Legal Commentary

October 28, 2020

HAN KUN
汉坤律师事务所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Brief Comments on the Draft Personal Information Protection Law

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU

On October 21, 2020, the Standing Committee of the National People's Congress officially released the draft for the first reading of the ***Personal Information Protection Law*** (the **"Draft Law"**). This marks the initial unveiling of China's first law dedicated to the protection of personal information.

The Draft Law follows the global trend of strengthening the protection of personal information. Meanwhile, it also embodies distinctive Chinese characteristics and intends to set out the basic regime for personal information protection in a comprehensive and systematic fashion. The Draft Law reflects, develops and enhances the personal information protection framework outlined in the *Civil Code* and the *Cybersecurity Law* (the **"CSL"**). Moreover, the Draft Law also draws on lessons from the EU General Data Protection Regulation (the **"GDPR"**) and other mainstream personal data protection laws in terms of the definition of personal information, extraterritorial effect, penalties (a fine up to 50 million RMB (around 7.4 million USD) or 5% of annual turnover) and the legal basis for personal information processing, which marks a breakthrough among existing laws and regulations. In addition, it is clear that legislators have considered the special needs of the Internet, artificial intelligence, digital marketing and other big data industries and have endeavored to reach a balance between the free and orderly flow and protection of personal information. Certain provisions are more tailored and operable than under previous draft laws and regulations, such as those relating to cross-border data transfers, legal basis for data processing, and the application of individual rights, which provide safeguards for promoting the effective circulation and development of data.

Identification and relation: an expanded definition of personal information

Article 4 of the Draft Law defines personal information as "any information relating to an identified or identifiable natural person which has been recorded in electronic or other form, excluding anonymized information". This provision further adds a "relation" criterion to the basis for defining personal information with "identification" as its core under the CSL and the Civil Code.

- "Identification" emphasizes "information to person". "Identification" as used in the definition of personal information does not require that a natural person actually be identified, merely that such information can be used to identify a certain person within a specific group. For example, although

a device number cannot identify a natural person without a mobile phone number, name, or identification number, it still falls within the scope of personal information because it is unique and can be used to identify a natural person within a user group.

- "Any information relating to identified or identifiable natural persons" reflects the new "relation" criterion. Relation emphasizes "person to information". For example, although information reflecting the activities or hobbies of a particular natural person may be neither unique nor identifiable, it should still be regarded as personal information.

From the perspective of comparative law, many foreign laws such as GDPR mainly combine "identification" and "relation" criteria to define personal information. In addition, earlier Chinese judicial interpretations and voluntary national standards, which serve as important references in regulatory enforcement, have used the "relation" criterion, such as, respectively, the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information* and the *Information security technology: Personal information security specification* (the **"PI Specification"**). The Draft Law absorbs past practical experience and includes a "relation" criterion, which we believe would provide for more comprehensive and adequate protection of personal information.

Another highlight of the definition of personal information is that anonymized information is not excluded from personal information. The Draft Law distinguishes "anonymization", which means *"the processing of personal information to the extent that the information cannot identify or link to a particular individual and cannot be recovered"*, and "de-identification", which means *"the processing of personal information that is impossible to identify or associate a particular individual without additional information."* Anonymized information is usually statistical information and has lost individual "granularity", while de-identification is usually achieved via deletion or transformation of the identifier. However, a case-by-case examination would still be required to determine whether certain information is anonymized, and hence not subject to protection, or merely de-identified and still subject to protection.

Extraterritorial effect: long-arm jurisdiction in cross-border scenarios

Currently, the CSL and other laws or regulations mainly apply to domestic network operators. However, in practice, many overseas operators do not establish entities in China while directly collecting domestic individuals' personal information through cross-border services. It is not entirely clear whether China's relevant laws and regulations on personal information protection apply to these overseas operators.

Article 3.2 of the Draft Law fills this gap, providing that "this Law applies to the overseas processing of personal information of natural persons within the territory of China, where the processing activities are related to (a) the offering of goods or services, or (b) analysis or evaluation of the behavior of domestic natural persons." This provision is similar to the "targeting" criterion and "monitoring" criterion established by the Article 3 of GDPR, regarding territorial scope. In reference to the GDPR-related guidelines and the *Information Security Technology: Guidelines for Cross-Border Data Transfer Security Assessment (Draft for Comment)*, overseas operators may be subject to the Draft Law under Article 3.2 where they provide services in Chinese, use Chinese currency, offer the delivery of goods targeting users in China, or

create profiles of Chinese users.

