Data and Cybersecurity Compliance in China

February 2020

1421 Consulting Group

1. Executive Summary

The rise of digitization and the commodification of big data have changed the business world and will redefine sustainable business models in the 21st century. China's "leapfrog" development plans have allowed them to become a leader in technology, blockchain, artificial intelligence, and 5g. As China continues to make progress the rest of the world is observing their strides.

The central government of the People's Republic of China has made it clear that data and cybersecurity regulation will be a focus of policy makers. While a weak web of regulations and industry guidelines previously dominated the regulatory environment, the last two years gave way to a transformation of the regulatory environment. In an exercise to promote the standardization of cybersecurity and data practices throughout mainland China, a Cybersecurity Law (hereafter "CSL") was released in 2017.

The subsequent legislation hints at an increased focus on user data rights, personal information protection, and responsible data practices. It is expected that further regulations will be released to provide a clearer standard across industries. While some sensitive industries will still be subjected to stricter, industry specific regulation, these changes demonstrate a growing maturity in China's cyber regulatory environment.

Yet to be determined is how these regulatory changes will be enforced in practice. As many different government entities vie to have their status increased, it is unclear who will enforce the CSL as a whole. This will be important for businesses to keep an eye on.

The various guidelines and assessments released impact any business that must collect and store data. In order to remain compliant under China's evolving guidelines and regulations, it is important that businesses assess their own data practices and make sure they are following the "best practices" as defined locally. This report will highlight the regulation changes and provide SME specific recommendations for how best to evaluate your business model moving forward.

1421 Consulting Group

1421 Consulting Group (1421) is a leading consulting company excited about China and driven to help western companies navigate their way in China. Our specialization focusses on supporting Western companies setting up and successfully growing their business in China. We offer a combination of services to help our clients reach their goals, namely; strategy and business consultancy, market entry study, legal advice, administration support, (local) payroll service, company registration and quality control services

1421 Consulting Group has three offices on the Mainland of China; Beijing, Chengdu and in the Greater Bay Area (Shenzhen). These are three of the strongest economic zones of China, with the government based in Beijing, innovation in Chengdu and large industries in the PRD.

Contents

2. Introduction

China's rapid development over the last three decades has given way to new industries, new opportunities, and countless technological developments. Data and cybersecurity have become hot-button issues as technological integration is pushed throughout all industries. Companies in the tech-industries have sought to create solutions to monitor and protect the storage of user data in today's increasingly digital world and many governing bodies have followed suit.

In 2016, the European Union published the General Data Protection Regulations more commonly referred to as "GDPR." Many businesses across the world with business activity inside the EU lamented the increased regulation and protections that they claimed would stifle their ability to innovate and profit off of the amount of data collected. While many businesses involved in the collection and commodification of data opposed GDPR, the regulations were clear in their intent and impact with the enforcing organization clearly stated which left no questions about the path one should take to ensure compliance.

During the same time as the EU's venture into personal data protection and business accountability, China was quietly building their own framework for data protection and regulation. While this venture began with many disparate laws and industry standards, the last five years has fostered the emergence of a unified stance on data protection standards, norms, and uses. While the regulations are stricter for industries engaging in matters that concern national security, the wide-sweeping policies impact almost every business in China. Including the Wholly Foreign Owned Enterprises.

Understanding and proactively seeking compliance in accordance with the Cybersecurity Law, industry specific regulations, and assessment guidelines is necessary to ensure the longevity of any business operating in China that is reliant on technology. The emerging legal framework for data protection and business responsibility are only the beginning as China seeks to further digitize all aspects of life.[1] Protecting personal data and data with implications to national security will remain at the forefront of President Xi Jinping's priorities.

3. Data and Cybersecurity Governance

Currently in China, there are many different government entities vying for the power to create and enforce data governance and cybersecurity policy. All these different national-level entities have unique goals and interests related to the expansion and evolution of China's data and cybersecurity infrastructure. In China's decentralized bureaucracy it can be quite difficult to determine which government entity is leading the way in the push for more sector regulation and who will lead the charge in the enforcement and management of these new data regulations. Unlike the clearly defined public projects and goals of many western democratic governments, decisions about which agency will lead the push for policy research or enforcement can only be clear after implementation and enforcement cases come to light.

[1] Xi Jinping speech at the "National Cybersecurity and Work Conference", April 20, 2019, Beijing, China.

3.1. Who's calling the shots?

When it comes to cybersecurity regulations, there have been substantial developments over the last few years, but which organization has authority over developing and implementing policies in this field? President Xi Jinping noted that the fields of data and cybersecurity should be a key focus of the Party to deal with the risks and development of a new digital world.[2] To tackle these challenges, Xi created a Leadership Small Group (LSG) in 2014 bringing together prominent members of relevant government ministries and the military together to discuss the need for cybersecurity policy measures.

Currently, China does not have a single authority responsible for all legislation concerning data and privacy protection, instead it is very much a joint effort between pre-existing agencies. Due to the amount of funding and the importance placed on the development of cybersecurity regulations, multiple organizations have been actively pursuing to establish authority in this field. Relevant government organizations include:

- The Cyberspace Administration of China (CAC);
- The Ministry of Public Security (MPS);
- Ministry of Industry and Information Technology (MIIT);
- The National Information Security Standardization Technical Committee (TC260), and;
- The State Administration for Market Regulation (SAMR).

