CHINA: DATA SECURITY & LOCALIZATION

BEITEN BURKHARDT

Legal provisions concerning data protection and localization requirements pertaining to personal information ("**PI**") as well as non-personal/business data can be found in various PRC laws and regulations and standards. Legislation and standards on data security and localization are developing rapidly and become more nuanced. The PRC Civil Code ("**Civil Code**") having become effective on 1 January 2021 is the most recent legislation with a focus on the protection of PI, while the PRC Cyber Security Law ("**CSL**", effective since 1 June 2017) had prioritized on general data localization/transmission/security requirements. Also the draft (i.e. not yet effective) PRC Personal Information Protection Law ("**PPI Draft**") focuses on PI protection.

Cyber Security

The CSL addresses in particular matters relating to data localization/transmission/security requirements of PI and non-personal/business data, as do several national/technical standards as well as other related laws and regulations:

1. DATA LOCALIZATION

The CSL targets all entities that qualify as "network operators" (网络运营者). In addition, further requirements apply to network operators that fall into the group of "key information infrastructure operators" (关键信息基础设施的运营者, "**KIIO**").

The CSL sets forth stipulations regarding the setup, provision, operation, maintenance and use of network infrastructure and the way data (both PI and non-personal/business data) is processed through such network infrastructure. The CSL does not grant individuals civil rights for the protection of their PI (opposed e.g. to the Civil Code or the PPI Draft).

Art. 37 CSL provides that "*PI and important business data collected and generated in the operation of KIIO within the PRC territory shall be stored within the [PRC] territory. Where it is necessary to provide such information and data to abroad due to business needs, security assessments shall be carried out according to the measures formulated by the Cyberspace Administration of China in conjunction with the relevant departments of the State Council; if there are other provisions in laws and regulations, those provisions shall prevail.*" Thus, a data localization requirement under the CSL applies if all following criteria are met:

- The data collected qualify as PI or important business data collected in China

PI Definition under the CSL: "*Various types of information 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.*"

The CSL does not define what constitutes "important business data". However, certain draft legislation related to data-security has defined "important data" as "*data closely related to national security, economic development and societal and public interests*" and further provide that "*the specific scope of the important data shall be determined with reference to relevant national standards and guidelines on important data identification*." Thus, "important business data" could e.g. be data of a certain commercial value for which one would take measures to protect them and to keep them confidential. This could e.g. entail technical information and business information which is not known to the public, which is capable of bringing economic benefits to its legal owner, which has practical applicability, and which the legal owner has taken measures to keep secret.

- Such data are necessary to be transmitted from China to abroad due to business needs

There is no business-needs-test defined under publicly available and effective Chinese law. Still, it could be reasonable to argue – until otherwise in the future a binding business-needs-test would be provided – that information collected in a business with international layout (e.g. having its headquarter outside the PRC) must from a perspective of operability, equality and fairness be able to transfer data from the headquarter to a subsidiary located in the PRC and vice versa.

- Such data are collected and generated by KIIO

In terms of who qualifies as KIIO, the CSL declares that "*the State shall carry out special protection of important industries and fields, such as public communication and information services, energy, communication, water conservation, finance, public services and e-government affairs, and key information infrastructures that may endanger national security, people's livelihood and public interest in case of damage, function loss or data leakage on the basis of graded protection system for network security*."

Protection of PI

General matters pertaining to the protection of PI are addressed in the Civil Code and detailed matters are regulated e.g. in the "Information Security Technology Standard – PI Security Specification" (《信息安全技术 个人信息安全规范》GB/T 35273-2020, "**PI Security Standard**"), a standard of relevance in this context and a benchmark for the handling of PI in the PRC.

1. RIGHT OF PRIVACY AND PI PROTECTION UNDER THE CIVIL CODE

The Civil Code grants "the right to privacy" as an individual's civil right and provides that the "PI of a natural person shall be protected by law". Other than the CSL, the Civil Code addresses individuals and thus any non-compliance therewith may lead to claims by an individual whose rights have been infringed upon by a business (or other entity/individual).

