CRi
Computer Law Review International
A Journal of Information Law and Technology

Articles

Daniel Albrecht

Chinese first Personal Information Protection Law in contrast to the European GDPR

Greater challenges for foreign companies managing personal information protection risks

The development of big data brings convenience to life but also breeds chaos. The first personal information protection law of PRC was designed to curb collection of excessive personal information and its misuse, which is often a subject of complaints, the law seeks to ensure users' knowledge and consent when their personal data is collected and processed. This article compares relevant regulations of the PIPL with the GDPR with regard to 13 different aspects. From the comparison, we can see that most regulations in the PIPL are similar to those in the GDPR, especially in the context of general processing principles and data subject's rights. But there are still some differences at other aspects, such as cross-border data transfer rules.

I. Overview

1. Introduction of PIPL

1 On August 20, 2021, the first Personal Information Protection Law of the People's Republic of China (PIPL) has been issued and took already effect on November 1, 2021. This law not only shows China's extremely serious attitude on personal information protection, but also serves as the bridge for international digital cooperation.

2 The PIPL, regarded as China's version of the GDPR[1], lays out a comprehensive set of rules for how business operators should collect, use, process, share and transfer personal information in China. The GDPR strives to align the laws of the EU Member States, although it leaves some options at the discretion of the national legislatures. It aims to balance the protection of personal data with the free flow of data. Although bearing a resemblance to the GDPR and other recent privacy legislation in major jurisdictions in some important areas, the law introduces several provisions that are consistent with recent trends in other Chinese laws in the areas of data and technology, such as the Data Security Law and the newly enacted Export Control Law. These include, for example, rules establishing extraterritoriality of the Draft Law and a "blacklist" that would restrict or prohibit listed foreign organizations from receiving personal information from China. Unlike the fundamental rights-oriented protection of the GDPR, the Chinese regulations mostly evolved within a security context, making the safety of persons and property the main criterion.

1 Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. The General Data Protection Regulation (GDPR) is the latest version of Europe's cornerstone data protection law. It became applicable in May 2018.

2. Interaction of PIPL with the Cybersecurity Law and the Data Security Law

3 Additionally, this Law, once enacted, will work together with the Cybersecurity Law and the Data Security Law to establish a broader regulatory framework related to data. As such, much is to be seen in the next few years on how these laws will interact and how the government agencies will be dividing their roles and responsibilities with respect to these laws.

3. Differences between the PIPL and the GDPR

4 There are nevertheless certain marked differences between the PIPL and the GDPR on notification requirements. For example, in contrast to the GDPR the legal bases for processing personal information, although set out in Art. 13 of PIPL, are – according to PIPL – not required to be expressly spelt out in a privacy policy.[2] Another example includes the following: the PIPL requires a Personal Information processor to specify expressly the retention period. A retention period of personal information shall be the shortest time necessary to achieve the processing purpose, except as otherwise provided by any law or administrative regulation. Unlike Art. 13 II a) of the GDPR which allows a data controller to specify the criteria used to determine the retention period if it is not possible to pre-determine the retention period, there is no such equivalent provision in the PIPL.[3] The PIPL further supplements the existing data protection regime previously established by the Cybersecurity Law (CSL)[4] and national guidelines, and it provides another pillar in China's efforts to regulate how companies use data and to further protect the personal data of its citizens.[5]

II. Personal Information/Sensitive Personal Information, Art. 4 PIPL

1. Personal Information

5 The PIPL defines "personal information" as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person, excluding information that has been anonymized" (Art. 4 PIPL). This definition clearly specifies that anonymized information does not classify as personal information, however there is no relevant stipulation under the GDPR. Other parts largely align with the term "personal data" under the GDPR, which is broadly defined as "any information relating to an identified or identifiable natural person.[6]"

2. Sensitive personal information

6 The Law defines "sensitive personal information" as "personal information whose leakage or unlawful use may lead to discriminatory treatment or serious damage to personal or property safety, including race, ethnicity, religious beliefs, personal biometrics, medical health information, financial accounts, and personal whereabouts" (Art. 29 PIPL).[7] This definition, by contrast, does not neatly align with the GDPR's equivalent concept of "special" personal data, which focuses on data categories. As a result, GDPR identifies some additional categories of data as "special" personal data but excludes some categories listed in the PIPL.

