COVINGTON

China Released Updated Draft Data Security Law and Personal Information Protection Law for Public Comments

May 3, 2021

Data Privacy and Cybersecurity

On April 29, 2021, the Standing Committee of the National People's Congress of China ("**NPC**"), the country's top legislator, released the updated draft *Data Security Law* (the "**DSL**") and draft *Personal Information Protection Law* (the "**PIPL**") for public comments (official Chinese versions of these two draft laws are available here and here, and Covington's unofficial English translation is available here and here). The commenting period ends on May 28, 2021 and comments can be submitted through NPC's official website.

Why are these two new draft laws significant?

In 2016, China promulgated its first landmark legislation in the cybersecurity and data protection area, the *Cybersecurity Law* ("**CSL**") (Covington alert available here), which primarily focuses on cybersecurity and the protection of the country's Critical Information Infrastructure ("**CII**"). To further address the rising concerns related to the protection of personal information and "important data" (left undefined in the DSL, but used broadly to refer to data that is important from a national security perspective), China followed up with two more significant legislative proposals in 2020: the first drafts of the DSL and the PIPL. The DSL is designed to regulate data processing activities that could have a national security impact, in particular those related to "important data," while the PIPL focuses on protecting personal information. The second drafts of both of these laws have now been released for public comments. Once finalized, these three laws, the CSL, DSL, and PIPL, will form an over-arching framework that will govern data protection and cybersecurity in China for years to come.

Beyond these three laws, the proliferation of sectoral specific rules, as well as other Chinese laws such as the *Anti-espionage Law* and the *Encryption Law*, could make data compliance in China more complex. While some laws do not appear to be primarily focused on data protection and cybersecurity, they may have indirect impacts on data processing activities in specific sectors or under specific scenarios. For example, besides the CSL, operators of CII are also subject to data security obligations under the *Anti-espionage Security Prevention Work Regulation* ("**Anti-espionage Regulation**"), which was released by the Ministry of State Security on April 26, 2021 and took effect on the same day. The Anti-espionage Regulation requires that, among other things, CII operators must adopt technical measures to ensure data security of their network and their "core information technologies." Moreover, the Encryption Law, which took effect in January 2020, mandates CII operators carry out a security assessment and go through a national security review for their use of encryption. It remains to

be seen how this complicated web of regulatory requirements may be consolidated or whether the divergence will remain even after the finalization of the DSL and the PIPL.

Given the sweeping scope and the broad territorial reach of these laws, companies that process Chinese personal information or non-personal data should closely monitor these developments in the coming months.

Below we summarize updates in the second drafts of the DSL and PIPL as compared to the first drafts of these las.

Data Security Law: Key Changes in Second Draft

As explained in our blog post that summarized key provisions of the first draft of the DSL (available here), this law aims to create a framework for the protection of broadly defined "data security" from a national security perspective. In the second draft, it is clarified that this law does not govern the processing of state secrets, personal information and military data (Article 51 and 52), but it will apply to all other scenarios where companies process non-personal data, with a particular focus on the governance of "important data."

If the draft DSL is finalized as currently drafted, entities "processing data" will need to establish an internal data security program in compliance with the requirements under the Multi-Level Protection Scheme ("**MLPS**"), a cybersecurity framework mandated by the CSL (to be explained below); to build specific internal policies to manage "important data" according to the catalogue of important data issued by Chinese agencies; to consider strategies for the cross-border transfer of "important data"; and to develop plans to respond to requests for data "stored in China" from "judicial or law enforcement organs" outside of China.

Five key changes made to the second draft of the DSL:

1. **"Data Processing Activities"**

   The first draft of the DSL states that this law applies to entities carrying out "data activity" on data that "covers all electronic and non-electronic records of information." The second draft replaces this term with "data processing activity," which is defined broadly to include "the collection, storage, use, refining, transmission, provision, or public disclosure of data" (Article 3). This revision reinforces the sweeping scope of data-related activities that are subject to the DSL and also aligns with the term of "processing" under the PIPL, which is similarly defined as "the collection, storage, use, refining, transmission, provision, or public disclosure of personal information."

