BCLP. Client Intelligent

Insights

CHINA'S PERSONAL INFORMATION PROTECTION LAW TAKING EFFECT SOON. HOW IS IT DIFFERENT FROM WHAT WE KNEW EARLIER?

Oct 07, 2021

SUMMARY

China recently has passed its Personal Information Protection Law. The law will take effect on 1 November 2021.

The law is expected to have a significant impact on businesses which have or are planning to have some presence in China.

The full text of the new law was released at the same time that it was passed. Businesses have just over two months to prepare themselves for it. This article sets out how the final version of the PIPL differs from what we knew from the earlier drafts of the law which had been made available to the public.

On 20 August 2021, after the third and final read, China passed its first ever Personal Information Protection Law ("PIPL"). The PIPL will take effect on 1 November 2021.

When the first draft PIPL was released last year, we published an introductory guide to the key provisions to the draft law. After the release of the first draft PIPL in October 2020, a second draft PIPL was released on 29 April 2021 for public consultation. Businesses had four months to consider the second draft PIPL and make appropriate plans for compliance with the new law, before the final version of the law (which differs in a number of material ways from what had been released) was passed.

The full text of the final PIPL had not been released to the public before it was passed on 20 August 2021. While the key provisions highlighted in our earlier blog post still remain, the final PIPL, which eventually comprises eight Chapters and 74 Articles, contains a number of revisions and clarifications to the second draft.

We set out below the main revisions to and clarifications of the second draft PIPL which now are reflected in the codified version, so as to assist businesses, organisations or other data users (which already have considered the earlier drafts of the PIPL) in understanding what further changes to company policies and/or action plans are needed before 1 November 2021.

1. **Chapter One** of the final PIPL contains general provisions.

1. Article 3 removes the references to data handling activities carried out by "organisations or individuals", making clear that PIPL covers all personal data handling activities carried out within China. The provision giving extra-territorial effect to the PIPL as mentioned in our introductory guide also was passed.

2. The definition of data handling in Article 4 now expressly includes the deletion of personal data.

3. In Article 5, the principle of "necessity" is added as one of the principles which data handlers have to bear in mind.

4. In the second draft PIPL, Article 6 sought to regulate the handling of data and provided, among other things, that the scope of data handling shall be limited to the minimum necessary to give effect to the handling purpose and that no handling activity unrelated to the handling purpose shall be allowed.
   In the final PIPL, Article 6 is broken down into two parts: (i) data handling and (ii) data collection. While data collection is limited to the minimum necessary to give effect to the handling purpose, data handling activities now are required to be "directly related" to the handling purpose.

5. In addition to what previously was stated in the second draft PIPL about the prohibition of handling activities which compromise national security and public interest, Article 10 adds that illegal collection, use, processing, transmission, sale, provision or publication of personal data are prohibited. This is expected to be broad enough to cover acts of doxxing and cyberbullying.

2. **Section One**, **Chapter Two** of the final PIPL sets out general provisions regarding data handling.

1. Article 13 sets out the circumstances under which data handling is permissible. Article 13(ii) adds that data handling is permissible where it is necessary for human resources management purposes in accordance with labour laws and collective contracts[1]. Article 13(vi) also adds that the handling of personal data is permissible where the data already were made public legally.

2. Article 20 regulates the situation where there are more than one entities involved in the handling of personal data. In the final PIPL, this Article clarifies that such data handlers are to bear joint and several liability when breaches of data rights "cause harm".

3. Article 23 permits the provision of personal data by data handlers to third parties in limited circumstances. In the second draft PIPL, it had been proposed that data handlers could provide

personal data to "others" as long as the actions specified in the Article are taken. In the final PIPL, "others" is clarified to mean "other data handlers".

4. Article 24 permits the use of personal data in automated decision making processes, provided that the process is transparent and the outcome is fair and reasonable. The final PIPL further adds that there shall be no unreasonable differentiation in the treatment of individuals in conditions of transactions such as price.