Of this list, the first three are considered to be the most important.

The CAC, founded in 2014, is seeking to assert its authority over cybersecurity and digitalization. As the office of a Xi Jinping-led Leading Small Group, it commands a certain authority. Currently, the CAC is responsible for planning and coordinating cybersecurity and relevant administrative and supervisory work, while other relevant departments created by the State Council are responsible for supervision and administration in their own specific sectors. As such, most of the recent general cybersecurity regulations have been drafted by the CAC.[3]

The MPS is responsible for running the system that blocks Chinese access to certain parts of the global internet, often referred to as the "Great Firewall of China". In the past, MPS also had primary responsibility for critical infrastructure protection, however, since the new law came into effect, the CAC also has obtained part of this portfolio. Apart from this, the MPS can also distribute administrative penalties and oversees criminal investigation against unlawful activities relating to collecting, selling and disclosing personal information. The MIIT in turn, as a major developer of digital strategies and plans, is responsible for a substantial amount of regulation of ICT sector industrial policies. Its think-tank subordinate, the China Academy of Information and Communications and Technology (CAICT) also plays a role in the drafting of ICT-related policies and development.

It is important to note that while this section highlights the national level ministries and commissions working on data and cybersecurity issues, many provinces and even some counties have their own government organizations working to create a streamlined process for dealing with these modern concerns. The decentralized nature of China's government often allows local public officials the power to engage in policy entrepreneurship and test their policy ideas on a local level. It is likely that some provinces will create their own regulations in order to confront local concerns and exercise their right to regulate their

[2] *Qiushi,* September 15, 2017, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm
[3] For more information on the CAC's goals for future policy development, please reference the following article by New America's "DigiChina" project.

own locality. This paper will focus primarily on the national legal framework for policy making and enforcement, but it is imperative to understand any specific local laws or differences that may exist in addition to the national level policies.

Apart from relevant government organizations, there are also a select number of non-government organizations that can influence cybersecurity policymaking, mainly consisting of Chinese industry alliances and associations, and the BAT(J) companies.

Chinese industry alliances and associations relating to the technology sector in China include for example the Cybersecurity Association of China (CSAC) and the China Artificial Intelligence Industry Development Alliance. As these groups are made up of many important Chinese ICT company members, they function as intermediaries between the private sector and the government, allowing for the transmission of policy ideas and feedback in either direction.

The BAT(J) companies are China's largest, most influential internet companies: Baidu, Alibaba, Tencent and since recently also JD.com. These companies created the ecommerce, search engines, and internet landscape that runs the Chinese internet today. As leaders in the Chinese tech market, their affiliated research institutes have also gained a certain amount of influence on public policy debates related to upcoming technologies.