3. Real-name registration

7 A special Chinese obligation without a counterpart in the GDPR is real-name registration, which has already existed extensively in many fields for more than a decade.[8] It is given broad coverage by Art. 6 and Art. 24 I CSL, which oblige controllers that provide network access or other services to "require users to provide identity information" and otherwise not to offer services to them.[9]

III. Processing of Personal Information Art. 4, Art. 69 PIPL

8 Processing must be fair. This principle of "good faith" is included in the PIPL. The Law imposes personal information protection obligations on parties acting as a "personal information processing entity," which is an "organization or individual that independently determines the purposes and means for processing of personal information" (Art. 69 PIPL). This appears to be the Chinese law equivalent of the "data controller" concept mentioned in GB/T 35273-2020 and EU GDPR, who has the right to make independent decisions on personal information processing activities. "Processing" is defined in Art. 4. The PIPL includes this legal basis of the data processing: consent; response to a public health emergency, or in an emergency to protect the safety of natural persons' health and property; compliance with legal responsibilities or obligations; processing personal information that is already made public within the reasonable scope and in accordance with the requirements of the PIPL; for purposes of carrying out news reporting and public opinion monitoring for public interests; and other circumstances permitted by laws and regulations. It remains unclear what "separate" consent means in practice. For now, it appears to suggest organisations should avoid bundled or forced consent to such activities, especially on app interfaces.

IV. Data subject's Rights Art. 44–Art. 50 PIPL

9 The rights of the data subjects are regulated in Art. 44–Art. 50 PIPL These rights include the right to know (Art. 44), the right to decide (Art. 44), the right to restrict (Art. 44), the right to

2 Personal Data Regulation in China, China Briefing, Alexander Chipman Koty, May 13, 2021.

3 China Draft Personal Information Protection Law: Deep Dive (3): Individual Rights; Michelle Chan, Clarice Yue, John Shi, Sven-Michael Werner; 11-2020.

4 Hacking into China's Cybersecurity Law, Wake Forest L Rev 57, Jyh-An Lee, 2018.

5 Personal Information Protection Law: CHINA'S GDPR is coming, Todd Liao/K Lesli Ligorner/W. Reece Hirsch/Gregory T. Parks/Paulina Whitaker/Yuting Zhu, August 24, 2021.

6 In the EU, this broad definition, and the extensive interpretation of personal data by the Court of Justice of the European Union makes non-personal data increasingly rare, see Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 41 f., 44, 61–72, 77 f.

7 Overview of Draft Personal Information Protection Law in China, KPMG, Henry Shek/Richard Zhang/Brian Cheung/Quin Huang/Danny Hao/Rocky Wu.

8 Feng (n 1) 74; Qi, Shao, and Zheng (n 28) 1347; Ma and Roth (n 2) 358.

9 Real-Name Registration Rules and the Fading Digital Anonymity in China, Jyh-An Lee/Ching-Yi Liu, 2016.

refuse (Art. 44), the right to consult duplicate, data portability (Art. 45), the right to supplement (Art. 46), the right to correct (Art. 46) and the right to delete (Art. 47).

10 According to Art. 12 to Art. 23 GDPR, there are a series of rights related to data subjects, including the right to know, to decide, to restrict, to refuse, to consult, to duplicate, to supplement, to correct, to delete and the right to data portability. The types of rights granted to data subject by PIPL are basically the same, except for some restrictions on the exercise of rights and the content of some rights.

11 For example, pursuant to Art. 44 PIPL, individuals have the right to restrict or refuse the processing of their personal information by others, except as otherwise provided by any law or administrative regulation, which leaves much room to limit the scope of the right to refuse or restrict their personal information processing given the last sentence. GDPR distinguishes between market-oriented utilization and non-profit utilization and makes it clear that data subjects have the right to refuse even if their personal information is used for non-profit purposes, except for utilization in the public interest.

12 The "right to delete" according to GDPR also includes the content of the right to be forgotten, but there are great controversies about the right to be forgotten at home and abroad, which is not stipulated in China's PIPL.

