Jihong Chen, Lu Han, Dennis-Kenji Kipker

An Introduction into the New Chinese Data Protection Legal Framework

Coming into effect on 1 June 2017, the Cyber Security Law of the People's Republic of China (the "CSL") established the legal foundation of cybersecurity and data protection. The purpose of the law is to protect network security, maintain cyberspace and national security, safeguard public interests, and protect the legitimate rights and interests of citizens, legal persons and other organizations.

1 Legal Systematic

Under the CSL, data security is part of the obligations of data protection, as both have to be combined to safeguard the legitimate interests of data subjects. The CSL was passed and promulgated by the Standing Committee of the 12th National People's Congress of the People's Republic of China, which determined that it is a nationally applicable law at the level of Chinese legislation. The legislative system of China is relatively complex, and the different kinds of possible regulations with legal relevance can be systematized as follows:

- Laws by the National People's Congress and its Standing Committee
- Administrative regulations by the State Council
- Local regulations, autonomous region regulations and separate regulations by the people's congresses or their standing committees of the provinces, autonomous regions and centrally administered municipalities
- Rules by the ministries and commissions of the State Council, the People's Bank of China, the State Audit Administration as well as the other organs endowed with administrative functions directly under the State Council
- Rules by the people's governments of the provinces, autonomous regions, centrally administered municipalities and the cities or autonomous prefectures divided into districts

2 Basic Legal Framework of Data Protection in China

The legislative system, the legal framework and the regulation of data protection in China is complicated. The main difference between Chinese and European Law is the fact that in China, laws have a more holistic approach and are, for this, relatively inconcrete. As a result, Chinese laws have to be concretized by sector specific rules, implementing provisions and national standards. The basic legal framework of Chinese data protection is formulated by such laws and rules, along with some national standards, as follows:

3 Important Legal Definitions of Data Protection

Unlike GDPR, the data regulatory in China aims at not only personal data area but comprehensive range of data, including State

Mr. Jihong CHEN

as a partner of Zhong Lun Law Firm, has been practicing and providing legal services for a large number of international enterprises since 1996. He has participated in the research and legislation activities of cybersecurity and data protection laws and regulations in China.
E-Mail: chenjihong@zhonglun.com

Ms. Lu HAN

as a senior associate of Zhong Lun Law Firm, specializes in the areas of privacy and data protection, cybersecurity, TMT and E-commerce.

E-Mail: hanlu@zhonglun.com:

Dr. Dennis-Kenji Kipker

Executive Director of Certavo GmbH – international compliance management, Scientific Managing Director of the IGMR at the University of Bremen, Legal Advisor of CERT@VDE, Frankfurt am Main, Member of the Board of the European Academy for Freedom of Information and Data Protection (EAID) in Berlin.
E-Mail: kipker@uni-bremen.de

Legislation Level	Authority	Specific Regulation
Law	National People's Congress of the People's Republic of China	General Rules of the Civil Law
Law	National People's Congress of the People's Republic of China	Criminal Law of the People's Republic of China (Amendment No. 7 and No. 9)
Law	Standing Committee of the National People's Congress	Tort Liability Law of People's Republic of China
Law	Standing Committee of the National People's Congress	Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (2012)
Law	Standing Committee of the National People's Congress	Law of the People's Republic of China on the Protection of Consumer Rights and Interests (2013 Amendment)
Law	Standing Committee of the National People's Congress	Cyber Security Law of the People's Republic of China ("CSL")
Rule	Cyberspace Administration of China	Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Draft, the "2017 Draft Assessment Measures")
Rule	Cyberspace Administration of China	Administrative Measures on Data Security (Draft, the "Data Security Measures")
Rule	Cyberspace Administration of China	Measures on Security Assessment for Cross-border Transfer of Personal Information (Draft, the "2019 Draft Assessment Measures")
Rule	Cyberspace Administration of China	Provisions on Cyber Protection of the Personal Information of Children (Draft)
Rule	Cyberspace Administration of China	National Cybersecurity Incident Response Plan
Implementing Provisions	Supreme People's Court and the Supreme People's Procuratorate	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
National Standard	National Information Security Standardization Technical Committee	GB/T 35273-2017 Information Security Techniques – Personal Information Security Specification
National Standard	National Information Security Standardization Technical Committee	GB/T-Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft)
National Standard	National Information Security Standardization Technical Committee	GB/T-Information security technology – Security Impact Assessment Guide of Personal Information (Draft)

