enhance original WeChat functions such as "liking" or "sharing" posts. Additional extended functions such as deleting spam requests or fake accounts are also achievable with this software. Because the software collects and monitors account and user information as well as social relationships and stores them on the server of one of the defendant companies, the software is considered as infringing. The Hangzhou Internet Court ruled in favor of WeChat owner Tencent in the first instance. The defendant companies are ordered to pay damages in the amount of CNY 2.6 million (approximately EUR 319,000) and to take

measures to remedy the damages incurred. This case is a clear example that protection against unfair competition in China is also relevant in terms of data.

Personal Information Protection Law (PIPL)

On October 21, 2020, the *Personal Information Protection Law (PIPL)* was published and released for comments. The law is intended to strengthen the protection of personal data along with the *CSL* and *DSL*.

Foreign companies need to pay particular attention to the extraterritorial impact of this law and the rules on cross-border transfer of personal data. Just like the establishment criteria and the destination criteria of the European Data Protection Regulation (GDPR), the *PIPL*, once in effect, will apply not only to the handling of personal data within China, but also to activities outside of the country. For example, if a company processes personal data for the purpose of providing products or services to individuals in China, or for the purpose of analyzing and evaluating the activities of individuals in China, the PIPL will also apply to activities outside of China. Another risk is posed by Article 42 of the *PIPL*: foreign companies who actually or allegedly harm the interests of Chinese citizens or even endanger China's national security by processing personal data outside of China can be blacklisted - with the consequence that the provision of data to these companies is restricted or banned completely.

The law includes basic principles for processing personal data. For example, data may only be processed using legal methods. They may only be collected to the extent necessary for the purpose of the processing, and the processing must be open and transparent. The data subject must be informed about the nature and scope of the data processing and also about who is processing the data and for what purpose. The personal data processed shall be accurate and, if necessary, updated in a timely manner. The data processor shall be responsible for the processing and shall take appropriate security measures to protect the data. After the purpose for which the personal data was collected has been fulfilled, it must be deleted in a timely manner. With few exceptions, the basis for processing personal data must be the informed and voluntary consent of the data subject. Many of the regulations governing the collection and processing of personal data are very similar to the requirements of the General Data Protection Regulation (GDPR), for example on the topics of data storage and data order processing.

Similar to the GDPR, the *PIPL* also distinguishes between personal data and sensitive personal data. According to the *PIPL*, the latter may only be processed for specific purposes and only if necessary. The definition of sensitive personal data is expanded somewhat in the current draft of the PIPL compared to the *Personal Information Security Specification*. For example, race, ethnicity and religious beliefs are now also listed. A separate declaration of consent from the data subject is required for the processing of sensitive personal data.

The *PIPL* also provides data localization requirements by default for operators of critical information infrastructure, as well as for processors of personal data if the amount of data they process exceeds a certain threshold set by the Cyberspace Administration. If there is a need to provide this data to foreign organizations, it is necessary to obtain the explicit consent of the data subject and have a security review conducted by the Cyberspace Administration beforehand.

If the amount of data processed by a company does not exceed the specified limit, it is nevertheless stipulated that a data protection impact assessment must be carried out and the subsequent pro-

cessing of the data must be documented before the data is made available abroad. The impact assessment must include a review of the legitimacy, justification and necessity of the purpose and methods of data processing. In addition, the risk of a data breach must be assessed, as well as the adequacy of the protective measures taken. In addition, certification for the protection of personal data must be carried out by specialized organizations or a processing contract must be concluded with the party to whom the data is provided, which should guarantee an appropriate level of data protection at the data recipient.

The *PIPL* has not yet come into effect and it is likely that the current draft is not the final version of the law that will eventually come into operation. However, it is very likely that in the future, self-auditing, regulatory review, or even regulatory approval will be required prior to the provision abroad of "important" or personal data by companies in China.

Excursus: National Security Law

The National Security Law (NSL), which came into effect in June 2020, also has implications for companies operating in Hong Kong in terms of technology and data. For example, Internet service providers must now provide authorities with access to user data and review their cross-border data flows. Companies in the field of technology will have to restructure their business operations if Western export bans apply to sensitive technologies.

With the suspension of the United States - Hong Kong Policy Act, the preferential treatment of the U.S. in licensing, exporting and transferring sensitive technology products no longer applies. As a result of the suspension, all exports, re-exports and transfers of such products to Hong Kong will now be treated as goods destined for the PRC, and U.S. companies will not be allowed to sell sensitive technology products to Hong Kong. The EU will respond similarly, and an initial document introducing restrictions has already been published.