Article 52 of the Draft Law further provides that overseas operators shall establish a special organization or designate a representative in China to be responsible for affairs relating to personal information protection, and the name and contact information of such organization or representative is to be record-filed with the personal information protection regulatory authorities. However, the Draft Law does not specify the qualifications or legal duties of such organizations and representatives. Additionally, the Draft Law also provides that the Cyberspace Administration of China (**"CAC"**) may add to a blacklist and restrict or prohibit the provision of personal information to foreign organizations and individuals whose personal information processing activities harm the rights and interests of Chinese citizens or endanger China's national security and public interests.

PI Processors and entrusted parties: boundary to be clarified for entrusted processing relationships

Similar to the Civil Code, unlike GDPR, the Draft Law does not distinguish data controllers and data processors, rather it uses the concept of "personal information processor" (**"PI Processor"**), which refers "an organization or individual that on its own decides the purpose or means of personal information processing matters."

Although the Draft Law does not distinguish "controller" and "processor", it still provides the following special rules on "entrusted processing" of personal information:

- PI Processors shall make an agreement with the entrusted party regarding the purposes and means of the entrusted processing, the types of personal information to be processed, protection measures, and the rights and obligations of both parties, and supervise the entrusted party's personal information processing activities;
- The entrusted party shall process personal information in accordance with the agreement and not process personal information exceeding the agreed-upon purposes, means, and so forth. After the agreement is performed or the entrustment relationship is terminated, the personal information shall be returned to the PI Processor or deleted;
- Without the consent of the PI Processor, the entrusted party shall not further entrust others to process the personal information.

Superficially, "PI Processor" and the entrusted party are similar to the "controller" and "processor" under GDPR, while it is not clear whether they are complete equivalents. For example, under the Draft Law, only PI Processors, who decide the "purpose and means of processing", are subject to security guarantee obligations (Article 50), remedial measures for personal information leakage (Article 55), interviews (Article 60), and liability for damages (Article 65). If "PI Processor" is equivalent to "controller" under GDPR, not applying the aforesaid rules to the entrusted party may create loopholes for personal information protection. In addition, in some "entrusted processing" scenarios, case-by-case examination would still be required to determine whether a party would be deemed a joint processor, rather than an entrusted party, based on its greater decision-making power over the "purpose and means of processing".

Legal basis for personal information processing: not limited to "consent"

According to Article 41 of the CSL, network operators must, without exception, obtain consent before processing personal information. This provision emphasizes individual rights and served to crack down on rampant infringement of personal information at the time of the CSL's promulgation, such as stealing, selling, or secretly collecting personal information. However, with the development of personal information protection practice, it has been difficult for companies to obtain user consent in increasingly diverse and complex scenarios, and the quality of consent is continually challenged by users and authorities. The Civil Code for the first time under law provides "exceptions to obtaining consent", which are limited processing public information and safeguarding the public interest or the rights and interests of natural persons. The PI Specification and some other voluntary national standards provide additional exceptions and distinguish consent requirements for different types of personal information processing; but, due to their non-binding effect, companies still face great uncertainty in relying on these exceptions in practice.

In order to resolve these practical problems, the Draft Law for the first time adds, in addition to individual consent, other legal bases for personal information processing, which include:

- Necessary for the conclusion or performance of a contract to which the information subject is a party;
- Necessary for the performance of legal duties or obligations;
- Necessary for responding to public health incidents or to protect natural persons' security in their lives, health, and property in an emergency;
- To the extent reasonably necessary, for news reporting and media supervision for the purpose of protecting public interests; and
- Other circumstances provided by laws and administrative regulations.

We take the view that more legal bases for personal information processing stipulated in the Draft Law can provide choices for PI Processors, improve the quality of consent, make consent more authentic, effective and targeted, and enhance the control of individuals over their personal information.