Secrets, Personal Information (including Personal Sensitive Information), Important Data, and other special types of data with industry characteristics[1] such as human genetic resources, map data, etc. Compared to the European Union data protection framework with its distinction between personal data and sensitive personal data, the Chinese categories and definitions under CSL are more complex.

- **Personal Information:** Various types of information recorded in an electronic format or otherwise that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, etc. of the natural person. Coming into effect in May 2018, GB/T 35273-2017Information Security Techniques – Personal Information Security Specification (the "Personal Information Specification"), published by the National Information Security Standardization Technical Committee of China (the "ISSC"), adds additional types of information into the scope of "Personal Information": various types of information recorded in an electronic format or otherwise that can be used separately or in combination with other information to identify a specific natural person or reflect the activities of a specific natural person, such as the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, communication records and content, account password, property information, credit information, whereabouts, accommodation information, health and physiological information, transaction information of a natural person.
- **Special categories of Personal Information** may fall into the scope of Personal Sensitive Information, which is set out in Part VI of this paper.
- **Important Data:** The kind of data if divulged, may directly affect national security, economic security, social stability and public health and security, such as unpublished government information and large-scale population, genetic health, geographical or mineral resources data, while explicitly ruling out the possibility of production and operation and internal management information of an enterprise as well as personal information being considered as Important Data.
- **Personal Information Processing:** Includes the collection, storage, use, sharing, deletion, transfer of control, publicly disclosure, user profiling, personalized display etc.
- **Anonymization:** Anonymization means the process whereby personal information is technologically processed to make personal information subjects unidentifiable, and the personal information cannot be restored to its previous state once processed. Moreover, information generated from anonymized personal information is not considered personal information.
- **Personal Information Controller:** Whereas GDPR defines the "controller" as an entity which determines the purposes and means of personal data processing, and the "processor" as an entity which acts on behalf of the controller, the CSL only contains the definition of the "Personal Information Controller" as an organization or an individual who has the right to determine the purposes and means of the processing of personal information.
- **Network Operators:** This is one of the most important legal definitions of the CSL, and, compared to GDPR, a different approach. "Network Operators" can be defined as owners, administrators of the network and network service providers. The term is broadly interpreted, and as a result, any entity in China that uses computer systems connected to communications networks can be considered a Network Operator, which is in charge of being compliant with the respective data protection regulations. Under CSL, Network Operators shall fulfill a se-

1 Data with industry characteristics should be regulated by specific rules. Moreover, these data may intersect with the scope of Personal Information or Important Data. For example, part of human genetic resources will be deemed as Personal Sensitive Information, and part of map data may be deemed as Important Data.

ries of obligations which scope is much broader than data protection and data security.

- **Critical Information Infrastructure (CII):** Infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest. The CII is among the top of the State's list for protection. The CSL stipulates that operators of CII (CIIO) shall fulfill relevant special obligations in addition to complying with the cybersecurity protection obligations required of general Network Operators, which are not only for data protection and data security.
- **Collection:** The behavior of gaining the right to control personal information, including automatically collecting personal information voluntarily provided by personal information subjects, through interactions with personal information subjects or in logs concerning personal information subjects' behavior, and indirectly obtaining personal information by sharing, transferring or gathering public information or by other means.
- **Sharing:** Process where a personal information controller provides another controller with personal information, and both controllers have respective and independent rights to control personal information.
- **Public disclosure:** The act of publishing information among the general public or to unspecified groups.
- **User profiling:** The process of conducting analysis or forecasting of a natural person's personal characteristics, such as his or her occupation, financial conditions, health, education, personal preferences, credit, behavior, etc., by collecting, gathering together and analyzing personal information, in order to create a unique model of his or her personal characteristics. The act of directly using a natural person's personal information to create a unique model of his or her characteristics is considered direct user profiling, while the act of using personal information not sourced from a natural person himself or herself, such as the data concerning the group to which such natural person belongs, to create a model of his or her characteristics, is seen as indirect user profiling.