2. **Data Categorization and Classification**

   The second draft of the DSL calls for the central government to establish a national level "data categorization and classification system" to govern data based on "the level of importance to the State's economic and social development, as well as the degree of damages to the national security, social interests or the lawful interests of citizens and organizations, if the data is tampered, damaged, leaked or illegally obtained or used." Furthermore, the central government shall issue a catalogue of "important data" and impose enhanced protection requirements on "important data" (Article 20). Note that unlike an entity's internal data classification program, which allows a company to

organize its structured and unstructured data into defined categories such as public or confidential data, the above "categorization and classification system" will be a regulatory mechanism developed by the State and will be mandatorily applied to all companies and across sectors.

At the regional and sectoral level, agencies are mandated to release more detailed catalogues to identify the scope of "important data" in their respective regions or sectors and strengthen the protection of such data based on the national level data categorization and classification system (Article 20).

Notably, certain sectoral regulators in China have already experimented with the data classification approach to improve data governance in their specific sectors. For example, in the financial sector, according to *Guidelines for Data Security Classification* released by People's Bank of China ("**PBOC**") in September 2020, "financial data" (defined as various types of data that are collected or generated by financial institutions in the course of their operation) shall be classified into five levels based on the impact on national security, public interests, interests of personal information subject, and lawful interests of enterprises, if such data is damaged. Level 1 data includes, for instance, personal information that is voluntarily disclosed by individuals, and can be disclosed publicly. Data ranging from level 2 to level 4 include personal information collected by financial institutions for their daily operations, such as password and account number. Level 5 data includes data processed by large-scale financial institutions to provide "critical" services or data that would threaten national security or harm public interests if compromised.

Similarly, the Ministry of Industry and Information Technology ("**MIIT**"), China's telecom regulator, released the *Data Classification and Grading Method of Basic Telecommunication Enterprises (*"**Telecommunication Method**"*)* in December 2020, which provides guidance for the classification of data generated by basic telecommunication service providers. The Telecommunication Method similarly categorizes data into four levels according to its impact on national security, public interests, company interests, or users' interests if the data is leaked.

3. Data Security Obligations on Entities

The second draft of the DSL specifically highlights that entities carrying out data processing activities must comply with the data security requirements under the MLPS (Article 26), under which the government classifies companies' networks physically located in China according to their relative impact on national security, social order, and economic interests, if the system is damaged or attacked. Consistent with the CSL and its proposed implementing regulations, networks classified at level 3 or above are subject to enhanced security requirements. Further, the above data processing entities are required to establish a system to ensure data security, which includes training personnel and implementing other technical measures (Article 26).

4. Cross-border Transfer of Important Data

Another highlight of the second draft of the DSL is that it introduces separate frameworks for the cross-border transfer of "important data" by CII operators and other non-CII data processing entities (Article 30), while the details of such transfer requirements are not included in the draft itself.

- Transfer by CII operators. The second draft states that CII operators must follow the rules established under the CSL, which require CII operators to locally store "important data" that is collected or generated in China and undergo a security assessment conducted by designated agencies, if the cross-border transfer is necessary for business needs.
- Transfer by other data processing entities. Data processing entities that are non-CII operators are required to follow separate cross-border data transfer rules to be published by the Cyberspace Administration of China ("CAC") and other government agencies.

5. **Request for Data by Foreign Judicial or Law Enforcement Organs**

   Finally, the second draft of the DSL stipulates that where a foreign judicial or law enforcement organ requests for data that is "stored" within China, such data shall not be provided unless China's "competent government agency" has approved such a provision (Article 35). Where treaties or agreements concluded or participated in by China have relevant provisions about transferring data based on foreign requests, it is allowed to act in accordance with those provisions (Article 35).

   Note that Article 41 of the second draft of the PIPL includes a parallel prohibition on transferring personal information that is stored in China to a judicial or law enforcement organ outside of China without approval. It is unclear how to define data "stored in China" and how a data processing entity can apply for the approval at this time.

Personal Information Protection Law: Key Changes in Second Draft

The NPC released the first draft of the PIPL on October 21, 2020 (Covington alert available here) for public comments. The second draft largely follows the structure of the first draft but also introduces a few new obligations on personal information processing entities, which is defined as an "organization or individual that independently determines the purposes and means for processing of personal information," a term that is largely consistent with the "data controller" concept under European Union's General Data Protection Regulation ("**GDPR**").

Below we discuss five key changes of the second draft of the PIPL from its first draft.