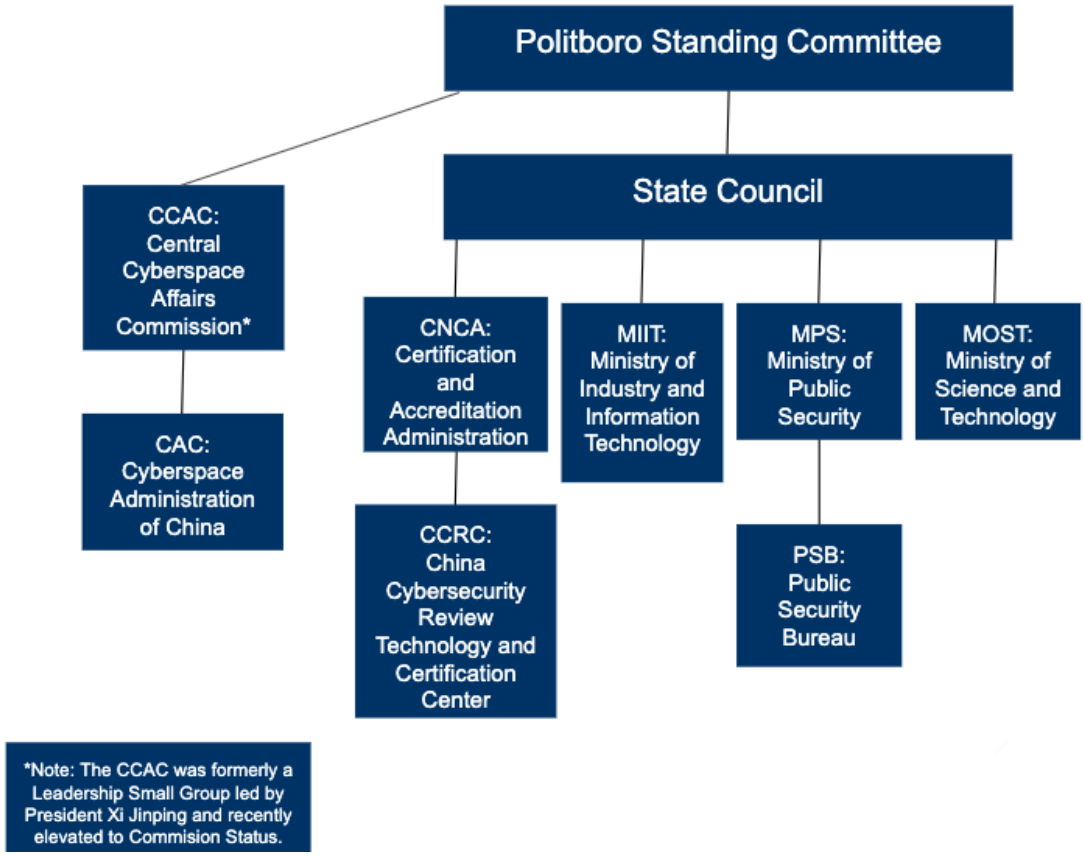

Figure 1 Calling the shots

4. Emerging Legal Framework

Until recently, China's data privacy framework consisted of a patchwork of rules, industry norms, and loosely regulated standards. While the laws regulating certain industries were clear and easy to follow, many emerging industries fell by the wayside. The Cybersecurity Law, hereafter "CSL", which came into effect in June 2017 was the government's attempt to integrate all disparate laws into a more comprehensive, national-level piece of legislation.

The law generally applies to the personal data collected over networks. Many specific aspects of personal information security, regulation, and storage remain to be clarified under the umbrella framework offered in the CSL but have given way to new laws drafted for comments from industry actors. These laws include the Information Security & Technology Personal Information Impact Assessment, Personal Information Deidentification Guidelines, and the Guidelines for Cross Border Data Transfer Security Assessment. These laws submitted for comment will clarify the existing framework and strengthen the protection of individuals' personal data collected by businesses. These laws also provide a clear framework for how to assess the risk of certain data sets.

4.1. Cybersecurity Law Overview

The Cybersecurity Law released in 2017, was the much-awaited regulatory development that came out of many years of working groups

The CSL clarifies the responsibilities of storing and protecting data collected by network operators. The CSL defines a "network operator" as both the owners and administrators of a network as well as network service providers. The CSL also defines a "network" as any system that consists of computers or other information terminals, and related equipment for collecting, storing, transmitting, exchanging and processing information. This definition expands the scope of businesses covered by the CSL and provides new responsibilities and compliance requirements for all businesses collecting any data sets through their work in mainland China.

The CSL also expands the definitions of "personal data" to include any information that identifies a natural person either by itself or in combination with other information. This includes a person's name, address, telephone number, date of birth, identity card (身份证) number and any biometric identifiers. Due to this expansionary interpretation of what is personal data, businesses that collect simple consumer data may find themselves covered by this new law.

In the CSL, network operators are prohibited from collecting data that is not relevant to the services they offer. This is understood to cover any data that does not coincide with the business's declared "scope of business" in their legal registration.[4] Like many other aspects of the new CSL, it is still unclear how this will be enforced in practice and which of the many organizations involved in managing various aspects of the new cybersecurity framework will be tasked with enforcing it.

[4] "Business scope" is a legally declared list of activities all businesses plan to engage in.

4.2. CSL Compliance Measures

The Cyber Security Law requires all network operators to store users' personal data in strict confidence. This includes an obligation to implement technical measures to monitor and record the operational status of their networks and the occurrence of cybersecurity incidents.

Under the CSL, businesses classified as "network operators" are also required to back up and encrypt anything that is considered to be "important data." All "important data" must be stored by the network operator for a minimum of six months after initial collection. The CSL failed to clarify what data will be understood to be "important" under the new regulations. In the later released document entitled the "Security Assessment Measures", however, "important data" was defined as any data that is related to national security, economic development and societal and public interests.

This rather broad definition leaves the door open for a broad application of the label. For instance, it is widely understood amongst data companies that profit off selling insights into digital trends that any location data, such as foot traffic monitored by some map apps, is highly sensitive and classified as "important." To many laymen this could seem strange, but industry experts understand that monitoring movement around potentially sensitive locations throughout the mainland can be interpreted as an issue of national security under this classification system.

In order to ensure compliance, the network operators are also required to explicitly inform users that their data is being collected before the data is stored. The user must be informed of the purpose, means, and scope of the intended data collection. All processing of personal data must then remain in accordance with the scope of the agreed upon terms provided to the user initially. The CSL therefore operates on a user-consent basis meaning that no collection of data is inherently illegal so long as the user agrees to the terms of the network operator.

The Cyber Security Law imposes a mandatory obligation to promptly inform Data subjects of a data breach or other loss of personal data. A network operator is also required to report the incident to the relevant sector regulator and to take immediate remedial action. In certain cases of negligence, a network operator can be held criminally responsible for the loss of data.

After the release of the CSL, many questioned if these same standards of consent-based data collection and processing applied to employee information. The definition of a "network" underneath the CSL is broad enough to include a company's internal networks and systems, but it is widely understood that the superseding law should be the "Provisions of Employment Service and Employment Management" that has been in effect since 2008. These provisions require employers in China to keep employee information confidential unless written consent from the employees in question is obtained.

4.3. Data Localization

The Cybersecurity Law mandates local storage solutions for all businesses deemed to be operators of "critical information infrastructure." The CSL did not define this term, but it appeared earlier in a document on the Cyberspace Security Strategy of the Cyberspace Administration of China (CAC). This 2016 document defines "critical information infrastructure" as all "information infrastructure that affects national security, the national economy and people's livelihoods, such that, if data is leaked,

damaged or loses its functionality, national security and public interests may be seriously harmed."

