COVINGTON

China Releases First Draft of Personal Information Protection Law

October 23, 2020

Data Privacy and Cybersecurity

On October 21, 2020, the National People's Congress ("NPC"), China's top legislative body, released its first draft of the Personal Information Protection Law (the "Draft Law") for public comment (official Chinese version available here and Covington's unofficial English translation here). The period for public comment ends on November 19, 2020 and comments can be submitted through NPC's official website.

As the country's first comprehensive law in the area of personal information protection, the Draft Law aims to "protect the rights and interests of individuals," "regulate personal information processing activities," "safeguard the lawful and orderly flow of data," and "facilitate reasonable use of personal information" (Art. 1).

Although bearing a resemblance to the European Union's ("EU") General Data Protection Regulation ("GDPR") and other recent privacy legislation in major jurisdictions in some important areas, the Draft Law introduces a number of provisions that are consistent with recent trends in other Chinese laws in the areas of data and technology, such as the draft Data Security Law and the newly enacted Export Control Law. These include, for example, rules establishing extraterritoriality of the Draft Law and a "black list" that would restrict or prohibit listed foreign organizations from receiving personal information from China.

Additionally, this Draft Law, once enacted, will work together with the Cybersecurity Law (with a particular focus on cybersecurity) and the draft Data Security Law (with a particular focus on data that is of importance to China's national security) to establish a broader regulatory framework related to data. As such, much is to be seen in the next few years on how these (draft) laws will interact and how the government agencies will be dividing their roles and responsibilities with respect to these laws.

In this alert, we summarize a few of key aspects of the Draft Law and highlight certain similarities and differences between the Draft Law and GDPR.

I. Key Terms

1. Personal Information/Sensitive Personal Information

The Draft Law defines "personal information" as "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person" (Art. 4). This definition is largely consistent with the definition of "personal information" under China's

Cybersecurity Law, which refers to "various types of electronic or otherwise recorded information that can be used separately or in combination with other information to identify the natural person" (Art. 76). This definition also largely aligns with the term "personal data" under GDPR, which is broadly defined as "any information relating to an identified or identifiable natural person."

The Draft 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). This definition, by contrast, does not neatly align with the GDPR's equivalent concept of "special" personal data, which focuses on data categories (but not propensity to cause harm). As a result, GDPR identifies some additional categories of data as "special" personal data but excludes some categories listed in the Draft Law.

2. "Processing Entity" of Personal Information

The Draft Law imposes personal information protection obligations on parties acting as a "personal information processing entity [or individual]," which is an "organization or individual that independently determines the purposes and means for processing of personal information" (Art. 69). This appears to be the Chinese law equivalent of the "data controller" concept under the GDPR.

3. Process/Processing

"Processing" is defined broadly as "the collection, storage, use, refining, transmission, provision, or public disclosure of personal information" (Art. 4). Again, this is consistent with the GDPR, under which "processing" refers to "any operation or set of operations" performed on personal data," including the "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" of personal information.

II. Extra-territorial Effect of the Draft Law

The Draft Law extends its territorial scope to the processing of personal information conducted outside of China, provided that the purpose of the processing is (i) to provide products or services to individuals in China, (ii) to "analyze" or "assess" the behavior of individuals in China, or (iii) for other purposes to be specified by laws and regulations (Art. 3).

These criteria are strikingly similar to the territorial scope provisions found in Article 3 of the GDPR, but without the limiting effects of the GDPR's recitals and EU common law. It appears that this approach is incorporated into the Draft Law 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 analyzing or assessing the behavior of individuals in China.

Moreover, Article 52 of the Draft Law 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

similar to the GDPR's requirement for the appointment of an "EU representative" under Article 27. Where this obligation applies, such entities must also provide the name and contract details of the office or representative to the competent government agency (-ies) responsible for personal information protection in China ("Competent Agency").

Note that China has also introduced rules with extra-territorial effect in other recent laws, including the draft Data Security Law, which states that organizations and individuals outside of China that conduct data activities which may "harm China's national security, public interests, or the rights of Chinese citizens" may be subject to that law.

III. Cross-border Transfer of Personal Information

1. General Requirements for Cross-Border Transfer

1. Notice and Consent. The Draft Law imposes separate notice and consent obligations on processing entities for cross-border transfer of personal information, on top of general notice and consent requirements for in-country collection and use of personal information.