5. Article 26 deals with the collection and use of photographs, videos and identification data of individuals for the purpose of public safety. In the second draft PIPL, it had been proposed that such data "shall not be made public or provided to others". The final PIPL no longer contains express prohibition of the publication or provision of such data. Instead, it provides that such data "shall not be used in other purposes".

6. Article 27 permits the handling of personal data which previously have been made public. The second draft PIPL had proposed that consent of the relevant individual is required where the handling of such data "exceeds the reasonable scope of relevance to the purpose for which such data was made public". The final PIPL simplifies the relevant provision by requiring consent where the handling of such data "significantly affects the rights of the person".

3. **Section Two**, **Chapter Two** of the final PIPL relates to the handling of "Sensitive Personal Data".

1. The final PIPL redefines "Sensitive Personal Data". Sensitive Personal Data now covers personal data which, once leaked or used illegally, are prone to causing harm to the personal dignity of an individual or to the safety of property belonging to an individual. Personal information of minors below the age of 14 now falls under the category of "Sensitive Personal Data".

2. The final PIPL requires separate consent from the individual for the handling of Sensitive Personal Data, regardless of upon which basis/es the collection and handling of data are premised. This offers more protection to individuals when compared with the proposal under the second draft PIPL which had required separate consent only if data handling was based upon consent.

3. Individuals also have the right to be informed about the handling of Sensitive Personal Data belonging to them. The final PIPL requires that individuals be informed about the necessity and the impact on personal rights of the handling activity, unless secrecy is mandated elsewhere in the PIPL.

4. The final PIPL adds another layer of protection to minors below the age of 14 by requiring data handlers to devise specific data handling policies applicable to such data.

4. **Section Three**, **Chapter Two** of the final PIPL regulates how Chinese governmental bodies may handle personal data. This part of the PIPL is less relevant to businesses as non-governmental

bodies, but may be of greater interest to natural persons as data subjects.

1. Article 35 relates to the rights of individuals whose personal data are handled by governmental bodies when carrying out statutory duties. The second draft PIPL had proposed that governmental bodies shall inform and obtain consent from the affected individuals. Under the final PIPL, individuals only have the right to be informed.

5. **Chapter Three** concerns cross-border transfers of personal data.

1. The necessary conditions under which cross-border transfer of personal data is allowed largely are similar to what we set out in our introductory guide. The condition which is likely to be most relevant to many businesses is the contractual regulation of rights and liabilities between the data handler and the overseas receiving party. In both the second draft PIPL and the final PIPL, data handlers are required to sign contracts with overseas receiving parties using the standard contractual clauses issued by the Cyberspace Administration of China (CAC). However, as of the date of writing this article, such standard contractual clauses have not yet been released to the public for adoption and compliance.

2. When compared with the second draft PIPL, the final PIPL contains provisions which defer expressly to international treaties relating to the transmission of personal data outside of the Chinese territory.

3. Data handlers are to take all necessary measures to ensure that the handling activities carried out by overseas receiving parties also complies with the standard of protection set out under the PIPL. In the second draft PIPL, it had been proposed that this requirement is to apply where there is a contractual arrangement between the data handler and the overseas receiving party. Under the final PIPL, this requirement applies in any event.

4. Requests by foreign judicial bodies to obtain access to personal data stored within Chinese borders will be considered and processed in accordance with relevant laws or international treaties. The final PIPL adds that such requests also may be granted based on the principle of reciprocity.

6. **Chapter Four** sets out the rights of individuals in connection with the handling of personal data.

1. In addition to the rights to peruse, copy, supplement, and correct personal data held by data handlers, the final PIPL adds that individuals also have the right to request that their personal data be transferred to another data handler specified by the individuals, as long as the new data handler also complies with the conditions set out by the CAC.

2. The final PIPL also expands slightly the circumstances under which personal data need to be deleted by adding that individuals have the right to request deletion if the purpose for which such data were collected becomes impossible to fulfill.

3. With regard to personal information belonging to deceased persons, the final PIPL clarifies that close relatives of the deceased may, in accordance with their legal and legitimate interests and except otherwise arranged by the deceased prior to their demise, peruse, copy, correct or request deletion of personal information relating to the deceased.