CAC later released a document[5] outlining industries and sectors that are "critical information infrastructure" operators. These industries are subject to change in the next few years and will likely be the target of subsequent industry specific standards. The current list of industries include:

- energy, finance, transportation, water management, sanitation and healthcare, education, social security, environmental protection and public utilities, etc.
- information networks, such as telecommunications, radio and television, the Internet as well as businesses providing cloud computing, big data and other large-scale public information network services
- scientific research and production in fields such as national defense, industrial equipment, industrial chemicals, food and drugs
- radio stations, television stations and other news agencies

The CSL requires that businesses operating in these critical sectors at a large enough scale store their data locally since 2017. The intention is not to include every business that falls into one of these sectors, but rather those that operate on a large enough scale that they provide critical infrastructure within their sector. No subsequent laws or regulations have clarified which agency will oversee and enforce this regulation.

It is important to note that many industries had localization requirements prior to the CSL's passage in 2017. For example, financial personal data collected in China has had local storage requirements since 2011. Some industries not mentioned above may still require local storage of data collected in China.

4.4. Subsequent Legal Framework

Three subsequent legal documents have expanded and clarified the scope of the Cybersecurity Law. These laws include the Information Security and Technology Personal Information Impact Assessment, Personal Information Deidentification Guidelines, and the Guidelines for Cross Border Data Transfer Security Assessment. In this section, the assessments and guidelines purpose will be explained briefly.

4.4.1. Personal Information Impact Assessment[6]

The Personal Information Security Specification requires that stricter security measures to be used, such as encryption, when storing "sensitive" personal data. This assessment and security specification allow the Ministry of Public Security to monitor businesses that collect potentially harmful data.

Draft Ministry of Public Security (MPS) Regulations on the Graded Protection of Cyber Security (the MPS Regulation) released in June 2018 will require businesses to obtain certification from the MPS if the disruption of their network would result in serious harm or worse to individual rights and interests or harm to public interests or national security. The security classification, which rates the business on a sensitivity scale between 1 (low risk) and 5 (high risk), is based on criteria such as the function of the network, the nature of the service offered, the types of data being processed and the

[5] CAC's draft Regulations on the Protection of Critical Information Infrastructure published in July 2017.
[6] The PIA can be found here.

potential damage of a security incident, in particular, the impact on national and economic security interests. This broad definition allows the MPS liberty to rate businesses on a wide scope of issues and impact. The MPS will conduct an audit of every network graded 3 or above at least once per year.

Under the Security Assessment Measures and the Personal Information Security Specification, if an organization has more than 200 personnel and its main business involves processing personal data, or if the organization is expected to handle the personal data of more than 500,000 people over the next 12 months, then it should establish a department with dedicated staff to handle personal data security. This role within a company may lead to direct personal liability for breaches of the core data privacy provisions under the law.

The Personal Information Security Specification also defines "sensitive" personal data as personal data that, if disclosed or illegally processed might endanger personal and property security, damage personal reputation, or physical or psychological health, or lead to discriminatory treatment, etc. This may include personal ID card numbers, biometric data, bank account numbers, personal communications, credit records, geolocation data and health data, as well as the personal data of children under the age of 14 years. This standard requires an "opt-in" method, where the data subjects must provide written consent to businesses that plan to collect and store their personal data.

Furthermore, Impact Assessments are required for businesses considered to be data controllers[7]. They must submit an assessment yearly or sooner if there has been a major change to their business scope, use of information systems, or security plans. The assessment is understood to examine if the business has had an adverse effect on the lawful rights and general interests of their data subjects. The assessment will also ensure that proper anonymization of data collected is occurring in order to protect the identities of the subjects.

4.4.2. New Rights of Data Subject

The Personal Information Security Specification introduces for the first time various new rights comparable to the individual rights under many Western legal frameworks. The rights allow data subjects to request the erasure of all personal data collected by a private business and ensures that businesses anonymize data when users close their accounts. The users also gain the right to request that their data be transferred to a third party. Businesses must comply with these user requests within thirty days.

4.4.3. Personal Information Deidentification Guidelines (Draft)

The Draft Guidelines provide a voluntary technical specification, the purpose of which is to provide guidance to data processers on the de-identification of personal information. The Draft Guidelines specify the purposes, principles and procedures for the de-identification of personal information. They also introduce common de-identification technologies, such as sampling, aggregation and cryptographical tools, and an introduction to common de-identification models.

Put simply, the Personal Information Deidentification Guidelines simply provide an overview of how businesses should store and protect the data of their subjects. When sensitive data is collected, it must be anonymized so that if a breach were to occur, it would be difficult to ascertain the subject's identity when parsing through the data. The guidelines explain that any data that pieced together could expose a subject's identity should be stored separately and encrypted. Businesses that store this data are held responsible for the adverse effects a data breach and identification of subjects.

[7] Data controllers are the managers or hosts of data sets.

