18 May 2021

Comments by the Centre for Information Policy Leadership on China's Updated Draft Personal Information Protection Law

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to provide comments to the Standing Committee of the National People's Congress (NPC) of the People's Republic of China on the updated version of its Draft Personal Information Protection Law (PIPL).

CIPL previously provided comments to the NPC on the initial draft of the PIPL in November 2020.[2] CIPL stands by those recommendations, many of which are still relevant and applicable to the updated PIPL. CIPL strongly recommends that the NPC revisit our previous comments as it further revises the PIPL and notes that our comments below on the updated PIPL do not override our earlier comments on the issues we are addressing below. A copy of our earlier comments can be found here: https://bit.ly/3exVWo8 (Mandarin) https://bit.ly/2Sv2zir (English). In particular, CIPL recommends that the NPC specifically consider our previous recommendations around legal bases for processing; children's and sensitive personal information processing; clarifying the role of third party service providers in relation to personal information processors[3]; international transfers of personal information (including alignment with the APEC Privacy Framework and APEC Cross-Border Privacy Rules (CBPR)); appointment of an information protection officer and representative in China; breach notification rules; and penalties for non-compliance.

CIPL welcomes this initiative to create a robust system of data protection in China in conjunction with China's Cybersecurity Law and Draft Data Security Law. CIPL commends the NPC on many of the updates it has made to the initial draft of the PIPL following the first public consultation on this law. For example, CIPL appreciates that the NPC has clarified that the concept of purpose limitation necessitates limiting processing in ways that ensure minimum impact to individual rights. Moreover, CIPL appreciates that the NPC has specified that where an individual withdraws consent to processing, such withdrawal shall not

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] See CIPL Comments on China's Draft Personal Information Protection Law, 18 November 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/%E5%85%B3%E4%BA%8E%E4%B8%AD%E5%9B%BD%E3%80%8A%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95%EF%BC%88%E8%8D%89%E6%A1%88%EF%BC%89%E3%80%8B%E7%9A%84%E7%AB%8B%E6%B3%95%E5%BB%BA%E8%AE%AE_-_cipl%E6%8F%90%E4%BA%A4.pdf (in Mandarin) and https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_chinas_draft_personal_information_protection_law__18_november_2020_-_english_.pdf (in English).

[3] In many privacy laws, the "personal information processor", as understood under the PIPL, is known as a "data controller" and "third party service providers" are often referred to as "data processors". CIPL recommends that the NPC adopt these globally accepted terms in the PIPL to ensure consistency domestically (e.g. the Personal Information Security Specification (Information security technology – Personal information security specification, National Standard of the People's Republic of China, GB/T 35273-2020) refers to a "personal information controller") and globally as Chinese organizations interact in the global data economy.

affect processing activities that have taken place prior to the withdrawal. These changes and additions to the PIPL will add certainty for domestic and international organizations seeking to comply with the law and ensure that the Cyberspace Administration of China (CAC) has more clarity on the scope and parameters of the PIPL for carrying out its data protection activities.

In this response, CIPL reiterates several of its previous recommendations which it believes are of critical importance to ensuring an effective privacy law that is in line with global norms of data protection. CIPL also highlights several new considerations that the NPC should take into account as it continues to work on the PIPL. CIPL believes that by adopting the below recommendations, China will better position itself as a global leader in the digital economy while upholding a high standard of data protection for data subjects and ensuring the appropriate protection of private and public sector data.[4]

1. Providing further clarity on when consent is required under the PIPL

Article 13 of the PIPL sets forth several legal grounds for processing personal information, including consent, contractual necessity, compliance with statutory obligations or responsibilities, responding to public health emergencies or for the protection of life, health or property in emergency situations, news reporting and other circumstances as stipulated by laws and administrative regulations. CIPL welcomes the introduction of an additional legal ground in this revised version of the PIPL to process publicly available personal information within a reasonable scope.

CIPL also welcomes that the revised version of the PIPL states that while other relevant provisions of the law stipulate that the processing of personal information shall require consent of individuals, consent is not required for circumstances stipulated in Article 13(2) – 13(7). It would be helpful if the NPC made a cross-reference to this clarification in other provisions of the PIPL that require consent for specific processing. For instance, under Article 39 of the PIPL, if a personal information processor is transferring personal information overseas, it must obtain the separate consent of individuals, in addition to utilizing one of the relevant transfer mechanisms outlined under Article 38. However, if the transfer of personal information overseas is essential for entering into or performing a contract, it would appear that such a transfer could take place without the need to obtain consent given that circumstances stipulated under Article 13(2) would apply in this scenario.

