BEITEN BURKHARDT

BLOG ARTICLE

14 April 2021

China: Protection of Personal Information – Moving Closer to a Chinese GDPR?

China thus far has no comprehensive special legislation concerning the protection of personal information ("**PI**"). Only as of 1 January 2021 did the PRC Civil Code ("**Civil Code**") stipulate a chapter addressing the "Right of Privacy" and "PI Protection".

In addition, 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**", applicable since 1 October 2020) provides for a set of rules resembling in part the stipulations of the European Data Protection Regulation ("**GDPR**").

On 13 October 2020, the ”China Personal Information Protection Law (Draft)”(中华人民共和国个人信息保护法（草案）) ("**PIPL**") has been published for review. While it is not known when exactly it will come into effect, it is generally estimated this may be by end of this/early next year. The PIPL (when enacted) will be the first comprehensive law governing the protection of PI in China.

1. Scope of Application & Extraterritoriality

The material scope of application of both Civil Code and PI Security Standard mainly depend on the definition of the terms "*Personal Information*" and "*Data Handler*". In case an entity processes PI (Civil Code) and processes PI whereby qualifying as "*Data Handler*" (PI Security Standard) within the PRC, such entity falls within the scope of application. In general, this consideration also applies to the PIPL.

Term	**Civil Code**	**PI Security Standard**	**PIPL**
Personal Information	"*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,*	"*Any information that is recorded, electronically or otherwise, that can be used alone or in combination with other information to identify a natural*	*"Any type of information recorded by electronic or other means related to an identified or an identifiable natural person recorded electronically or by other means, exclud-*

	residential address, phone number, email address, health Information, location information, etc."	*person or reflect the activity of a natural person.*"	*ing anonymized information.*"
Data Handler	N/A	"*Organizations or individuals that have the ability to determine the purpose, manner, etc., of processing PI*."	"*An organization/individual that independently determines handling purposes, handling methods and other personal data handling matters*."

Neither the Civil Code nor the PI Security Standard provide stipulations in regard to extraterritorial effect. Thus, the actual presence of an individual Data Subject in the PRC is the decisive factor for the territorial scope of applicability. Further, the material scope of application is in general limited to the aforementioned activities within the PRC and similar activities by organizations outside the PRC do not fall within the scope thereof.

This would change substantially under the PIPL which extends the territorial scope to PI processing activities outside the PRC where such activities are made:

- for the purpose of providing products and/or services to individuals situated in China
- in order to analyze/assess the behavior of individuals situated in China
- in other circumstances as provided by Chinese laws and regulations (yet to be defined)

Organizations/individuals outside the PRC that fall under the scope of the PIPL must:

- set up a dedicated organization in the PRC or to appoint a representative in the PRC to handle matters related to personal data protection, and
- provide certain contact information of that organization/representative to the competent Chinese regulators

The material scope of application under the GDPR is similarly broad as under PRC laws and regulations due to similar definitions of key terms:

Term	GDPR
Personal Data	"*Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"
Data Processor/ Controller	Processor: "*A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". Controller: "*The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

The GDPR further distinguishes between Processor and Controller, while such differentiation under PRC laws, regulations and standards is rather made on the basis of individual agreements between organizations.

By implementing a "long arm" reach with its clause on extraterritorial effect, the PIPL drastically extends its scope of application and clearly resembles Article 3(2) of the GDPR that provides that the territorial scope of application covers "*the processing of personal data of Data Subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

- *the offering of goods or services, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the Union; or*
- *the monitoring of their behaviour as far as their behaviour takes place within the Union. Consistent with the GDPR, the PIPL does not apply to personal information processing conducted by a natural person for personal or family affairs.*"

Hence, with the PIPL the processing of PI under Chinese law would move significantly closer to a territorial scope of applicability as provided under the GDPR and companies located outside the PRC may become subject to the PIPL.

2. Condition for the Processing of PI & Consent

The legal basis for the processing of PI in the PRC the Civil Code, the PI Security Standard (and other PRC rules and regulations) and the PIPL requires not only consent of the Data

Subject, but also fulfillment of the following requirements:

Civil Code	PI Security Standard	PIPL
• consent (unless anonymized PI) • disclosure of data processing rules • disclosure of the purpose, method scope of processing • compliance with agreements concluded between data processor and individual (if any), as well as the provisions of laws and administrative regulations	• consent (unless anonymized PI) • security impact assessment, security measure based thereon implemented • disclosure of purpose, type, data recipient, consequences of transfer • sensitive PI: type of sensitive data, identity of recipient, data security capabilities disclosed • Specification of responsibilities of obligations of data recipient established through agreements • Set up of recordal/storage of data processing activities • Establishment of data security breach response system • Inform Data Subject of storage/use and Data Subject's rights to access, rectification, deletion and de-registration	• Consent (unless anonymized PI) • required for conclusion/performance of a contract with the Data Subject • required for the performance of statutory duties/obligations • required to respond to public health emergencies, or to protect the Data Subject's life, health and property in an emergency situation • purpose of news reporting, public opinion supervision or other acts conducted in public interest (all within reasonable scope) • other applicable situations under laws and regulations

The PIPL extends the legal basis for the processing of PI and mirrors the GDPR in this regard:

GDPR
Processing shall be lawful only if and to the extent that at least one of the following applies: 1. the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes; 2. processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; 3. processing is necessary for compliance with a legal obligation to which the controller is subject; 4. processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; 5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; 6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

In comparison to the GPDR however, there is a key difference regarding the legal basis for the processing of PI. In case of a *"legitimate interest*", the GDPR requires and assessment to establish a priority between the legitimate interests of the Data Controller/third party and the interests/fundamental rights and freedoms of the respective Data Subject. The legitimate interest basis for processing PI promotes a more flexible handling of data processing activities.