4.4.4. Guidelines for Cross Border Data Transfer Security Assessment (Draft)

This second draft of guidelines on Cross Border Data Transfer was released by the National Information Security Standardization Technical Committee (TC260) in August of 2017 following the CSL. The guidelines are currently "non-binding" but provide very specific norms for any transfer of data from China. The guidelines also clarified some points of the CSL through defining "important data" and the broad definition of "information data." The Appendix A of the guidelines provides examples of what can constitute important and information data, including many notable examples of personal information such as medical records, genetic and biometric information, account information and transaction records, e-commerce account information and transaction records, and personal consumption habits.

The guidelines also provide information that is useful in order to assess the level of security necessary for each data transfer. Depending on the size of the data being transferred and the sensitivity of the data, different assessment requirements are in place. Larger data sets will generally be more sensitive and require a more thorough assessment before a cross-border transfer is permitted.

These guidelines define a "data transfer" as any movement of personal data outside of China. The guidelines specify that even remote access to data stored in China are data transfers even if proper encryption and de-identification technologies are implemented. For this reason, the cross-border data transfer regulation poses great risk for foreign companies with offices inside and outside of China.

In order to legally transfer data, businesses must complete a security assessment for cross-border transfers administered by the Cyberspace Administration of China (CAC). The security assessment is an internal self-certification process conducted and documented in a written report by the transferring entity. This security assessment requires businesses to report on factors such as the necessity of the overseas transfer, the amount of personal data, the various security measures in place during transfer, and any implications the transfer of such data could have to local or national security. It is understood that unless the business can prove that they have a "genuine need to transfer data overseas for reasons of operational necessity" that the transfer request will be declined.

The security assessment should be carried out by a working group comprising legal, security, technology and management personnel. The report must be kept for a minimum of two years. Transmission logs must also be kept for two years. For large transfers, data sets including personal information of 500,000 people or data sets larger than 1,000GB, all network operators are required to submit the security assessment report to the relevant authorities before making the transfer.

4.5. Enforcement of the CSL

While it remains unclear in most cases which governmental organization is tasked with enforcing compliance, the laws and subsequent guidelines have clarified the punishments for violating aspects of the CSL.

4.5.1. Penalties under the Cyber Security Law

Penalties for infringements of the core data protection provisions of the Cyber Security Law may include a fine of up to 10 times the amount of unlawful gains or a fine of up to RMB 1,000,000. Persons in charge of data protection compliance within an organization and other responsible

individuals may be separately subject to a fine of between RMB 10,000 and 100,000, or between RMB 50,000 and 500,000 for serious cases.

Furthermore, according to the interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information (effective 1 June 2018), it was declared that in certain cases an individual could be held criminally responsible for violating the CSL.

4.6. Conclusion

The legal framework surrounding cybersecurity and data in China is rapidly developing into one of the strictest systems internationally due to the broad definitions of personal data and the narrow view on what data is necessary to a business's operation. Through examining the laws drafted for comment, expanding the scope and impact of the Cybersecurity Law of China, it is clear that the focus on protecting user data and national security through codifying cybersecurity and data norms will continue to be a focus of the Party throughout the next decade.

Figure 2 Changes after CSL

5. CSL compared to GDPR

After the release of China's Cybersecurity Law (CSL), many foreign businesses sought to understand China's emerging legal framework of data protection in the context of another global law on data protection and cybersecurity- the EU's GDPR. Although the purpose of both laws is similar, in that they seek to protect user data and provide guidelines for new technology applications, the overall regulations, intricacies, and enforcement mechanisms are quite different on several key points.

5.1. Personal data protection

The GDPR approaches this part of its regulation as a component of the rights of the individuals. And identify personal data as any information relating to an identifiable or identified person. Moreover, the GDPR further also enhanced obligations on special categories of personal data. This includes ethnicity, political views, religion, philosophical beliefs, trade union membership, health data, sexual related subject and genetic or biometric data.

The CSL data has a bit of a different approach as China is more focused on the national protection to secure the network infrastructure and the data passing through it. This can be seen from the fact that the CSL also captures non-personal information, called "important data" in the legislation. This data is closely related to national security, economic development and public interest. The CSL also has a definition of personal data and identify it as: any kind of information that independently or in combination with other information could be used to identify a person's identity. This includes any personal data that if disclosed could cause harm to persons, property, reputation, mental and physical health. This would include names, ID numbers, birthdates, biometric data and addresses.

5.2. Data Breaches

Under the GDPR, there are clear guidelines for how to manage data breaches as they happen. There is a standard notification system that is utilized for all breaches. GDPR encourages but does not require businesses to store their data in GDPR-compliant locations.

Under the CSL, however, the guidelines for how to manage a data breach as a company are based instead on the sensitivity of the data breached and the likelihood that the data released could have a substantial negative impact on the lives of those whose data was illegally accessed. The CSL safeguards against breaches by providing clear standards and regulations on storage of all data within China.

5.3. Personal Data

Both the GDPR and the CSL allow individuals to request the removal or correction of their personal data. Furthermore, both the GDPR and the CSL require the consent of the individuals and companies should provide enough disclosure to data subject for the collection of data. In this way both regulations seem similar. However, the biggest difference in this part is that the GDPR states that there must be affirmative consent, whereas the CSL does not specifically state that this is needed, but this is further clarified in the "Guidelines" (2018).