Recommendation: Cross-reference the fact that consent is not required for circumstances stipulated in Article 13(2) – 13(7) in other provisions of the PIPL that require consent for specific processing activities to make clear that such consent is only required in the absence of an alternative legal basis for processing.

2. Providing further clarity on the impact of withdrawing consent

As noted above, CIPL appreciates that the NPC has clarified that where an individual withdraws consent to processing, such withdrawal shall not affect processing activities that have taken place prior to the withdrawal. CIPL recommends that the NPC further clarify that for certain forms of ongoing processing which rely on the integrity of datasets, such as in the case of medical research that has already

[4] Please note that the comments in this submission are based on two unofficial translations of the Personal Information Protection Law. It is possible that, as a result, we may have misunderstood the particular intent or nuance of certain issues. To the extent this is true for any particular comment, please disregard that portion of this submission.

commenced prior to the withdrawal of consent, the withdrawal of consent shall not affect such ongoing processing either.

Recommendation: Clarify that withdrawal of consent does not affect certain ongoing forms processing that rely on the integrity of datasets and to which an individual initially provided consent (e.g. processing data for medical research that has already commenced).

3. Adding a legitimate interest processing ground

CIPL believes that the PIPL would benefit from the addition of a legitimate interest style processing ground to ensure that routine and common personal information processing which does not neatly fit within the other available processing grounds, and where consent may be impracticable, not feasible or ineffective, may still take place in China. For example, processing information for network and information security; to detect, prevent or investigate fraud or crimes; for employee data processing; to personalize online content; and to enable the use of data for social good and the benefit of society.

Legitimate interest or processing grounds that are similar in nature are becoming a hallmark of many modern day privacy laws. For example, the EU GDPR, the Brazil LGPD and the recently amended Singapore PDPA all include a legitimate interest ground for processing. [5]

Adding legitimate interest in the PIPL would require the personal information processor to conduct a balancing test or assessment to demonstrate that it or a third party has a legitimate interest to process the personal information and that these interests are not overridden by the rights of the data subject. Such a balancing assessment must also be demonstrable to privacy enforcement authorities, such as the CAC. By engaging in such balancing assessments, organizations can ensure appropriate risk-based prioritization of mitigations and controls and more effective data protection based on actual risk.

A narrower and less flexible form of the legitimate interest processing ground can be found in India's proposed Personal Data Protection Bill.[6] The "reasonable purposes" ground enables processing of personal information without obtaining consent if such processing is necessary for reasonable purposes as may be specified by regulations, after taking into account multiple factors, including whether the personal information processor can reasonably be expected to obtain the consent of the individual. To the extent that China decides not to include a legitimate interest ground for processing in the PIPL, this may be a useful, though less flexible and less protective alternative to consider.

Recommendation: Given its increasing use in data protection laws globally and its utility in ensuring that many forms of processing operations not covered by other legal grounds can still take place, CIPL recommends that the NPC include a legitimate interest ground for processing in the next version of the PIPL.

[5] See Article 6(1)(f) GDPR; Article 7(IX) of the Brazil LGPD; and First Schedule, Part 3 of the Singapore Personal Data Protection (Amendment) Act 2020.
[6] See Section 14 of the India Personal Data Protection Bill 2019.

4. Enabling a risk-based approach to determining whether an organization is processing the personal information of minors in the context of mixed audience websites

The revised PIPL requires a personal information processor that processes the personal information of a minor under the age of 14 to obtain consent of the parents or guardians of the minor. CIPL encourages the NPC to enable a risk-based approach for organizations to determine whether they are processing personal information of minors in the context of mixed audience websites. Such an approach can include considering factors such as the nature of the online service/product offered, the accessibility of the service, the potential attractiveness of the service to children and whether children have been attracted to similar or competing services, whether the registration process for a website/service reflects an assumption that users are above the age of 14, etc.[7] This would enable the processing of personal information on such mixed audience platforms/sites without the need to verify the age of every single user, which could raise significant data protection and data minimization concerns. Of course, for websites and platforms clearly directed to children, an organization would be required to obtain parental consent to process the data of every child using the service.

