MAYER | BROWN

25 May, 2021

Legal Update

Full Steam Ahead: Second Draft of China's Personal Information Protection Law and Data Security Law

On 29 April 2021, the second drafts of China's Personal Information Protection Law (Second Draft PIPL)[1] and the Data Security Law (Second Draft DSL) were released. Once passed, the Second Draft PIPL will become China's first comprehensive law that protects personal information, and the Second Draft DSL will further regulate data processing activities that could impact national security, particularly "important data".

While the Second Draft PIPL and the Second Draft DSL do not substantially amend the first drafts issued in October 2020 and July 2020, respectively, some further obligations and clarifications have been added. We summarise some of these key changes below.

Second Draft PIPL

DATA PROCESSORS

In a major departure from the previous draft, the Second Draft PIPL expands the obligations imposed on third parties entrusted to handle personal information (i.e., the equivalent of a data processor under the GDPR (the EU General Data Protection Regulation)).

Under the first draft, data processors were not directly regulated. Instead, they were only required to process the personal information in accordance with the relevant data processing agreement with the data controller (referred to as the "personal information processor" under the Second Draft PIPL), to delete or return the personal information once the agreement is fulfilled or terminated and to not further sub-contract the processing of the personal information, unless it obtains the data controller's consent.

Under the new Article 58, data processors must perform the relevant obligations under Chapter V of the Second Draft PIPL and adopt necessary measures to ensure the personal information is kept secure. In particular, this may mean that overseas data processors that process personal information to provide goods or services or analyse or assess the behaviour of data subjects in China (or under any other circumstances prescribed under the laws or regulations), will need to appoint a local representative or establish an office in China[2]. This may have major implications

[1] See our article regarding the first draft of the PIPL: https://www.mayerbrown.com/en/perspectives-events/publications/2020/12/asia-ip-tmt-quarterly-review-fourth-quarter-2020

[2] Article 53and 58 of the Second Draft PIPL.

for foreign companies that have no onshore operations, but which are providing services to data controllers handling personal information collected in China.

In addition to establishing a local presence, data processors will also now need (among other things) to conduct regular audits to verify that their processing activities are compliant with China's laws and regulations; carry our risk assessments prior to processing sensitive personal information, using automated decision-making, disclosing any personal information or making any cross-border transfers; comply with breach notification obligations; and comply with the new obligations imposed on large internet platform service providers (discussed below).

OBLIGATIONS ON LARGE INTERNET PLATFORM SERVICE PROVIDERS

Another significant amendment proposed by the Second Draft PIPL are the additional obligations on data controllers which provide basic online platform services to a substantial number of users and which operate complex business models[3]. Such data controllers would be required to:

(1) Establish an independent body, mainly consisting of external personnel, to oversee the data controller's processing activities;

(2) Stop providing services to those who are offering products or services via the data controller's online platform, who are in serious violation of the data processing requirements under the relevant laws and regulations; and

(3) Regularly publish corporate social responsibility reports in relation to personal information protection.

It is likely that further measures or interpretations will be issued to provide clarity on the application of the above requirements. In particular, clarification will be welcomed in respect of what would constitute a substantial number of users or complex business models, what would amount to a serious violation of the laws and regulations, and what needs to be included in the social responsibility reports.

It is important to remember that as with the original draft, the Second Draft PIPL is intended to have extra-territorial effect. Article 3 provides that the Second Draft PIPL shall apply to any processing of personal information that occurs outside China, if the purpose of processing is to provide products or services to individuals in China, to analyse and evaluate the behaviour of individuals in China, or any other circumstances specified by the laws or regulations. The effect of this article is that online platform service providers based overseas, may need to comply with the above requirements even if they do not have an onshore presence, and/or will have to establish an office or appoint a legal representative in China[4].