GDPR	CSL
Data Protection	
• Individual focus • Personal data is any information relating to an identifiable or identified person.	• National Focus • Personal data is any kind of information that independently or in combination with other information can be used to identify a person. • CSL also covers and protects sensitive non-personal data related to National Security & Economic Development.
Data Breaches	
• Standard guidelines for all types of data breaches • Firms are not required to store data in GDPR complaint location.	• Guidelines and response depend on the sensitivity of the data • Standard regulations for all types of data storage
Personal Data	
• Individuals can request to remove or adapt personal data. • Companies are required to disclose to an individual how and what type of data is collected. • Affermative consents by the individual is required	• Individuals can request to remove or adapt personal data. • Companies are required to disclose to an individual how and what type of data is collected. • Consent by the individual is required. How this must be given is not defined.
Fines	
• Fines can go up to 10-20 million Euro	• Highest fine is up to 10 times the amount received by the company from illegal gains. • Serious offences can result in the suspension or withdrawal of the business license.
Data Transfers	
• Prohibited to transfer personal data to non-EEA members, unless data security is deemed strong enough. • No mandatory assesment of data storage practices within the company.	• Before data transfer a security assesment must be made and approved by industry officials • There is an annual mandatory self-assesment for data storage practices within a company.

Figure 3 Comparison between GDPR and CSL

5.4. Fines

Both regulations have fines for companies that do not comply. For the GDPR these fines can go up to €10 million or €20 million this depending on what type of violation is conducted. However, if a company exercises control over another company and form a single economic entity, this is up to 4% of the company's total worldwide annual turnover of the previous year. This depends on whichever fine would be higher.

For the CSL the fines are considerably lower in most applications, with the highest fine being 10 times the amount received from illegal gains. This does not mean that CSL is less strict, however, as serious offenses can result in the suspension or even withdrawal of a business license therefore barring the business from operating in China. Unlike the GDPR, it remains unclear exactly what arm of the government will be tasked with enforcing various aspects of the CSL.

5.5. Data Transfer

In order to have an approved data transfer under the CSL, foreign companies which collect "important" or "personal" data within the territory of China must first submit a security assessment related to the intended data transfer. Under the GDPR, there is a general prohibition on transfer of personal data to non-EEA recipients, unless the recipient country has been deemed to have a decent data protection level.

Another difference is that unlike the GDPR, the CSL requires that network operators conduct a security self-assessment every year where data controllers must self-evaluate their own breach risk level and their own personal information de-identification compliance levels. Companies must also complete an assessment if cross-border data transfer occurs, an operator of CII is transferring data over the border, if the nature of a cross-border transfer changes, or if it is required by regulators.

CASE STUDY: Chinese Cybersecurity Company

The third company interviewed by 1421 is a nationally certified high-tech enterprise with internationally advanced data backup technology. This company is devoted to the R&D and marketing of operation and maintenance level storage and backup hardware-software products with independent intellectual property rights. With its strong core technology research capacity, standardized hardware-software development and management process as well as a specialized technical support team, they became the only manufacturer in China that can produce completely domestic all-in-one backup and recovery solutions for customers from various industries. This data and cybersecurity company, as a manager of the storage and security of data in China, is viewed as an expert manager of domestic data security systems. 1421 met with this company in order to evaluate the domestic perspective on the tightening legal framework surrounding private companies use of data.

When discussing the increased security laws with a representative from this company, they noted that these changes would be the most taxing for large, Chinese companies. They stated that while foreign companies might have to increase their business costs in China that they could leave if they felt it would not be profitable. Chinese companies, on the other hand, had to adapt to the new legal environment in order to be able to internationalize and remain compliant in their country of origin.

For this company, they view these new changes as welcome as it will hold the private companies to similar standards that the semi-public companies have had to grapple with for years. This cybersecurity firm works with the Chinese government on military contracts for decades monitoring sensitive location information. The company sees the decryption and focus on protecting Chinese citizens as the next step in maturity of China's cyber sector. They noted that more mature cyberspheres, such as the EU, have also begun restricting the amount of information that can be transferred or utilized by companies without notifying the people whose data is being manipulated.

5.6. Conclusion

While there are key similarities between the GDPR and CSL, the CSL's overall enforcement mechanisms remain much opaquer. It is widely speculated that the CSL will continue to evolve in order to suit the needs of China as it focuses more national attention on protecting the data of its citizens and ensuring national security.

---

6. Industry Specific Issues

Aside from the intricacies of the Cybersecurity Law and subsequent guidelines issued by various government organizations, there also are legal requirements relevant only to specific industries in China. While the goal of the CSL was to integrate all the different industry standards, because of the specific technical or sensitive aspects inherent to certain industries, this has not been possible. CSL is seen as the superseding national standard, but pre-existing industry level regulations that require stricter security or monitoring are still enforced despite the CSL.

Many industry laws come from ministry-level government organizations relevant to the industry at hand, but they often require the input and support of the party affiliated industry associations. Specific guidelines and norms are most commonly found in industries related to key areas of concern, such as, telecommunications, cloud computing, data storage and management, etc.

In this section, we will review two ways in which these industry specific regulations manifest: as Industry Laws or as mandatory or "voluntary" Industry Certifications.