4 Principles of Personal Information Processing

The GDPR mentions several data processing principles, which are the legal basis of every use of personal data. Some of these principles can be found in Art. 5, such as the principle of legality, good faith and transparency, or the principle that personal data must be collected for defined, clear and legitimate purposes, and may not be further processed in a manner incompatible with these purposes (earmarking). Another important principle, according to GDPR, is data minimization, which might also be considered as a result of the earmarking principle, that the amount of data collection should be limited to what is necessary for the purpose of processing. Several other processing principles of GDPR include aspects related to data security, such as accuracy, memory limitation, integrity and confidentiality.

Compared to European Union Law, the CSL contains basic principles for Personal Information processing, which are quite similar to GDPR. In the CSL, it is regulated that when collecting or processing Personal Information, an entity should comply with the principles of legality, justification and necessity, publicize the rules for collection and use, clearly indicate the purposes, methods and scope of the information collection and use (the "Notice Requirement"), and obtain the consent of those from whom the information is collected (the "Consent Requirement"). Network operators are also obliged not to collect any personal information which is not related to the services provided.

Combining the above-mentioned legal principles, the Personal Information Specification puts forward seven basic principles as follows when carrying out activities to process personal information:

- **Consistency between rights and liabilities:** Network operators shall bear liabilities for any damage caused to the legal rights and interests of personal information subjects by its activities of processing personal information.
- **Clear purposes:** Purposes of processing personal information should be lawful, justified, necessary and clear.
- **Solicitation for consent:** Network operators shall explicitly specify the purposes, manners, scope and rules in respect of the processing of personal information and seek the authority and consent.
- **Minimum sufficiency:** Network operators shall merely process the minimum categories and amount of personal information necessary for achieving the purposes authorized and consented to by personal information subjects, unless otherwise agreed with personal information subjects. They shall delete the personal information in a timely manner once these purposes are achieved.
- **Openness and transparency:** Network operators shall make public the scope, purposes, rules, etc. in respect of the processing of personal information in an explicit, easily understandable and reasonable manner, and accept public oversight.
- **Guarantee of security:** Network operators shall be capable of ensuring the security of a certain degree corresponding to the security risks and take sufficient management measures and technological approaches to safeguard the confidentiality, completeness and availability of personal information.
- **Involvement of personal information subjects:** Network operators shall provide personal information subjects with opportunities to access, modify and delete their own personal information and to withdraw their consent and cancel their own account.

Obviously, the Personal Information Specification provides more detailed guidance and good practice for enterprises to improve the internal Personal Information Protection System. Since the Personal Information Specification has officially been released, it has been widely used for compliance practice in various Chinese industries. Even if the Specification is not a law, but only a national Chinese standard – especially compared to EU law, where the GDPR is already relatively concrete – it is of high importance as a reference for data protection and cybersecurity management and enforcement by authorities.

5 Legitimation for the Processing of Personal Information

The usage of Personal Information in China should meet the principles of obtaining the consent of the personal information subject, as stipulated in the CSL, supplemented by the exceptions listed in the national standard "Personal Information Specification".

5.1 Consent

Unlike GDPR, the legal basis of Personal Information collection under the CSL is entirely consent-based. Any legal grounds for the processing of personal data can only be considered as exceptions. The CSL requires the network operators to expressly notify personal information subjects about the purposes, means and scope of the collection and usage of Personal Information, and consents of personal information subjects must be obtained prior to such collection and usage. Any processing of Personal Information thereafter must be carried out within the scope of the consent. A renewed consent is required when the processing exceeds the original scope of consent.