4. The final PIPL further provides an express cause of action to individuals where data handlers refuse to entertain the requests by individuals to exercise their rights.

7. **Chapter Five** concerns the responsibilities of data handlers.

1. Article 57 deals with data leaks. It requires data handlers to take remedial actions immediately and notify the relevant authorities and individuals concerned. In the second draft PIPL, it had been proposed that these requirements only are to cover data leaks which already have happened. Under the final PIPL, these requirements extend to cover data leaks, unauthorised data changes or loss of data which already have happened or which potentially will happen.

2. Article 58 is relevant to data giants which provide important internet platform services, have significant numbers of users, and/or carry out complex types of businesses operations. The final PIPL contains a number of additional requirements for these data handlers when compared with what was understood from the second draft PIPL:
   - Set up a comprehensive compliance regime in accordance with national laws in order to protect personal information.
   - Abide by the principles of openness, fairness and justice in devising platform rules. The platform rules clearly should set out the data handling policies adopted by the product or service providers on the platform, as well as their responsibilities in protecting personal information.

3. In cases where data handlers have entrusted handling activities to third parties, such third parties are required to abide by the requirements in Article 59. The final PIPL contains an additional requirement that such third parties are to assist the data handlers in complying with the obligations under the PIPL.

8. Although **Chapter Six** primarily governs governmental bodies responsible for the protection of personal data, there are a number of changes reflected in the final PIPL that should be noted by all data handlers.

1. In addition to the various duties already set out in earlier drafts of the PIPL, the final PIPL requires the relevant authorities to conduct assessments of the protection afforded to personal information used in Apps[2] and announce the results of such assessments.

2. The relevant authorities are required to promote the setting up of rules and standards related to the handling of Sensitive Personal Data. The final PIPL clarifies that these rules and standards specifically are targeted at regulating smaller-scale data handlers.

3. Another additional duty of the authorities expressly provided for under the final PIPL is to build a comprehensive complaint and reporting system.

4. The final PIPL further gives the relevant authorities the power to refer data handlers to the public security bureau for criminal investigation.

9. **Chapter Seven** concerns legal liability.

1. The key provisions with regard to monetary penalties and suspension of business largely have remained the same.

2. A number of permissible sanctions have been added to the final PIPL:
   - The relevant authorities may order the suspension or termination of the operation of Apps or software which are in breach of the law.
   - Where the breach is serious, managerial personnel who directly are responsible for the breach may, under the final PIPL, be banned from assuming office as directors, supervisors, senior management personnel or data protection controllers in the relevant companies for a certain period of time.
   - Public officers within the relevant authorities also may be subject to sanctions (the exact kinds not specified in the law) for negligence, abuse of power and favouritism.

3. With regard to a civil claim for damages arising from data mis-handling, the data handler is liable unless it can demonstrate that it is not at fault. The position is the same both under the second draft PIPL and the final PIPL.

4. In terms of quantum under the civil claim, the second draft PIPL had provided that the amount is to be determined with reference to the loss suffered by the individual concerned or the profit gained by the relevant data handler. The final PIPL has adopted the same wording but sheds no further light on how the amount of damages is to be determined with reference to those two factors.

10. **Chapter Eight** concludes the PIPL. It provides that the PIPL as passed on 20 August 2021 will take effect from 1 November 2021.

Disclaimer: This article sets out only the major changes found in the PIPL as passed when compared against the earlier drafts released to the public. It is not intended to be a comprehensive summary of the provisions under the PIPL. The PIPL is available only in the Chinese language. The English translations set out in this article are unofficial and are provided for reference only. This article is not intended to be relied upon as legal advice. Businesses are advised to seek bespoke legal advice to suit your respective and specific situations and circumstances.

---

1. Foreign enterprises setting up factories in China often are required to sign collective contracts with labour representatives or trade unions instead of individual contracts with staff and workers.

2. The final PIPL contains no further explanation as to what “Apps” mean. From the context, we believe “Apps” would cover mobile applications and computer software.

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