V. Extra-territorial Effect, Art. 3, Art. 53 PIPL

1. Art. 3 PIPL

13 According to Art. 3 the PIPL extends its territorial scope to the processing of personal information conducted outside of China, provided that the purpose of the processing is to provide products or services to individuals in China, to "analyse" or "assess" the behaviour of individuals in China, or for other purposes to be specified by laws and regulations. These criteria are strikingly similar to the territorial scope provisions found in Art. 3 of the GDPR[10], but without the limiting effects of the GDPR's recitals and EU common law.[11] It appears that this approach is incorporated into the PIPL to ensure the Chinese government can enforce these rules against parties anywhere in the world who are targeting their goods and services to consumers in the Chinese market, or otherwise analysing or assessing the behaviour of individuals in China.

2. Art. 53 PIPL

14 Moreover, Art. 53 of the PIPL requires offshore processing entities that process personal information of Chinese individuals to establish a "dedicated office" or appoint a "representative" in China to be responsible for personal information protection in China. This appears to be Data Privacy and Cybersecurity like the GDPR's requirement for the appointment of an "EU representative" under Art. 27 PIPL.[12]

VI. Cross-border data transfer rules, Art. 38 PIPL

15 Concerning cross-border transfers of personal data, Art. 44–50 GDPR require an adequacy decision from the Commission concerning the level of data protection in the third country or other safeguards such as binding corporate rules or approved codes of conduct.[13]

16 The PIPL classifies the cross-border of personal information into two categories: one for critical information infrastructure operators and the personal information processors that process personal information reaching the threshold and the other one for common personal information processors. Personal information collected and generated by the first category shall be stored in China. If it is truly necessary to provide information to an overseas recipient, the security assessment organized by the national cyberspace administration shall be passed.

17 Personal information collected and generated by the second categorycan transfer overseas only if one of the following criteria is fulfilled: the organisation has passed a CAC security evaluation; the organisation has obtained certification from a CAC-accredited agency; the organisation has put in place CAC standard contractual clauses (not yet published) with the data recipient; or for compliance with laws and regulations or other requirements imposed by the CAC.

VII. Data governance, Art. 59 PIPL

18 Art. 59 of the PIPL obliges the "entrusted parties", i.e., those who are commissioned by Personal Information processors to process personal data, like "data processors" within the meaning of the GDPR, to take the necessary protective measures to transfer the personal data to the PIPL protection.

19 Although the processing of personal data in the public sector is generally permitted, it cannot take place without restrictions. Rather, it must be carried out to an "appropriate extent" and in accordance with the PIPL.

20 Data controllers must not provide personal information stored within China to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority. This aligns with a similar provision in the new Data Security Law. It remains unclear whether this extends to the requests from overseas industry regulators. Chinese authorities may provide personal information stored within China to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.

21 By adding specific references to the employer's "work order" (劳动规章制度) as well as "collective agreements" (集体合同), employers now have a solid legal basis to rely on when processing personal data in the employment context.

10 The Right to Be Forgotten is Taking Shape: CJEU Judgments in *GC and Others* (C-136/17), GRUR International 380, 385–388.

11 GDPR, Art 3. Concerning the interpretation of this norm, Case C-507/17 *Google v CNIL*.

12 China Releases First Draft of Personal Information Protection Law, October 23, 2020; Covington; Yan Luo/Daniel Cooper/Tim Stratford/Eri Carlson.

13 Case C-311/18, ECLI:EU:C:2020:559 – *Facebook Ireland and Schrems*.

VIII. Data Protection Compliance Audits and Certification, Art. 53 PIPL

22 Personal Information Processors should note the specific circumstances when Data Protection Compliance Audits are required and must also put in place a process for conducting regular data protection compliance audits. There are different references to promoting the provision of certification services by professionals, this is currently only limited in the context of cross border data transfers.[14]

23 Separate from this, the PIPL requires data protection audits to be conducted after implementation of data processing activities, on a regular basis. This is consistent with the current audit requirement under the Personal Information National Standard. There is currently no specific guidance on how frequent the audits would need to be conducted to satisfy the requirement of conducting the audit on a "regular basis". In addition, data protection audits are not limited to only specific types of processing activities but to all data processing activities of a Personal Information Processor in general.