5.2 Exceptions for Collection and Usage of Personal Information

However, in practice, network operators may refer to several exceptions listed in the Personal Information Specification which do not require consent prior to collection and usage of Personal Information. Based on a new draft revision of the Personal Information Specification, published on June 25, 2019, a personal information controller may collect and use personal information, without the need to obtain the consent from personal information subjects, under any of the following circumstances – which have certain similarities compared to the legal grounds mentioned in Art. 6 GDPR, but are more detailed:

- The collection and use are in direct relation to State security or national defense security
- The collection and use are in direct relation to the public security, public sanitation, or major public benefits
- The collection and use are in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.
- The collection and use are for the sake of safeguarding significant legal rights and interests, such as the life and property of personal information subjects or other individuals, but it is difficult to obtain their consent
- The personal information collected has been published to the general public voluntarily by the personal information subject
- The personal information controller is a news agency and the collection and use are necessary for releasing news reports in a legal manner
- The personal information is collected from information that has been legally and publicly disclosed, such as legal news reports and information published by the government
- The collection and use are necessary for signing and performing contracts as required by personal information subjects; the privacy policy should not deem as the mentioned contracts
- The collection and use are necessary for ensuring the safe and stable operation of the network operator's products or services, such as identifying and disposing of faults in products or services
- The collection and use are necessary for the personal information controller, as an institute for academic research, to have statistical programs or academic research for the sake of the general public, and it has processed the personal information, which is contained in the results of academic research or descriptions, for de-identification purposes, while announcing these results to the general public
- The processing of data is related to the Personal Information controllers' obligations stipulated by laws and regulations

5.3 Exceptions for Transfer of Personal Information

As mentioned above, the consent is the legal basis for the use of personal data under Chinese data protection law. This is especially the case for the disclosure of personal information to others, e.g. by transferring data, which is normally not possible without the prior consent of the personal information subject. Anyway, the Administrative Measures on Data Security (Draft, the "Data Security Measures") released on May 28th, 2019 by CAC, allows the transfer of personal information without a prior consent in the following cases:

- The personal information is collected through legal public channels and the provision of it is not against the willingness of the data subjects
- The personal information has voluntarily been disclosed by the data subjects
- The personal information has been subject to anonymization
- The provision of such information is necessary for the performance of responsibilities and functions of law enforcement departments in accordance with the law
- The provision of such information is necessary for safeguarding state security, social and public interest or the lives of data subjects

6 Protection of Personal Sensitive Information

Special categories of personal data have to be protected by additional legal measures. The respective regulations in European law can be found in Art. 9 GDPR, which states that the processing of such data is prohibited, unless there are special circumstances fulfilled, e.g. the data subject has given explicit consent or the processing is necessary to protect the vital interests of the data subject. In Chinese law, the "Personal Information Specification" defines Personal Sensitive Information as "the personal information that may cause harm to personal or property security, or is very likely to result in damage to an individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused", which includes identification numbers, personal biometric information, bank accounts, records and content of communications, property information, credit reference information, whereabouts and tracks, hotel accommodation information, information concerning health and physiology, information of transactions, personal information of children under the age of 14. It is obvious that the understanding of sensitive information in China is different and broader than in the EU, where special categories of personal data only encompass data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data and data concerning a natural person's sex life or sexual orientation.

In China, personal sensitive information may only be processed on the basis of an explicit consent of the personal information subject. When obtaining it, personal information controllers have to ensure that the personal information subjects declare a specific and unambiguous expression of their free will and that they are fully informed when consenting. If the Data Security Measures come into effect, network operators shall file the rules for collection and use of such data, purposes, scales, methods, scopes, types and retention periods of sensitive data at the local cyberspace ad-

ministration while collecting personal sensitive information for the purposes of business operations.

As a kind of personal sensitive information, children's data is specially protected as well. On June 1st, 2019, CAC published the "Provisions on Cyber Protection of the Personal Information of Children (Draft)", which stipulate that network operators shall seek for explicit consent from the children's guardians prior to collect or use children's personal information in the case when the minors are aged under 14. If it wants to process the personal information of minors aged 14 or older, the controller has to seek for explicit consent from the minors or their guardians.