Recommendation: Enable personal information processors to make a contextual determination based on a number of factors to determine whether they are processing the personal information of minors in order to meet the requirements of Article 15 for mixed audience websites and services.

5. Revising some aspects of the international data transfers provisions

As a preliminary point, CIPL believes that the NPC should reinstate the general goal of safeguarding the orderly and free flow of personal information under Article 1 of the PIPL. China is an APEC Member Economy, and has helped develop and endorsed the APEC Privacy Framework and the APEC Cross-Border Privacy Rules system. One of the core objectives of the APEC Privacy Framework is to ensure the free flow of data in the Asia-Pacific region and to promote "effective privacy protections that avoid barriers to information flows".[8] CIPL understands that there may be governmental, public interest and security concerns surrounding the international transfer of some forms of personal information outside of China (e.g. highly sensitive personal information related to national security interests). However, enabling the responsible and safe transfer of personal information across borders is essential to a successful and robust digital economy. Furthermore, the PIPL has built in stringent protections concerning the cross-border transfer of personal information outside of China which will address many of the existing concerns. As such, CIPL believes that the NPC should still acknowledge the need for the orderly and free flow of personal information as an overarching objective of the PIPL.

---

[7] A similar approach is followed in the United States. See Complying with COPPA: Frequently Asked Questions, Websites and Online Services Directed to Children, including Mixed Audience Sites and Services, available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions. See also CIPL White Paper on GDPR Implementation in Respect of Children's Data and Consent for a discussion on how such an approach could work, 6 March 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf.

[8] See, for example, APEC Privacy Framework at Foreword and Preamble, paragraph 4, available at https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.

The PIPL recognizes that personal information may need to be transferred overseas for business needs. Such transfers are permissible if certain conditions are met, including the signing of a contract with overseas receiving parties that stipulates the rights and obligations of the sending and receiving parties. The revised version of the PIPL specifies that a standard contract will be formulated by the CAC for such transfers. CIPL recommends that in formulating any model contract, the CAC take account of similar contracts globally, including the ASEAN Model Contractual Clauses for Cross Border Data Flows,[9] as well as the upcoming revised Standard Contractual Clauses that are due to be published shortly by the European Commission. Doing so will ensure that any model contracts for transfers produced by the CAC are in line with existing approaches to model contracts for transfers. CIPL believes that such contracts should be designed in a way that facilitates flexibility for the contracting parties to customize the agreement depending on the context of the transfer as well as the overall business relationship between the entities.

Additionally, CIPL wishes to reiterate several of the recommendations it previously made with respect to international data transfers in its initial comments on the PIPL:

- The CAC should clarify for organizations what is involved in order to pass the security assessment that would enable the cross-border transfer of personal information;

- The NPC should clarify the scope of supervision required to ensure that an overseas recipient of personal information from China meets the standards of protection enumerated in the PIPL. This could be achieved by way of guidance by the CAC stipulating that such supervision includes conducting due diligence before entering into the model contract with the overseas recipient, delineating the purpose for the transfer in the contract and taking appropriate action if the recipient is in breach of its contractual obligations.

- The NPC should add codes of conduct and corporate rules to the available transfer mechanisms listed in the PIPL.

- The NPC should remove the requirement to obtain consent on top of the other transfer requirements outlined in the PIPL. CIPL has previously provided extensive comments to the NPC as to why such an approach is problematic for organizations and not in line with global norms of data protection.

- China has endorsed the APEC Cross-Border Privacy Rules (CBPR) system[10] in 2011 and, as an APEC economy, would be eligible to seek active participation in this cross-border transfer certification. CIPL encourages China to work towards joining the CBPR system and recommends that the NPC clarify that undertaking personal information protection certification for purposes of transferring

[9] ASEAN Model Contractual Clauses for Cross Border Data Flows, available at https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
[10] APEC CBPR, available at https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf.

data overseas for business needs could include APEC CBPR[11] certification if China were to join the system.

Recommendation: Reinstate the general goal of safeguarding the orderly and free flow of personal information under Article 1 of the PIPL; Consider existing model contractual clauses in other jurisdictions in formulating any model contracts for transfers under the PIPL and clarify the scope of supervision required under such contracts to ensure recipients of personal data meet the standards enumerated under the PIPL; Add codes of conduct and corporate rules to the list of available transfer mechanisms under the PIPL; Remove the requirement to obtain consent in addition to using the cross-border transfer mechanisms outlined under the PIPL; Work towards joining the APEC CBPR system and clarify that certifications for transfers under the PIPL could potentially include APEC CBPR and PRP certification.