LEGAL BASIS FOR PROCESSING AND CONSENT

The processing of personal information that is publicly available has been added as a new legal basis for processing under the Second Draft PIPL. This departs from the GDPR, which does not include publicly available personal information as a legal basis for processing. Under the Second Draft PIPL, personal information processors (the equivalent of data controllers under the GDPR) can process personal information if one of the following legal basis applies[5]:

(1) The data subject has provided their consent;

[3] Pursuant to Article 58 of the Second Draft PIPL, these obligations may also apply to data processors.

[4] Article 53 and 58 of the Second Draft PIPL.

[5] Article 13 of the Second Draft PIPL.

(2) The processing is necessary for the performance of a contract to which the data subject is a party;

(3) The processing is necessary for the fulfilment of duties or obligations imposed under laws or regulations;

(4) There is a need to respond to public health emergencies or to protect an individual's life, health or property in an emergency situation;

(5) The personal information is already publicly available, and the processing is within a reasonable scope in compliance with the PIPL;

(6) The personal information is being processed for the purposes of conducting news reporting, supervising public opinion or other such activities that are in the public interest and the processing is within reasonable scope; and

(7) The processing is permitted pursuant to other laws and regulations.

Article 13 of the Second Draft PIPL makes it clear that obtaining the data subject's consent is not mandatory if the processing falls within the scope of any other legal basis set out under paragraph (2) to (7) above. Based on the wording of Article 30 of the Second Draft PIPL, it seems that this equally applies to the collection of sensitive personal information, where the express consent of the data subject will only be needed if the personal information processor is seeking to rely on consent as the basis for processing, unless other laws or regulations stipulate that written consent is required[6]. In contrast, Article 39 of the Second Draft PIPL does not expressly limit the requirement for express consent on the cross-border transfer of personal information to only situations where consent is being relied on as the basis for processing. This conflicts with Article 13. Further clarity may be needed on whether express consent may still be required for cross-border transfers, even if other grounds for processing apply.

CROSS-BORDER TRANSFERS

The cross-border transfer requirements under the Second Draft PIPL, remain largely the same as in the original draft. The only key change is that if personal information is being transferred on the basis of an agreement with the foreign recipient, such agreement must be based on the "standard contract" stipulated by the Cyberspace Administration of China (CAC).

As a brief recap, the Second Draft PIPL now provides that personal information cannot be transferred outside of China, unless one of the following conditions are met[7]:

(1) A security certification is obtained, which is conducted by an accredited body in accordance with regulations specified by the CAC;

(2) An agreement with the foreign recipient is entered into based on the "standard contract" stipulated by the CAC, which sets out each party's respective rights and obligations, and ensures that the personal information will be protected to the same standard as that provided under the Draft PIPL; or

(3) The transfer is in accordance with other laws or regulations or other conditions prescribed by the CAC.

However, critical information infrastructure (CII) operators and any personal information processors who process personal information at a volume that exceeds the threshold specified by

[6] Article 13 and 30 of the Second Draft PIPL.

[7] Article 38 of the Second Draft PIPL.

the CAC (still to be determined), can only transfer the personal information overseas if a security assessment is completed by the CAC[8].

Aside from the above, a prior risk assessment must also be conducted by the personal information processor in relation to the cross-border transfers[9]. Records of the risk assessment must be retained for at least three years.

The above requirements under the Second Draft PIPL are largely consistent with China's Cybersecurity Law (CSL) and draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information issued in 2019 (Draft Measures). Note that separate to the Second Draft PIPL, CII operators and networks operators (essentially anyone who owns or operates a computer network, server or website in China) will need to comply with the data localisation and cross-border transfer restrictions currently in force under the CSL. The Draft Measures have not yet been brought into operation, and are likely to be subject to further amendments to align them with the Second Draft PIPL.