7 Rights of Personal Information Subjects

The CSL entitles several rights of personal information subjects, supplemented by the national standard "Personal Information Specification", which are similar to the rights of the data subject that are prescribed by the GDPR in chapter 3, Art. 12 following:

- **Right to deletion**: The right of personal information subjects to require the network operator to delete the questionable data if the personal information subject finds out that the collection and use of personal data violates the laws, administrative regulations or the agreement between the personal information subject and the network operator. The network operator shall then take measures to delete the personal information.
- **Right to rectification**: The right of personal information subjects to require any network operator to make corrections if the personal information collected and stored is inaccurate or incomplete. The network operator shall then take measures to correct the error.
- **Right to access**: Personal information controllers shall provide personal information subjects with methods regarding how to access the content, categories, sources, purposes of use of personal information, and identities or categories of third parties that have obtained the personal information.
- **Right to withdrawal of consent:** Personal information controllers are required to make it possible for personal information subjects to withdraw their consent to the authorized collection and use of their personal information and to refuse to receive commercials sent on the basis of their personal information. Once the consent has been withdrawn, controllers shall no longer process the personal information concerned thereafter.
- **Right to cancellation of accounts:** If personal information controllers offer services through registered accounts, they shall make it possible for personal information subjects to cancel their own account. The method to cancel an account should be easily and conveniently feasible; and after cancellation of the account, the controller shall delete or anonymize the personal information.
- **Right to request for copies**: Personal information controllers shall, upon the request of a personal information subject, make it possible for the subject to obtain a copy of the basic information, identification information and the information about the subject's health, psychological status, education and employment, or directly transit a copy of the above categories of the subject's personal information to a third party, provided that the technology is practicable.

8 Requirements and Tasks of the Data Security Officer

As the CSL treats the data security as part of data protection as we know, the data security officer is also in charge of personal information protection and important data protection issues. The law requires that all network operators shall formulate internal security management systems and operation instructions to determine the person in charge of cyber security (including data security, data protection and other cyber security requirements) and define corresponding accountabilities. Moreover, CIIOs shall set up a dedicated security management office and designate an officer in charge of security management of CII. The Data Security Measures further provide that network operators which collect important data or personal sensitive information for the purpose of business operations shall specify the officer responsible for data security. Accordingly, the officer shall participate in important decisions of relevant data activities, and report directly and independently to the principals of the network operators, whose responsibilities and obligations regulated by the Data Security Measures are as follows:

- Organizing the formulation of data protection plans and urging the implementation of such plans
- Organizing data security risk assessments and urging rectification and elimination of potential risks of security
- Reporting data security protection and incident handling to relevant departments and cyberspace administrations as required
- Accepting and handling the complaints and reports of users

Moreover, the Personal Information Specification supplements the details of the responsibilities and obligations of personal information protection and security for the officer.

9 Emergency Responses to Data Security Incidents

The CSL requires that network operators take technical and other necessary measures to ensure the security of personal information they collect, and to protect such information from disclosure, damage or loss. In case of disclosure, damage or loss of, or possible disclosure, damage or loss of personal information, network operators shall take immediate remedies, notify the users in accordance with the relevant provisions, and report to competent authority, Art. 42 CSL. The Data Security Measures further require in Art. 35, that in case of occurrence of cybersecurity incidents, where personal information has been divulged, damaged or lost, or the risk of data security incidents has increased significantly, network operators shall forthwith take remedial measures, and inform personal information subjects in a timely manner by such means as phone calls, text messages, emails or letters, and report the cases to the competent authority of the industry and cyberspace administrations in accordance with the relevant requirements. The Personal Information Specification also contains the details regarding how to work out an emergency response plan for personal information security incidents and how to conduct the emergency responses to the personal information subjects.

10 Data Localization

The CSL requires that personal information and important data collected and generated during operations of CIIOs shall be stored within the territory of China. Where it is necessary to provide CIIOs' personal information and important data abroad due to business needs, a security assessment shall be carried out.

As an implementing act of the CSL, the 2017 Draft Assessment Measures replace the concept of CIIOs with the wider term of the network operators, which significantly expands the scope of entities to which data export restrictions may apply. It requires that every network operator, when providing personal information and important data collected and generated within the territory of the PRC to overseas, should conduct a specific data cross-border transfer assessment. Based on this broad definition, arguably, any entity in China, such as owners, managers or providers of networks or network services, could be considered a network operator, and therefore would be subject to the security assessment requirements.