The term "privacy" is defined as "*a natural person's peaceful private life and his/her private space, private activities and private information that he/she does not wish to be known to others*". The right to privacy is protected against spying, disturbance, divulgence and disclosure.

PI is defined as "*various types of information recorded electronically or otherwise that can identify a specific natural person either alone or in combination with other information, including the natural person's name, date of birth, identity document number, biometric information, residential address, phone number, email address, health Information, location information, etc.*". In case PI contains private information, such information shall be subject to the provisions on the right to privacy as laid out above.

The term "*processing of PI*" includes the collection, storage, use, processing, transmission, provision, disclosure, etc. thereof. Thus, businesses that collect, store, use, process, transmit, disclose or provide PI to others qualify as "*data processor*" (信息处理者) under the Civil Code and there are no additional requirements to qualify as "*data processor*" (opposed to e.g. under the CSL where one needs to qualify as "*network operator*" to fall within its scope).

PI is protected against illegal collection, use, processing, transmission, trade, provision or disclosure to others. PI may only be obtained for such purpose as provided by law and shall be subject to information security standards as applicable from time to time. The Civil Code introduces lawfulness, appropriateness and necessity as general underlying principles for the processing of PI and prohibits excessive processing thereof (purpose limitation). In addition to these general principles, the processing of PI shall be subject to the following conditions:

- consent (given by the data owner or his/her guardian)
- disclosure of data processing rules
- disclosure of the purpose, method and scope of processing
- compliance with agreements between data processor and individual (if any), as well as the provisions of laws and administrative regulations

A natural person shall have the right to access PI that is processed by a data processor and raise objections/demand correction in case the processed PI is found to be erroneous. In case such natural person (data subject) finds that an information processor violates laws, administrative regulations or an agreement both parties entered into for the processing of PI, the data subject shall be entitled to request the information processor to delete the PI.

Entities that collect/store PI are prohibited from divulging/tampering therewith and shall obtain the data subject's consent prior to the transfer thereof to others. Only in case the PI is made "*unrecoverable*" (不能复原的) and no specific individual can be identified therefrom, such information may be transferred to third parties without prior consent of the data subject.

Data processors must ensure security of the PI they process by appropriate measures to prevent leaking, tampering or loss of such PI. In case of any leak, tampering or loss of PI, the data processor shall comply with certain information or reporting requirements and take remedial measures.

The Civil Code grants individuals the right to claim civil liabilities in case of infringements of their PI. Such claim however will be denied where PI

- is processed within the scope as consented by the data subject or his/her guardian
- was information already published by the data subject/other information of the data subject that has been legally published, is processed in a reasonable manner, unless the data subject has explicitly rejected such processing/the processing thereof infringes upon his/her major interests
- reasonably processed in order to protect public interests/the legitimate rights and interests of the natural person

2. PI PROTECTION UNDER THE PI SECURITY STANDARD

The PI Security Standard provides guidance on certain terms used but not otherwise defined e.g. in the CSL and the Civil Code and was formulated to "*address matters pertaining to PI controllers* ("PI Controller", 个人信息控制者) *when processing PI such as collection, storage, use, sharing, transfer, public disclosure, deletion or other activities related to the processing of PI*". "PI Controller" is defined by the PI Security Standard as "*organizations or individuals that have the ability to determine the purpose, manner, etc., of processing PI*".

The PI Security Standard not only provides definitions of key terms but also illustrative examples thereof, basic principles of PI security/collection/storage/use and entrustment thereof, data subject's rights and IT management requirements. In the following, we summarize some of the main contents of the PI Security Standard:

- Definition of PI

PI is defined as "*any information that is recorded, electronically or otherwise, that can be used alone or in combination with other information to identify a natural person or reflect the activity of a natural person*" and thus similar broadly to other PRC laws and regulations.

PI shall e.g. comprise "*the name, date of birth, ID number, personal biometric information, residential address, contact information, communication records and content, username and password, property information, credit information, records of whereabouts, accommodation information, health and physiological information, transaction information of an individual*".