Consistent with the Second Draft DSL, there are also restrictions under the Second Draft PIPL on the transfer of personal information requested by foreign judicial or law enforcement authorities, unless approval has been obtained from the relevant Chinese authority or it is in accordance with relevant international treaties[10]. The Chinese authorities can also take steps against foreign organisations that engage in processing activities that are seen as harming the rights and interests of Chinese citizens or which endanger national security or public interest (e.g., prohibiting the provision of personal information to them)[11]. Further, if any country adopts what the Chinese authorities deem to be discriminatory measures against China in relation to personal information protection, it may implement reciprocal measures against them[12].

OTHER CHANGES

Some of the other changes introduced in the Second Draft PIPL include the following:

(1) A prohibition on the processing of personal information through the use of coercion[13];

(2) A requirement to process personal information in a manner that has the least impact on the individual's rights and interests[14];

(3) A requirement that personal information processors should make sure that the personal information collected is of high quality and should avoid causing harm to the data subject's rights and interests due to any inaccuracy and incompleteness in the personal information[15];

(4) An obligation to obtain the consent of the minor's parents or guardian when data of a person under 14 years of age are collected (under the original draft, this requirement only applied if the personal information processor knew or ought to have known that the personal information concerned a minor)[16];

[8] Article 40 of the Second Draft PIPL.

[9] Article 55 of the Second Draft PIPL.

[10] Article 41 of the Second Draft PIPL.

[11] Article 42 of the Second Draft PIPL.

[12] Article 43 of the Second Draft PIPL.

[13] Article 5 of the Second Draft PIPL.

[14] Article 6 of the Second Draft PIPL.

[15] Article 8 of the Second Draft PIPL.

[16] Article 15 of the Second Draft PIPL.

(5) A clarification of the fact that any withdrawal of a data subject's consent to the processing of their personal information will not affect the processing activities that have been carried out before the consent was withdrawn[17];

(6) An expansion of the scope of protection of personal information granted under the Second Draft PIPL to apply to deceased individuals, whose rights granted under the law can be exercised by his or her next of kin[18];

(7) A requirement for personal information processors to follow principles of openness and transparency, and make known to the public their specific rules for processing, as well as the purpose, method and scope of the processing (this is on top of the notification obligations, which already appear in the first draft)[19];

(8) A requirement to provide an opt-out for marketing activities (where personal information is used for commercial marketing purposes and push notifications through automated decision-making)[20]; and

(9) Heightened liability for data controllers in situations where an individual claims that their personal information rights have been infringed, the burden of proof now rests with the data controller[21]. The data controller will be liable for damages, unless it can prove that it was not at fault.

Second Draft DSL

SCOPE OF APPLICATION

The Second Draft DSL applies to the processing of "data", i.e., any record of information in electronic or non-electronic form, but does not apply to the processing of personal information, state secrets or military data.[22] The Second Draft DSL also makes it clear that the law applies to "data processing activities" carried out within the territory of China, replacing the phrase "data activities" used in the first draft. The definition of "data processing activities" is, however, similar to that of "data activities", which includes the collection, storage, use, refining, transmission, provision and disclosure of data. As with the first draft, the Second Draft DSL is intended to have extra-territorial effect.

DATA CLASSIFICATION

Under the Second Draft DSL, the government is tasked with establishing a data classification management and protection system to govern data based on how important or essential the data are to national security and the public interest, and the level of impact that any data leak, tampering, damage or illegal acquisition may have on national security, the public interest or the lawful rights and interests of citizens or organisations. Each sector and region must also establish catalogues to identify important data in the relevant industry, in accordance with the data categorisation and classification systems established by the government, and impose special measures to protect such data.

[17] Article 16 of the Second Draft PIPL.

[18] Article 49 of the Second Draft PIPL.

[19] Article 7 of the Second Draft PIPL.

[20] Article 25 of the Second Draft PIPL.

[21] Article 68 of the Second Draft PIPL.

[22] Article 3, 51 and 52 of the Second Draft DSL.