IX. Data Protection Officer, Art. 52 PIPL

24 Furthermore – and like the GDPR[15] – a data protection officer (DPO) could also be required according to Art. 52 of the PIPL. This would depend on the quantity of personal information to be processed; the exact threshold involved would be determined by the respective data protection regulator, which could potentially refer to existing industrial standards. In contrast to the DPO requirement under the GDPR, the PIPL restricts the application scope only to certain companies – i.e., those that will process personal information exceeding a yet-to-be-announced amount threshold designated by the CAC.[16] Unlike the GDPR, some regulations contain a more general duty to appoint a data protection officer. On the other hand, there is mostly no mention of independence, and the tasks are less well described.[17] Details of the DPO should be published and registered with the data protection authority.

X. Data Protection Impact Assessments, Art. 55 PIPL

25 The PIPL also regulates the requirements under the existing non-binding national standards for the protection of personal data (the "National Standards of Personal Information") with regard to the acceptance of data protection impact assessments ("DPIA") under certain specific circumstances. Like the GDPR, the PIPL aims to evaluate, identify, and minimize non-compliance risks. The GDPR provides for a DPIA to be carried out prior to "high risk" processing operations.

26 Personal Information processors are obliged to carry out a DPIA: before the processing of sensitive personal data takes place; when using personal data for automated decision-making, which includes profiling the behaviour of individuals; prior to the appointment of third-party processors for the processing of personal data; before the transfer of personal data to third parties or the public and before the transfer of personal data abroad.

27 Unlike the GDPR, the PIPL provides no mechanism for consulting the data protection authority prior to the start of data processing, which involves a high level of unconstrained risk, but Personal Information processors are required to keep records of the DPIA along with records of these related processing activities and these are to be kept for at least three years.

XI. Data breach/incident notification, Art. 57 PIPL

28 Unlike Art. 33 I, III, Art. 34 I, III GDPR, the newer draft of Chinese provisions contains obligations to provide timely information to competent authorities and information subjects whenever data breaches occur and not only if it is likely to result in a high risk to the rights and freedoms of natural persons. In the event of a data breach, the Law requires processing entities to take "immediate" remediation actions and notify the Competent Agency, as well as the affected individuals. The text itself does not provide a time limit like the GDPR's 72-hour benchmark.[18] This notification should include the following: types, reasons, and possible harms from the personal information leakage, tampering, or loss that occurred or may occur; remedial measures taken by the Data Controller and measures that data subjects can take to reduce harm; and contact information of the Data Controller.

29 However, while notifying the authority is required, notification to data subjects is not mandatory if the Data Controller is able to take measures to effectively avoid damage caused by the data leakage, tampering or loss. If the authority believes that it may cause harm, it still can request the Data Controller to notify the data subjects. Other than the general requirement of "immediate" notification, the PIPL does not provide specific timing for notifying the authority or data subjects.

XII. Specific obligations on "Large" Internet Platform Providers

30 More like the GDPR but still less concrete, Art. 58 PIPL stipulates those self-regulatory norms by non-State organs "shall have the same effect as this Law if they meet the standards of this Law and are approved by the competent authorities." However, there is yet no enacted provision resembling Art. 41 GDPR that gives the possibility to legally enforce or monitor self-regulatory regulations, which weakens the power of the Chinese measures.[19]

31 Besides that, the PIPL introduces a broad requirement on internet platform providers that processes "large" volume of user data with "complicated" business operations to comply with additional obligations to set up an external and independent organisation to monitor data processing activities, to regularly

14 Greenleaf, Data Privacy (n 3) 208.

15 Art. 37 I GDPR: a data protection officer is obligatory if 'the processing is carried out by a public authority or body' or when the 'core activities' involve data subjects or sensitive data on a large scale.

16 Personal Information Protection Law: China's GDPR is coming, August 24, 2021. Todd Liao/K. Lesli Ligorner/W. Reece Hirsch/Gregory T. Parks/Pulina Whitaker/Yuting Zhu.

17 How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective, Anja Geller, September 20, 2020.

18 China Releases First Draft of Personal Information Protection Law, October 23, 2020; Covington; Yan Luo/Daniel Cooper/Tim Stratford/Eri Carlson.