Unlike GDPR, which only regulates personal data, when conducting a cross-border data transfer under Chinese law, not only personal data, but also important data shall comply with the data localization requirements. The steps of assessment which are prescribed by the Chinese data protection law are quite similar to the European specifications: Firstly, the requirements for the lawfulness of the data processing itself have to be fulfilled, and secondly, the relevant assessment shall be conducted prior to the cross-border data transfer. The first criterion requires the company to meet the notice as well as the consent requirement stipulated in the CSL. The 2017 Draft Assessment Measures (Art. 4) follow the same principles that personal information subjects shall be notified of the purpose, scope, content, receiver and the receiving country, and consent of such subjects shall be obtained prior the personal information cross-border transfer. However, the newly announced principles under the 2019 Draft Assessment Measures appear to be more flexible regarding the requirement of personal information cross-border transfer, merely requiring the notification to the personal information subjects of the basic information of the network operator and the receiver, as well as the purpose, type and storage period of the personal information to be transferred abroad. The 2019 Draft Assessment Measures also seem to set up a Chinese version of the Standard Contractual Clauses ("SCC") of GDPR, which include similar contractual regulations for cross-border data transfer. Moreover, the draft stipulates that all network operators shall apply to the local cyberspace administrations for security assessment prior to the cross-border transfer of personal information and report to the competent regulatory department for approval of the cross-border transfer of important data. At this stage, the 2019 Draft Assessment Measures are still not finalized. However, changes and shifts of the regulator's attitude are quite obvious in cross-border transfer of personal information compared with the 2017 Draft Assessment Measures.

11 Administrative Responsibility

Due to the complexity of the Chinese legislative system, the administrative authorities in charge of cybersecurity and data protection are numerous and diverse. The key supervisory structure of data protection in China are set forth below.

- **Cyberspace Administration of China (CAC)**: Coordinates cybersecurity work and related supvervisory and management tasks; supervises and manages network information security; coordinates the security protection of critical information infrastructure; supervises personal information and important data protection; coordinates the security assessment of cross-border data transfers; coordinates the collection, analysis and notification of cybersecurity information; coordinates the establishment of cybersecurity risk assessments and emergency work mechanisms; formulates contingency plans for cybersecurity incidences; organises national security reviews of network products and services.
- **Ministry of Public Security (MPS)**: Supervises the multi-level protection scheme (MLPS); supervises public and national security-related cybersecurity issues and criminal cases.
- **National Administration for the Protection of State Secrets (MSS):** Responsible for the supervision, inspection and guidance of multi-level protection related to confidentiality.

In addition to the above-mentioned unified national supervision schemes, enterprises in various industries should also be supervised separately by each competent authority in charge of the industry.

12 Conclusion and Outlook

The Chinese Data Protection Legal Framework is complex and multi-layered. A brief overview of the new regulations shows that there are many similarities of data protection under the Chinese legal framework with GDPR, but also some important differences. First, the CSL establishes the informed consent of personal data subjects as the legal basis of personal data collection. The "Personal Information Specification" as the corresponding national standard brings out several exceptions to compensate for the shortcomings of the single legal basis under the CSL. The Chinese Data Protection Legal Framework includes not only the regulations of personal data protection, but also important data and other types of data. It can be seen that the Chinese Data Protection Legal Framework shall not be considered equivalent to GDPR, which regulates personal data only. Another important difference is the regulatory distinction between data protection and data security. Under GDPR, data security is more or less just one single aspect of effective technical and organizational data protection. However, under Chinese law there are various independent cybersecurity requirements except for data security, such as the Multi-level Protection Scheme, the security review for network products and services, special requirements for critical information infrastructures, etc. In recent years, the legislation of data protection in China is active and fast-paced. Meanwhile, it can be seen that good practice in industries and enforcement actions are ahead of legislation trying to figure out the appropriate and efficient approaches for data protection in China. It is expected that China will accelerate data-related legislative activities in the coming years, and the data protection legal framework and regulatory mechanism will be enhanced and improved accordingly.