6.1. Industry Laws

Industry Laws are generally issued by the national ministry relevant to the industry at hand. These laws take effect nationwide and are targeted at controlling or monitoring certain aspects of industries that were previous left unregulated by national law. An example of an industry historically prone to very strict national industry laws in China is the telecommunications industry. Through the example of the telecommunications industry, the possibility of industry specific laws will be explored.

The telecommunications industry is highly regulated because of the sheer size of the data it can produce, the sensitivity of the personal data, and the implications the data collected by companies in the industry can have on national security[8]. The telecommunications industry in China is primarily monitored by the Ministry of Industry and Information Technology (MIIT). While the MIIT covers many industries and is growing and prominence, their focus on telecom activity is still a core responsibility of the ministry.

MIIT oversees the revision and enforcement of the two most prominent telecoms laws in China: the PRC Telecom Regulation and the Catalogue of Telecom Services by Category. The PRC Telecom Regulation modified twice since the laws

[8] See Personal Information of Telecommunication and Internet Users (2013)

implementation in 2000, stipulates that all network connections and data must be monitored by the MIIT as a matter of national security. This adds a higher level of scrutiny than the CSL or subsequent guidelines currently require for all data collected and managed by businesses deemed to be in the telecommunications industry.

Apart from sensitive industries such as the telecom industry, many emerging industries like cloud computing are also receiving increased scrutiny from MIIT. A document entitled "On the Clean-up of Networks" released by MIIT after the passing of the CSL brought new regulations and storage norms to the cloud computing industry. Although this document has no legal enforcement mechanism, it is considered the industry standard and many businesses believe that the guidelines in the document will likely be codified soon.

The new E-commerce law released in early 2019 also included regulations that expanded the scope of cybersecurity requirements for businesses in the e-commerce sector. E-commerce providers must comply with extra regulations in order to safeguard their data collected against any cyber incidents that may occur.

It is unclear whether all the existing industry laws will be integrated into a later version of CSL or a similar policy or if certain industries will continue to be regulated by ministry-level government organizations as well.

6.2. Industry Specific Certifications & Licenses

Another aspect of cybersecurity and data regulation not currently integrated into the framework of the CSL or various assessment guidelines exist in the form of industry certifications and licenses. There are currently "mandatory" and "voluntary" certifications required for certain higher-risk industries. These certifications or licenses are not new to the world of technology and cybersecurity in China- many other industries have long required domestic and foreign businesses to apply for extra paperwork in order to be allowed to operate. In this section, examples of extra certifications that expand upon the regulations of the CSL will be reviewed.

One example of a mandatory certification regarding data and network management is the "Mandatory Certification for Cloud Computing." This certification mandates that all businesses utilizing cloud computing services must apply for and obtain an "internet data center license." This license is related to the local storage requirements of all data collected in China as mandated by the CSL. The license is necessary for businesses of a large scale to have before they may open their local storage centers. Amazon China had to obtain this license in order to open and operate their center storage center in Ningxia Province in order to remain compliant.

Conversely, businesses collecting large amounts of personal information and data sets can also apply for and obtain the "voluntary" Information Security Certification.[9] This certification covers products that are meant to be sold to increase the security of business networks, such as communication and data security. While the certification is only mandatory for businesses selling products in the government procurement market, many private businesses engaged solely in B2B sales view the certification as a necessity to ensure their own compliance. When discussing this certification with

[9] For more information on this certification specifically, please see this paper by EU-SME.

a large, Beijing-based data protection company engaged in B2G work, the business representatives suggested that if not the Information Security Certification, another similar certification would likely be created for businesses engaging in B2B product sales of similar products.

CASE STUDY: Large Chinese Data Company

A leading Chinese data company that was founded to sell both raw data and insight reports to both domestic and foreign companies has redone their entire business strategy based on concerns surrounding the changing legal environment of data protection and cross border data transfers. When the company was founded, they collected data through their apk toolkit that allowed other companies to easily build apps in China in exchange for allowing the company to collect user data from their platforms. In the past, the company sold access subscriptions to any company for all sets of data.

After a report that a similar company, iResearch, was under investigation in early 2019 for selling sensitive location services data to a foreign company, the company shut down all sales and access of location data collected through their apk. The company then limited sales to foreign company only to "sandbox" access. This allowed foreign companies to access and manipulate data sets but limited what they could download from the system. No data sets could be copied themselves, but foreign companies could access download the graphs and charts they created from the data. This was seen as a loophole to the cross-border data transfer laws as the data is technically never leaving China as a set.

Due to further speculation that laws will continue to become stricter in their scrutiny of data sales to foreign entities, the company shut down their sandbox system and now only sells simple, non-sensitive insights to foreign companies. An example of a common insight would be a report on "Chinese screen time per day on average" where no personal information or sensitive demographic data is shared with the purchasing company. Because companies processing larger amounts of data are under increased scrutiny under the new legislation, the unique selling point of their company's large data sets now puts them at risk for increased costs of internal decryption, reporting on sales of data sets, and secure storage methods for their data.

The company then disbanded their international sales team internally as they believe they will not be able to profit from their old business model of giving foreign companies a window into Chinese consumer behaviour through data sets. It is unclear if this company will ever reopen their international sales department or reopen their sandboxes to foreign companies.