1. **Legal Basis for Processing Personal Information**

   Under the second draft of the PIPL, personal information processing entities can only process personal information when consent has been obtained or under the following circumstances (Article 13):

   - 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;
   - processing personal information that is already made public and such a processing must be carried out for reasonable purposes in compliance with the draft PIPL;

- 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.

The second draft of the PIPL clarifies that consent is not required if the processing is based on any of the legal basis listed above. At the same time, the PIPL still requires a separate consent if the processing entity shares personal information to others, processes sensitive personal information and transfers personal information overseas (Article 24, 30, and 39). It is possible to interpret the newly added language of Article 13 to mean that only if the processing is based on consent at the time of collection, a separate consent will be required before sharing personal information and processing sensitive personal information. But it is less certain whether a processing entity might still need to obtain consent from personal information subject before transferring personal information abroad even if the processing is based on grounds other than consent.

2. Cross-border Transfer of Personal Information

Comparing with the first draft, the only change introduced in the second draft of the PIPL about the cross-border transfer of personal information is that if a processing entity chooses to transfer personal information overseas by signing a transfer agreement, it must use the "standard contract" published by the CAC.

The rest of the requirements stay the same, including obtaining a separate consent for cross border transfers (potentially only when consent is the legal basis for processing) (Article 39), carrying out an internal risk assessment prior to cross-border transfer, and keeping records of such transfers (Article 55), and finally choosing one of the following mechanisms to transfer personal information abroad (Article 38):

- undergo a security assessment administered by the CAC (requirements for CII operators and processing entities that transfer a "large" volume (to be specified by the CAC) of personal information);
- obtain certification from "professional institutions" in accordance with the rules of the CAC;
- enter into a transfer agreement with the overseas recipient based on a "standard contract" to be published by the CAC; or
- transfer mechanisms in other laws and regulations (or the CAC presumably through implementing regulations).

3. Obligations of Processing Entities and Entities Entrusted to Process Personal Information

Consistent with the first draft, Chapter 5 of the second draft requires personal information processing entities to take organizational and technical measures to ensure the security of personal information, which include, for example, establishing internal management systems and implementing encryption protection measures (Art. 51). This also includes requiring processing entities located outside of China to establish a "dedicated office" or appoint a "designated representative" in China to be responsible for matters related to the protection of personal information (Article 53).

Note that the second draft adds that entities which are entrusted to process personal information (these parties that are likely to be considered as "data processor" under the GDPR), shall also fulfill all obligations under Chapter 5 (Article 58). This new requirement could mean, for example, that companies entrusted by other entities to process Chinese personal information, namely acting as data processors rather than controllers, may have to set up offices or appoint designated representatives in China and comply with obligations under the PIPL. If implemented, this requirement could greatly impact offshore data processors that do not have business presence in China, even though it is still unclear how the implementation will roll out.

4. Obligations on Large Scale Platforms

One of the most significant changes made by the second draft of the PIPL is Article 57, which requires "basic Internet platform service providers" that have a massive number of users and operate complex types of businesses ("**Platform Provider**") to fulfill the following obligations:

- establish an independent external supervising body comprised of external personnel to supervise the Platform Provider's personal information processing activities;
- cease to provide services to products/services providers operated on the platform (e.g. merchants on e-commerce platforms), if they seriously violate personal information processing requirements under applicable laws and regulations; and
- publish "personal information responsibility reports" on a regular basis.

5. Enforcement and Penalty

Both drafts of the PIPL state that agencies investigating potential violations of the PIPL have the power to interview, investigate, consult and obtain copies of relevant documents, conduct on-site inspections, and inspect devices and items related to personal information processing activities (Article 62). The second draft adds that if officers need to inspect devices or objects that are related to illegal personal information processing activities, they should obtain internal approval (Article 62). Also, the second draft of the PIPL empowers agencies to request the processing entity to appoint a "professional institution" to conduct a compliance audit for the processing entity if the agencies find certain processing activities are risky or security accidents are likely to occur (Article 63).

Finally, the second draft makes an important change about how burden of proof is allocated in personal information related litigation. According to Article 68, if an individual asserts a claim in the court that his/her personal information rights are infringed as a result of an entity's personal information processing activities, the processing entity bears the burden of proof. If the processing entity cannot prove that it is not at fault, it shall be liable for tort damages.

* * *

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
Sean Stein	+86 10 5910 0520	sstein@cov.com
Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@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.