6. Providing clarity on which types of personal information processors are required to set up an external independent body to supervise processing and publish social responsibility reports

Article 57 of the revised PIPL requires personal information processors that provide "basic online platform services" to a "huge" number of users and have a "complex" type of business to (1) set up an independent body composed mainly of external members to supervise the processing of personal information; (2) stop providing services to product/service providers within the platform that process personal information in serious violation of laws and administrative regulations; and (3) regularly issue social responsibility reports.

While such requirements can be useful to enhance organizational accountability, CIPL recommends that the NPC provide clarity as to the exact parameters that would trigger such requirements. Which types of online platform services are subject to such obligations? How many users constitutes a "huge" number? What does a "complex" type of business look like? Moreover, the NPC should provide further clarity on the role of the independent external body and its functions so that organizations have more certainty as to what is required of any group they set up for this purpose.

With respect to the second requirement to stop providing services to product/service providers within the platform that process personal information in serious violation of laws and administrative regulations, it would be helpful for the NPC to clarify how such an obligation applies to platform services that do not have insight into certain activities undertaken on their platforms (e.g. in the context of cloud service providers). Under such circumstances, it would be helpful for the NPC to clarify that such platform services would only have to stop providing services once they have actual knowledge that platform users are in violation of the law.

Recommendation: Clarify the parameters that trigger the requirements of Article 57 of the PIPL and how the requirements apply to online platform services that do not have insight into certain activities undertaken on their platforms.

[11] Note that a companion certification to the APEC CBPR exists in the form of the APEC Privacy Recognition for Processors (PRP). The NPC should also include the PRP in making any clarification that undertaking personal information protection certification for data transfers overseas could include APEC CBPR certification.

7. Approaching anonymization from a risk-management perspective, and not as a technique or end-state

Article 72(4) defines "anonymization" as the process of handling personal information in ways that make it unable to identify a specific natural person or be restored to its original state. This definition appears to focus on the technique or end-state of the data and points towards a standard which requires the absence of any theoretical possibility of re-identification. This is a very high standard to meet as nothing is completely irreversible and would have a chilling effect on the use of data analytics, which may impact the competiveness and innovation of businesses and the startup ecosystem.

CIPL believes that data should be excluded from the scope of the PIPL when individuals are not identified, having regard to all means reasonably likely to be used, by the personal information processor or any other person, to identify the individual. This more realistic standard provides an incentive for organizations to anonymize data using measures appropriate to the risk of identification, which can be assessed through appropriate risk assessment processes for a specific context. When this is coupled with procedural, administrative and legal protections against de-anonymization (e.g. internal accountability measures and a commitment of organizations not to re-identify data; enforceable contractual commitments with third parties not to re-identify data; and legal prohibitions on unauthorized re-identification by any third party), individuals are effectively protected.

As noted in CIPL's initial comments on the PIPL, this revised standard would be in line with Article 24 of the PIPL, which states that if a personal information processor provides anonymized information to a third party, the third party may not use technical or other means to re-identify individuals. Under the original definition of anonymization, such a risk would be impossible, as data would be unable to be restored to its original state or identify a specific individual. Thus, CIPL believes the standard proposed above is more consistent with the rest of the PIPL.

Recommendation: Revise the definition of anonymization to reflect the more realistic standard of reasonable anonymization coupled with procedural, legal and administrative safeguards.

Conclusion

CIPL is grateful for the opportunity to provide input to the Standing Committee of the National People's Congress of the People's Republic of China on the updated version of its Draft Personal Information Protection Law. In addition to the comments provided above, CIPL strongly recommends that the NPC revisit the previous comments that CIPL made on the initial draft of the PIPL as several of these remain relevant to the current draft. A copy of the comments can be found here: https://bit.ly/3exVWo8 (Mandarin) https://bit.ly/2Sv2zir (English). We look forward to future opportunities to comment on and provide input into this process.

If you would like to discuss any of the comments in this paper or require additional information, please contact Sam Grogan, sgrogan@huntonAK.com or Dora Luo, doraluo@huntonAK.com.