19 Ma and Roth (n 2) 356; Zhu (n 78) 108, 114.

publicise reports on personal information protection and to terminate their services to specific product or service providers that seriously breach relevant laws and regulations on protection of personal information. These additional measures appear to require such internet platform providers to demonstrate social responsibility by monitoring the data protection compliance of the users of their platforms, but further guidance will be required on what constitutes "large" volume of user data and "complicated" business operations. This applies to companies that are "foundational internet platforms", have many users, or have complex operational models.

32 While it is not exactly clear as to what types of companies the PIPL applies to, its provisions appear to target internet, social media and artificial intelligence giants like Alibaba, Baidu and Tencent – all of whom handle vast amounts of private information.

XIII. Liabilities, Art. 66 PIPL

33 Recognition of the GDPR[20] is largely attributable to the high penalties it empowers the various law enforcement agencies in Europe to impose. Especially for cases not covered by Art. 83 GDPR, Member States are required to establish criminal or administrative sanctions that are "effective, proportionate and dissuasive".[21] By contrast, similar serious legal consequences have been historically absent from Chinese data protection laws – something the PIPL addresses. Art. 66 PIPL introduces many more severe administrative penalties.[22] Non-compliance with the PIPL may lead to administrative fines of up to 5 % of the annual turnover or RMB 50 million and persons directly responsible may also be subject to fines from RMB 100,000 to 1 million and more significantly, such persons may be prohibited from assuming managerial positions in relevant organisations for a certain period of time.

34 Compared with corporate-level legal consequences under existing laws (e.g., up to RMB 1 million under the CSL) these legal consequences, including possible class action, present a markedly more compelling deterrent and should be effective in curbing abuse of personal information. The penalty equivalent to 5 % of annual turnover is even higher than that the GDPR ceiling at 4 % (alternative 10 million or 20 million EUR)[23], substantially increasing the compliance exposure of data-rich businesses.[24]

35 Beside this, the PIPL provides a range of sanctions, including suspension of apps and/or services, suspension of business, suspension of management, and criminal sanctions (for certain offences, and under relevant criminal laws and social credit score or equivalent business credit files may be affected).[25]

36 The right of appeal against administrative acts in China is most likely not sufficient to exclude disproportionate sanctions.[26]

XIV. Conclusion

37 The current relatively complex compliance landscape brings greater challenges on how companies can effectively manage personal information protection risks, especially how to consider personal information protection in the process of digital transformation and the application of new technologies such as big data, so as to ensure business development and expansion.[27] Unfortunately, the new regulations still do not clarify the important question of local data storage. The PIPL uses the term "personal information" which only slightly deviates from the term "personal data" used under the GDPR, and it has a similar definition and very broad coverage as its GDPR counterpart. Moreover, there is a special provision under the PIPL regulating the concept of "sensitive personal information" which like the GDPR would only allow processing for very limited and specific purposes while still subject to sufficient necessity to process, as well as requiring a separate/written consent from the data subject. The general processing principles under the PIPL could also find respective equivalents under the GDPR (such as legitimacy, purpose limitation, data minimisation, transparency).

Attorney at law Daniel Albrecht

Managing Counsel at Starke IP, Beijing

Corporate Law, Trademark Law, E-Commerce

law@starke-ip.com

www.starke-ip.com

20 According to Art. 83 I, III, Art. 58 II, GDPR, administrative fines imposed by the supervisory authorities shall be 'effective, proportionate and dissuasive'. They can be imposed in addition to warnings, reprimands, temporary or definitive limitations including processing bans, withdrawal of certifications or the suspension of data flows to third countries.

21 GDPR, Art. 83 II, Art. 58 II.

22 China's GDPR – What you need to know about the Personal Information Protection Law, Lexology, Michael Tan, December 15, 2020.

23 GDPR, Art. 83 IV, V, VI.

24 Squire Patton Boggs (n 29) 3.

25 PIPL has finally arrived, bringing helpful clarification (rather than substantial change) to China's data privacy framework, DLA Piper's Global Privacy and Data Protection Resource, August 23, 2021.

26 Greenleaf, Data Privacy (n 3) 220; e.g., Consumer Protection Law, art 59.

27 Overview of Draft Personal Information Protection Law in China, KPMG, Henry Shek/Richard Zhang/Brian Cheung/Quin Huang/Danny Hao/Rocky Wu.