6.3. Conclusion

Businesses should be aware of their industry's requirements and norms to remain compliant- especially if they are engaged in emerging industries heavily reliant on technology and data storage. While the national level legal framework continues to grow, it will likely borrow from industry norms and standards in order to respond to technological advancement and digitization.

---

7. Relevance to Foreign SME's

While most companies interviewed note that large companies will be under more scrutiny, SMEs should work to adjust their business model to be proactively compliant and safeguard against legal risks incurred by data transfers or data storage risks.

7.1. Data Protection Regulations in China – Importance for SMEs

With data security becoming more and more important, see for example the GDPR regulations implemented in the EU, China's data privacy framework has also been refined and expanded by the implementation of the Cybersecurity Law (CSL), PI Security Specification and other relevant laws and regulations. Data collection, storage, transfer etc. is all covered under this law. While large overseas data transfers regulations are in most cases not relevant for SMEs, there are certain regulations that are especially relevant to smaller companies that relate to data storage and the anonymization of personal data collected.

7.2. Classification of networks and data

Under the CSL, companies in certain industries must comply with stricter data protection regulations, these companies are referred to as "Critical Information Infrastructure" (CII) operators. According to CAC's Cyberspace Security Strategy, a critical information structure is one that affects national security, the national economy and people's livelihoods, in such that in case of a data breach, national security and public interest may be severely harmed. Sectors and businesses that are deemed to have critical information infrastructures, depending on the degree of impact of a data breach, include for example energy, finance, healthcare, education, telecom, radio, television, the internet etc. However, there is no exhaustive list to determine whether a business is a CII operator or not. To create a business compliance strategy, it is important to use the official information released to determine whether your SME is a CII operator and ensure compliance with data protection regulations.

Similarly, it is also important to be aware of additional regulations concerning so-called

"important data", which is sensitive information defined as data closely related to national security, economic development and societal and public interest. If planning on collecting and/or analyzing such data, it is necessary to make sure of compliance with regulations concerning important data.

7.3. Network and data protection costs

According to the CSL, all network operators have to appoint network security officers to protect the security of their network, and if a company is deemed to engage in activity that endangers "Critical Information Infrastructure" (CII), which might be the case for certain industries, also a security manager officer has to be appointed. Additionally, if personal data is collected, a Data Protection Officer has to be appointed and a Data Protection Department has to be set up. This might be a challenge for SMEs with few employees as it drives up costs. However, failure to comply can result in substantial fines being imposed on the enterprise. If an enterprise fails to make rectifications after being ordered to do so a fine ranging from RMB10,000 to RMB100,000 may be imposed. Additionally, a fine from RMB5,000 to RMB50,000 may be imposed on the person in charge. In the case of CII operators, the general fines may even be 10 times as high. This means that when entering the Chinese market, it is important for SMEs to also take the costs that come with hiring data protection officers into consideration. In some cases, depending on the company involved, it might make more sense to appoint a third party to process personal data on its behalf.

7.4. Storage & cross-border data transfers

When it comes to data storage, there are also some things to be aware of. For CII operators, personal data and data that is considered to be "important data" by CSL standards collected or generated in China must also be stored in China. Additionally, if such data for any reason must be transferred outside of China, a security assessment must be completed and approval from relevant industry authorities is necessary, which all form extra costs for the SME in question. It is important to note that cross-border data transfers are defined very broadly, meaning that it might be easy to unknowingly engage in such transfers. The Guidelines for such transfers for example specifically state that even remote access, whether encrypted or not, already constitutes a data transfer.

7.5. Policy environment

Lastly, SMEs who are or want to become active on the Chinese market should be aware of the general direction in which Chinese policy currently is developing, as this is something that is not set in stone and can change quickly. However, looking at the effort that has been put into the establishment and development of a more developed privacy protection system in the last few years, and the amount of policy encouraging use of big data and the development of new internet business modes such as in the Plan for Promoting the Upgrading of Key Consumer Goods and the Recycling of Resources (2019-2020), it is clear that for the foreseeable future, big data will most likely play an important role in China's planned economic future. As such it can be expected the laws and regulations concerning data protection and privacy will continue to be developed and enhanced to ensure smooth economic development in this area.

CASE STUDY: Small Health Food WFOE

1421 talked to a small foreign company registered in Beijing and Shanghai about the most recent changes to personal data and cybersecurity laws. This health food company has been active for four years in China and manages their own factory producing their products and sells their product exclusively in China. This company sells health food products over various ecommerce platforms such as t-mall and their WeChat official account.

The company collects minimal consumer information including name, address, phone number, order frequency, payment method (bank card or WeChat wallet), etc. The combination of the data together does qualify as "personal identifying information" because of the different metrics pointing to the residential address and phone numbers together. The company currently does not have any intent to take their products off of these larger ecommerce platforms. Concerns over data management contribute to this decision according to one of the company's CEO's who stated that "having the platforms bear the burden of data [management and encryption], remove some compliance hurdles for the company."

The company did note that they do not believe that small companies will be reviewed as much as larger companies. The CEO noted that if they were given the opportunity to run their own store, they would be willing to create a strategy to manage the data storage on their own, but that the cost would likely be too high for their current level of operations.