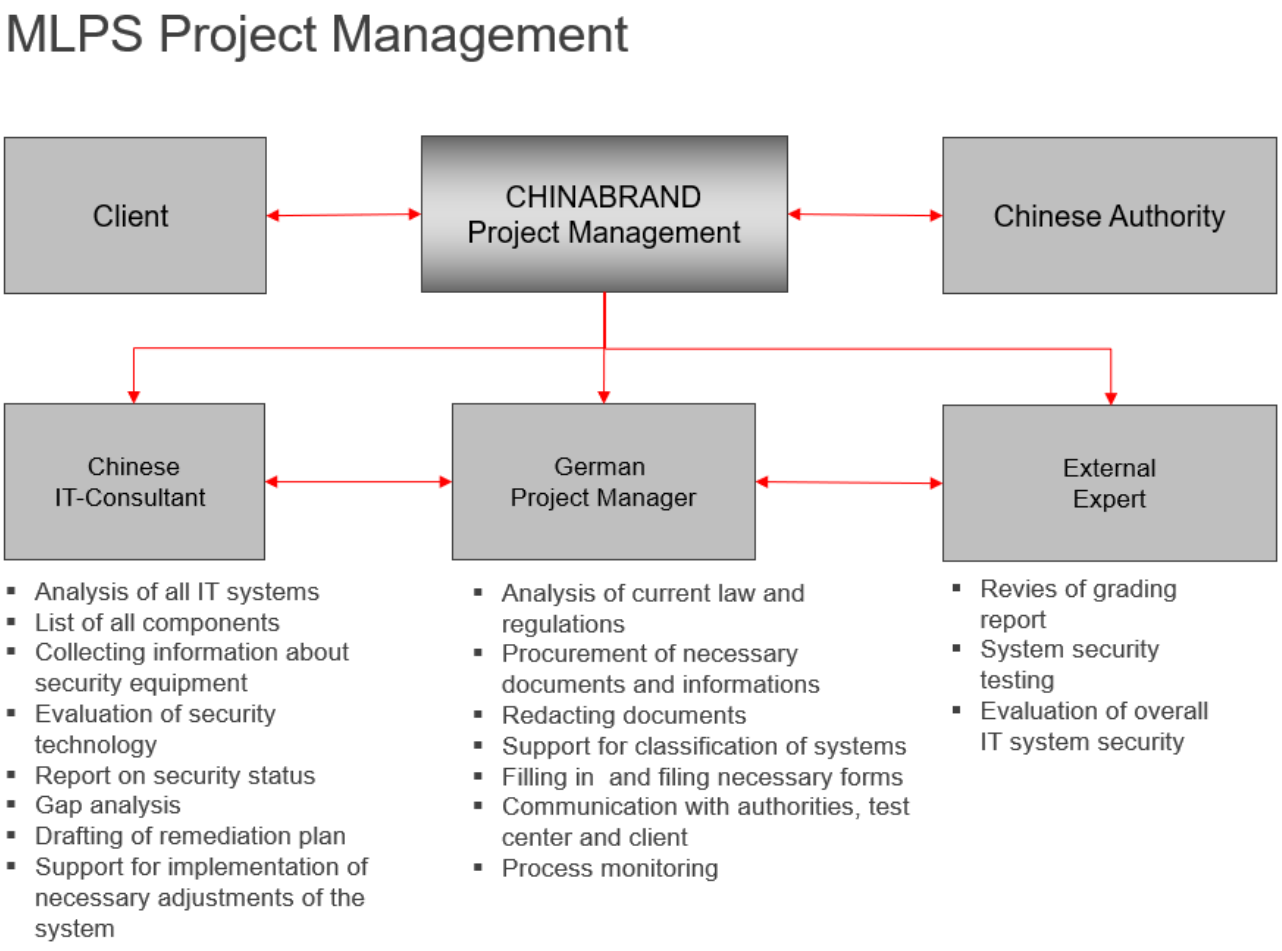
The tightened export restrictions will impact companies that can no longer ship sensitive and high-tech products to or receive them in Hong Kong. Accordingly, supply contracts and compliance policies should be reviewed and adjusted, cooperation with Chinese technology providers as well as alternative technologies should be considered.

Recommendations for Action

The ongoing enactment of new laws demonstrates China's determination to strengthen data protection and cybersecurity in general. This creates additional challenges for foreign companies operating in China. Constant new regulations will force them to constantly monitor Chinese legislation and adapt their compliance strategies.

Specifically, companies should take the following actions now:

CSL/ MLPS: The *multi-level protection scheme* is being vigorously enforced in China. Every company should review which IT systems need to be assessed and registered. Experienced consultants should be involved in this process in order to avoid mistakes. After determining which of the IT systems need to be audited and registered, the risk level of these systems should be assessed in a timely manner. After the risk level has been confirmed and filed with the regional public safety office, the legal requirements for IT systems of the identified risk levels must be collected, compared with the existing security measures and the systems must be adapted to the legal requirements accordingly.



CSL, DSL and **PIPL**: Western companies doing business in and with China should carefully analyze their current situation and the expected future requirements of the CSL, DSL and PIPL. The PIPL is still in the drafting phase to date, but it is expected to come into effect before the end of 2021. The requirements, which are similar to the European GDPR, include the creation of a department responsible for security, risk monitoring, data impact analysis, as well as reporting to the authorities. Companies that have already made efforts to implement concepts in accordance with the GDPR are at an advantage in this situation, although the requirements of the Chinese DSL differ in part from those of the GDPR. Therefore, a close review of the regulations is nevertheless necessary. In addition to reviewing and complying with the standards, other strategic decisions should be made regarding data activities in and with China

NSL: Companies operating in Hong Kong should assess their situation and establish a plan of action to deal with the authorities in the event of a review. We also recommend evaluating your own supply chains for new risks related to NSL and decoupling data exchange from the global network if necessary. This also applies to Hong Kong bilateral agreements that have previously allowed the free flow of data across borders between contracting parties. Here, the risks should be reassessed, existing business contracts should be reviewed and adjusted.

Further Informationen

Authors of this Whitepaper:

Dr. Hans Joachim Fuchs
CEO
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8016
drhjfuchs@chinabrand.de

Mareike Seeßelberg, LL.M.
Senior Consultant
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8015
mseesselberg@chinabrand.de

Zihao Liao, LL.M.
Consultant
CHINABRAND IP CONSULTING GMBH
+49 89 321 212 8013
zliao@chinabrand.de

You can find more information about our services here:

www.chinabrand.de

Contact and Feedback

Blog | LinkedIn | XING

CHINABRAND IP CONSULTING GMBH
Mareike Seeßelberg
Grashofstraße 3, DE-80995 Munich
info@chinabrand.de
www.chinabrand.de
+49 89 321 212 800