DATA SECURITY OBLIGATIONS

The Second Draft DSL effectively expands the scope of some of the obligations imposed on network operators and CII operators under the CSL. Under Article 26 of the Second Draft DSL, any entity that carries out data processing activities (which essentially means any entity whatsoever), must establish a data security management system, carry out data security training, and implement technical security and safeguarding measures pursuant to the multi-level protection scheme (MLPS). In addition, where important data is being processed by an entity, it must also designate a data security officer and establish a management office to ensure compliance with its data security obligations.

The MLPS is established by the government and prescribes security measures that must be met depending on different risk classification levels. The higher the risk to national security, social order or economic interests that may occur if an entity's system is damaged or subject to an attack, the higher their classification and the more stringent the security requirements.

CROSS-BORDER TRANSFER OF IMPORTANT DATA BY NON-CII OPERATORS REGULATED

The Second Draft DSL distinguishes between CII and non-CII operators on the cross-border transfer of important data. CII operators are regulated under the CSL and are broadly defined as entities whose business has the potential to cause harm to national security, national economy, people's livelihood and public interests in the event they suffer a security breach that leads to any destruction or loss of function or data. While CII operators must follow the rules set out under the CSL, the Second Draft DSL requires non-CII operators to conform to the requirements formulated by the CAC or other government agencies for the overseas transfer of important data[23]. These requirements have not yet been stipulated, and will likely be published only after the Second Draft DSL is brought into operation.

Even though the Second Draft DSL is still in draft form, it is important to remember that CII operators and network operators are still subject to the CSL, and the requirements relating to data localisation and cross-border transfers.

PENALTIES

Under the original draft, if a foreign judicial or law enforcement authority requested access to data stored in China, such data could not be provided unless approval has been obtained from the competent government authority, or a relevant international treaty applies[24]. Those in breach may now face severe punishments under the Second Draft DSL for non-compliance, which include the issuance of rectification orders, warnings, and a fine of up to RMB 1 million[25] on the organisation and up to RMB 200,000 on the person in charge and other directly responsible personnel. This places multinational companies in a difficult lose-lose situation, where compliance with a foreign authority's data access request may render them in breach of Chinese law, and non-compliance will render them in violation of the relevant foreign laws or court orders.

The penalties imposed for violating some of the other obligations under the Second Draft DSL have also been increased (e.g., raised from a fine of RMB 1 million to RMB 5 million), and liability has been extended to cover not only those in charge, but also any personnel that was directly responsible for the breach.

---

[23] Article 30 of the Second Draft DSL.

[24] Article 35 of the Second Draft DSL.

[25] Article 46 of the Second Draft DSL.

Takeaways

Large platform service providers and data processors (even those without operations in China), may be subject to enhanced obligations under the Second Draft PIPL, while any organisation that handles data (even data not seen as "important data") must comply with cross-border transfer restrictions, carry out an MLPS assessment and implement corresponding security measures under the Second Draft DSL. Both draft laws are intended to have extra-territorial effect, and entities that have customers, clients or service providers in China need to pay particular attention to see whether or not they would be caught by these laws once enacted.

Furthermore, the passing of the Second Draft PIPL and Second Draft DSL will not eliminate the complex matrix of laws in China relating to data. Companies must still also ensure compliance with the CSL, China's Encryption Law[26], Anti-espionage Security Prevention Work Regulation[27], and other various specific measures and standards (e.g., concerning mobile apps and facial recognition technology).

The Second Draft PIPL and Second Draft DSL are expected to be passed later this year, with possibly some further amendments, and brought into operation at the beginning of 2022. Companies should keep a sharp eye on developments, and take stock of their operations in preparation for what is to come.

The authors would like to thank Sophie Huang, Intellectual Property Officer at Mayer Brown, for her assistance with this article

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Karen Lee
+65 6327 0638
karen.hf.lee@mayerbrown.com

[26] Issued on 26 October 2019, and brought into force on 1 January 2020.

[27] Issued and brought into force on 26 April 2021.