In regards to consent, the PIPL distinguishes between consent, separate consent and written consent. Further, there are certain minimum standards that Data Handlers are required to comply with in order to ensure Data Subjects are capable of providing their consent as required by the PIPL:

Civil Code	**PI Security Standard**	**PIPL**
Definition: N/A	Definition: Consent: "*Act whereby a PI subject expressly authorizes the specific*	Definition: N/A

	processing of its PI, including affirmative act (i.e. explicit consent) or through passive act (i.e. by not leaving a webpage after being informed of the collection of PI)". Explicit Consent: "*Specific, clear and voluntary expression of will based on comprehensive information*."	
Requirements: No specific requirements, entities that collect or store PI shall obtain the Data Subject's/guardian's consent prior to the transfer thereof to others, unless made "unrecoverable" (不能复原的). The term "unrecoverable" is not defined in the Civil Code but presumably would require a level of anonymization of data that makes the identification of a specific individual impossible.	Requirements: PI Controllers shall inform the Data Subject about the purpose, method, scope and other rules for collecting/using PI, obtain consent from Data Subject. Sensitive PI: Explicit consent Biometric PI: Explicit consent and specific information provided separately such as purpose, method, scope, storage time and other rules for collecting/using such biometric PI Minors aged above 14 yrs: explicit consent from minor/guardians Minors ages below 14 yrs: explicit consent from guardian	Requirements: • freely given • specific • informed • unambiguous Minimum information standards to be provided in "clear, plain language and in a prominent spot": • business identity/contact information • purpose/method of data handling, types of PI handled and retention period thereof • methods/procedures whereby Data Subject may exercise its rights under the PIPL • other matters that shall be notified as prescribed by laws/administrative regulations Separate consent, when

		processor: • provides PI to a third party • publishes PI • processes sensitive PI • transfers PI to location outside the PRC Written consent required: • as provided by law e.g. for the processing of sensitive PI

3. Cross-border Transfer of PI

Stipulations regarding transfer of PI from the PRC to abroad can currently be found in the PRC Cyber Security Law (中华人民共和国网络安全法, "**CSL**").

Also the PIPL addresses cross-border transfers of PI and also such transfers due to "business or other needs" and allows transfers thereof if the Data Handler satisfied at least one of the following conditions prior to such transfer:

- passed the security assessment organized by Cyber Administration of China ("**CAC**")
- obtained a "PI protection certification" conducted by a specialized organization in accordance with CAC provisions
- entered into an agreement with the overseas recipient regarding the rights and obligations of both parties whereby the Data Handler shall monitor the recipient's compliance with the PIPL
- complied with further requirements as set forth by the CAC

However, Data Handlers shall (i) store PI collected and generated in the PRC within the PRC and (ii) pass a prior security assessment with the CAC prior to any off-shore transmission thereof, in case a Data Handler either qualifies as Key Information Infrastructure Operator under the CSL, or handles PI up to the volume threshold yet to be prescribed by the CAC. In addition, the Data Handler shall have obtained the Data Subject's consent prior to the offshore transfer and have informed the Data Subject regarding

- overseas Data Handler's business identity/contact information
- purpose/method of data handling
- types of personal data handled
- the Data Subject's rights against the overseas recipient

Under the GDPR, PI may be transferred to a non-EU country subject to the following adequate levels of protection and appropriate safeguards:

- adequacy decision,
- standard contractual clauses ("**SCC**s") adopted by the Commission, and
- binding corporate rules ("**BCR**"),
- approved codes of conduct,
- approved certification mechanism

In the absence of any of the aforementioned protection and safeguards, PI may be transferred subject to explicit consent. The mechanism of execution of data transfer agreements under the PIPL appears to be similar to SCCs and such subject to certification by accredited institutions/organizations under the GDPR (pending further guidance, e.g. through implementing regulations). Under the PIPL, there are however no provisions regarding a code of conduct, BCRs or an adequacy decision for the purpose of data transfer to third countries. It remains to be seen how the PRC legislator will address these matters, in particular in light of the PRC government's efforts to ensure its goal of "*Cyber Sovereignty*" which is also reflected in the rather restrictive stipulations set forth under the CSL.

4. Liabilities

The Civil Code grants individuals in their capacity as natural person the right to claim liabilities in case their right to the protection of PI is infringed upon by a business qualifying as "*data processor*". Hence, there is a clear basis for individuals to take legal action against data processors in case of infringements of their privacy rights. However, there are no specific administrative penalties for certain infringements mirroring those of the GDPR.

The PIPL sets forth different type of liabilities in case of non-compliance with the requirements thereunder. These liabilities depend on the extent of the infringement and may in severe cases trigger fines of up to RMB 50 million or 5 % of the infringer's annual turnover of the preceding financial year. In addition, also the infringer's business license can be ordered to be suspended or revoked. Further, persons in charge (legal representatives, senior management, data security managers, etc.) may be subject to fines of between RMB 100,000 to RMB 1 million. Also, any infringement will be recorded in the enterprise social credit system.

5. Conclusion

With the PIPL, China moves ahead in the protection of PI, streamlining it with international benchmarks while maintaining Chinese characteristics that reflect the importance China attributes to maintaining control over data flows, in particular those being made cross-border.

For the time being the PIPL is only a draft and hence in the final version some provisions may still be subject to change in the next stage(s) of the drafting process. Hence, business operators in China and those outside China but dealing with China shall monitor the related legislative developments to keep updated and prepared when the final PIPL is promulgated. Even considering the remaining uncertainties of the final promulgation of the PIPL, one may say that business operators already satisfying the GDPR standards will likely be in a good position to also comply with the final PIPL stipulations.

Susanne Rademacher

Simon Henke