   Under Article 39 of the Draft Law, processing entities must notify individuals of the following information and obtain "separate" consent for cross-border transfers:

   - identity and contact details of the overseas recipient;
   - purposes and means of processing;
   - categories of personal information to be transferred; and
   - the means to exercise, against the overseas recipient, personal information subject rights.

2. Prior Risk Assessment and Record Keeping. Article 54 of the Drat Law specifically requires processing entities to carry out a risk assessment prior to cross-border transfer of personal information, and to keep records of such transfers. These reports and records must be retained for a period of at least three years.

3. Transfer Mechanisms. In addition to the requirements mentioned above, the Draft Law also states that processing entities must choose one of the following mechanisms to transfer personal information abroad (Art. 38):

   - undergo a security assessment administered by Cyberspace Administration of China ("CAC") in accordance with Article 40 of the Draft Law, which states that operators of Critical Information Infrastructure ("CII") and processing entities that transfer a "large" volume of personal information (to be specified by CAC) must locally store personal information collected or generated in China and undergo a security assessment, if the cross-border transfer is necessary, unless otherwise allowed by laws, regulations and rules of CAC;
   - obtain certification from "professional institutions" in accordance with the rules of CAC; or
   - enter into a transfer agreement with the overseas recipient specifying the rights and obligations of both parties, and ensuring the overseas recipient can meet the protection standards as set out by the Draft Law.

Note that Article 38 also includes a catch-all provision that raises the possibility that other laws and regulations (or CAC presumably through implementing regulations) can provide other transfer mechanisms in the future.

2. Requirements for Cross-Border Transfer under Special Circumstances

If cross-border transfer of personal information is needed for purposes of "international judicial assistance" or to "assist administrative proceedings [outside of China]," approval from Chinese regulator(s) must be obtained. To the extent that China participates in international treaties or agreements which include provisions for the cross-border transfer of personal information, these treaties and agreements shall prevail (Art. 41). Note that China already enacted the International Criminal Judicial Assistance Law back in October 2018, which blocks disclosure of evidence obtained in China to criminal enforcement authorities outside of China in connection with a criminal matter, absent approval from the Chinese government. It appears that this provision in the Draft Law will include "administrative proceedings" in the scope of the blocking statute, and it will likely raise future questions related to transfer of personal information outside of China for purposes such as internal investigations or other legal proceedings.

The Draft Law also states that, should any foreign organizations or individuals conduct personal information processing activities "infringing Chinese citizens' rights and interests related to personal information," or "endangering China's national security or public interest," then CAC may place such foreign organizations or individuals on a publicly available list and take measures to restrict or prohibit processing entities from transferring personal information to them (Art. 42). This "blacklist" approach is similar to China's "unreliable entity list," which imposes restrictions on foreign enterprises, organizations, and individuals that are seen as: (i) "endangering the national sovereignty, security, or development interests of China"; or (ii) "suspending [or terminating] normal transactions with Chinese enterprises, organizations, or individuals, in violation of [commonly accepted] market-based principles, [thus] seriously harming the legitimate rights and interests of Chinese enterprises, organizations, or individuals."

Moreover, should any countries or regions act in a discriminatory or restrictive manner against China with respect to personal information protection, China has the right to take "corresponding measures" against such countries or regions (Art. 43). Again, similar provisions appear in the draft Data Security Law and the Export Control Law, although it is unclear how the government plans to enforce such a provision.

IV. In-Country Processing of Personal Information

The Draft Law provides specific requirements for the in-country processing of personal information. Some of these requirements are largely consistent with China's current regulatory rules, standards and best practices, such as data sharing, data subject rights, the implementation of an internal data security program, and so forth. We discuss some of the key requirements for in-country processing in a greater detail below.

1. Legal Basis of Processing

Under the Draft Law, processing entities can only process personal information in the following circumstances (Art. 13):

- consent has been obtained;

- the processing is necessary to enter into or perform a contract to which the individual is a party;
- the processing is necessary to perform legal responsibilities or obligations;
- the processing is necessary to respond to a public health emergency, or in an emergency to protect the safety of natural persons' health and property;
- to a reasonable extent, for purposes of carrying out news reporting and public opinion monitoring for public interests; and
- other circumstances permitted by laws and regulations.