Information such as user profiling, features and labeling, that results from a PI controller's processing of PI or other information that can be used alone or in combination with other information to identify a particular natural person or reflect the activity of a particular natural person, may be deemed PI.

- Purpose Limitation

The concept of "*purpose limitation*" is provided in both Civil Code and current PPI Draft in a very general manner. The PI Security Standard fleshes out this concept by requiring data controllers that offer services/products with different "business functions (业务功能)" to clearly separate these functionalities in regards to PI.

The "*business function*" shall refer to "*services offered to a PI subject such as maps/navigation services, online car hailing, instant messaging, online community, online payment, news/information, online shopping, express delivery or transport ticketing*".

Consequently, a data controller may not bundle consent for the entirety of the business functions of a product in case a data subject opts to only use/buy parts thereof (e.g. a basic product/service without all its extended functionalities), e.g. by forcing one-time consent. The use of the basic functionalities must not be affected by the refusal to consent to the use of its PI by the extended functionalities.

The use of PI for specific additional business functions requires a voluntary, affirmative action such as an active click/tick or fill-in information ("opt-in"). Upon exiting/deactivating the use of a business function ("opt-out"), no PI may be used by such function. After an opt-out, the respective business function may not actively pursue the data subject to opt-in again repeatedly. In case pooling/bundling of amassed PI is intended by the data handler e.g. for analysis purposes, consent thereto must be obtained by the data subject. Requests for the collection of PI for the purposes of raising service quality, improving user experience, developing new products or enhancing security are prohibited.

- User Profiling & Personalized Display

When creating a user profile, data controllers are prohibited from using certain characteristic descriptive features of a data subject. These features e.g. refer to obscenity, pornography, gambling, superstition or violence. A user profile may also not have any content that would constitute discrimination based on nationality, race, religion, disability, or disease. User profi-

ling in business operations may also not infringe upon the legal rights of individuals / entities or harm national security interests.

Direct user profiling may only be made if required for achieving the purpose of the consented PI use (e.g. for evaluating the financial credit status of a data subject), but not for placing commercial advertisements reflecting such status (e.g. more expensive / cheaper products, additional financing options).

In general, a data controller may use personalized display of information / search results for products / services, i.e. based on the data subject's PI such as Internet browsing history, hobbies, consumption records and habits. A data controller that opts for the use of personalized display is required to provide the option to independently adjust / control the degree of PI that is used for the personalized display. Personalized display shall be "significantly distinguished" from non-personalized display, e.g. by attaching specific marks to such display ("targeted push", 定推) or by showing it in different columns, sections etc. In case information, goods, services or search results are displayed to a data subject based on its PI, the data subject shall also have the option of a non-personalized display. More stringent requirements apply for the provision of news information services.

- IT Security Responsibilities

Under the required holistic PI security management system, "legal representatives or principals" (法定代表人或主要负责人) shall assume overall responsibility for PI security by deploying adequate human, financial and material resources. Data controllers are required to appoint a person / department in charge of PI protection, whereby the personnel shall have relevant experience in such field and be involved in all relevant PI business decisions / activities.

In any of the following cases, a full-time PI security manager shall be put in charge:

- the main business involves PI processing and the company has over 200 employees, or
- PI of over one million individuals is (expected to be) processed within 12 months, or
- sensitive PI of over one hundred thousand individuals is (expected to be) processed.

Susanne Rademacher
German Attorney-at-law | Partner
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Dr. iur. Jenna Wang-Metzner
Legal Consultant | Partner
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Simon Henke
German Attorney-at-law | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Corinna Li
Legal Consultant | LL.B. | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

Kelly Tang
Legal Consultant | LL.B. | LL.M.
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Beijing

BEIJING | BERLIN | BRUSSELS | DUSSELDORF
FRANKFURT AM MAIN | HAMBURG | MOSCOW | MUNICH

WWW.BEITENBURKHARDT.COM

01/2021