Unlike China's Cybersecurity Law, which provides "consent" as the only available legal basis for collection and use of personal information, the Draft Law takes an approach more similar to the GDPR, which sets out multiple legal bases for processing. However, certain legal basis available under the GDPR are not included in the Draft Law, such as legitimate interests.

Also, the Draft Law states that generally government agencies will have to follow the rules under this law for their processing of personal information and cannot exceed the scope of their legal authorization for their processing activities (Arts. 33-37).

2. Special Requirements for Processing of Personal Information Collected in Public Areas

The Draft Law sets out specific requirements for the processing of personal information collected in public areas (e.g., airports and train stations). Under Article 27 of the Draft Law, the installation of image collection or individual identification (e.g., facial recognition) devices in public areas is permissible if it is necessary to the protection of public security and individuals are given prominent notice.

Furthermore, the personal information collected by the abovementioned equipment in public areas can only be processed for public security purposes and must not be publicly disclosed or shared with third parties, unless a separate consent from the individual has been obtained or the disclosure is otherwise required by applicable laws and regulations.

3. Processing of Sensitive Personal Information

The Draft Law states that processing entities can only process sensitive personal information for specified purposes and such processing must be necessary. Furthermore, the Draft Law also specifies that, if processing entities know or should have known the personal information to be processed is from minors under fourteen years old, processing entities must obtain prior consent from guardians of the minors.

4. Personal Information Breach Response

In the event of a data breach, the Draft Law requires processing entities to take "immediate" remediation actions and notify the Competent Agency, as well as the affected individuals (Art. 55). Note that the text itself does not provide a time limit similar to the GDPR's 72-hour benchmark.

The notification must include the following information (Art. 55):

- the cause(s) of the data breach;

- the categories of the breached personal information and any potential damages caused by such a breach;
- remediation measures that have been taken;
- risk-mitigation measures that individuals may consider taking; and
- contact details of the processing entity.

Furthermore, if the processing entity takes measures that effectively prevent the potential harm caused by the breach from materializing, such processing entity is not mandated to notify affected individuals. However, if the Competent Agency deems that the breach may cause harm to affected individuals, it has the power to order the processing entity to notify such individuals (Art. 55).

The notification requirements under the Draft Law provides further details than the Cybersecurity Law, which requires network operators to take "immediate" remediation actions and notify users, as well as relevant government agencies, but had not provided any details. It remains to be seen whether (and how) the provisions under these laws will be consolidated into a single breach notification regime in China.

V. Liabilities for Violating the Draft Law

The Draft Law imposes stiff fines for non-compliance. Under the Draft Law, an organization that unlawfully processes personal information or fails to take necessary security measures to protect personal information may be subject to a baseline fine up to 1 million RMB. If the violation is considered serious, the fine may be increased up to 50 million RMB or 5% of the organization's annual revenue for the prior financial year (Art. 62). It is currently unclear whether an organization's annual revenue will be calculated on a global basis when assessing fines.

The Draft Law also states that, with respect to civil claims brought for personal information violations, individuals may obtain financial compensation for actual damages suffered or being compensated based on illegal gains derived from the unlawful processing. In the event that the illegal gains cannot be determined, the court has the discretion to decide on the compensation amount based on relevant facts. If the processing entity can prove that it is not at fault, its liability may be reduced or discharged (Art. 65). This provision will likely allow plaintiffs to obtain monetary compensations even if the actual damages cannot be proved. It is possible that there will be an increasing number of civil litigations on personal information infringement after the Draft Law is enacted.

Finally, under the Draft Law, the People's Protectorate, the Competent Agency, and organizations designated by CAC can bring lawsuits for violations that infringe the rights and interest of a large number of individuals (Art. 66).

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Yan Luo	+86 10 5910 0516	yluo@cov.com
Daniel Cooper	+32 2 545 7527	dcooper@cov.com
Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Eric Carlson	+1 202 662 5253	ecarlson@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Nicholas Shepherd	+32 2 549 5269	nshepherd@cov.com
Zhijing Yu	+86 10 5910 0309	zyu@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.