"Informed consent": differentiated context-based requirements and information subject's rights to choose

Adding more legal bases for personal information processing does not mean that consent is no longer important. On the contrary, based on the regulations and national standards such as the *Measures for Identifying the Illegal Collection and Use of Personal Information by Apps*, the PI Specification and other enforcement experiences, the Draft Law details requirements for "informed consent", so as to ensure that individuals can grant valid consent to specific personal information processing. The main provisions of the Draft Law on "informed consent" are as follows:

- **Notification content requirements**: Notification should include the identity and contact information of the PI Processor; the purpose and means of processing personal information, the type of personal information processed, and the storage period, and the means and procedures by which individuals

may exercise their rights under the Draft Law;

- **Exceptions to notification**: (1) Where laws or administrative regulations provide that secrecy shall be preserved or notification is not necessary, the PI Processor is permitted not to notify individuals; or (2) in an emergency situation, where it is impossible to notify individuals in a timely manner to protect people's lives, health and property, the PI Processor shall notify the individual after the emergency is eliminated;
- **Informed consent**: PI Processors shall obtain individuals' prior consent based on adequate notification. Laws and administrative regulations may also require separate consent or written consent in some scenarios;
- **Obtain consent again for secondary use of personal information**: Where there are changes to the purpose or means of processing information, or to the type of personal information to be processed, the individual's consent shall be re-obtained;
- **Freely given consent**: PI Processors shall not refuse to provide products or services on the grounds that individuals do not grant or withdraw consent to the processing of their personal information;
- **Withdrawal of consent**: Individuals have the right to withdraw their consent to personal information processing based on their consent;
- **Mergers and divisions**: Before PI Processors transfer personal information to any third party as a result of mergers, divisions, and so forth, the individuals shall be informed of the identity and contact information of the recipient party. Where the recipient party changes the original purpose or means of processing, it shall notify the individuals and obtain their consent again in accordance with the provisions of the Draft Law;
- **Provision to third party**: Where a PI Processor provides personal information to a third party, it shall inform the individuals the identity and contact information of the third party, the purposes and means of processing, and the type of personal information to be processed, and shall obtain independent consent from the individuals;
- **Process public personal information**: When processing public personal information, PI Processors shall adhere to the purpose of the disclosure of the personal information; where it exceeds the reasonable scope in relation to the purpose, the individuals' consent shall be obtained again. PI Processors shall decide whether the purpose of processing is compatible with the disclosure purpose in a reasonable and careful manner.

Sensitive personal information processing: no unnecessary processing

The Draft Law for the first time defines under law "sensitive personal information", which means the "information that once leaked or illegally used may cause individuals to suffer discrimination or serious harm to the security of their person and property, including information such as race, ethnicity, religious beliefs, personal biometric characteristics, medical health, financial accounts, personal whereabouts and so forth." The Draft Law has a special section which provides higher protection requirements for sensitive

personal information processing:

- PI Processors shall have a specific purpose and sufficient need to processes sensitive personal information;
- In addition to general notification matters, when processing sensitive personal information, PI Processors shall inform individuals of the necessity of processing sensitive personal information and the impact on the individuals;
- If a PI Processor processes sensitive personal information based on individuals' consent, such consent shall be obtained separately;
- Where laws and administrative regulations provide that processing of sensitive personal information requires obtaining related administrative licenses or imposes stricter restrictions, those provisions shall prevail;
- PI Processor shall conduct risk assessments before processing sensitive personal information and make a record of the processing.

In addition, considering images and videos of public places may involve sensitive personal information such as personal whereabouts and biometric information and are often abused in practice, the Draft Law provides that the installation of video devices or personal identification devices in public places shall be necessary to safeguard public safety and shall set up clear notification signage. Personal images or personal identification information collected through devices may in principle only be used for the purpose of safeguarding public safety and shall not be disclosed or provided to others.

Individual rights: right to know and control

The Draft Law provides a special chapter on information subject rights to emphasize their importance, including the right to know, the right to determine, the right to restrict, the right to object, the right to access, the right to correct, the right to delete, the right of explanation, and the right to object to automated decision-making. The highlights of this part mainly include:

- The Draft Law for the first time proposes the right to restrict and the right to object, meaning that individuals have the right to limit or reject the processing of their personal information, except as otherwise provided by laws and administrative regulations;
- The Draft Law details the conditions that apply to the right to delete, including: (1) the agreed period of retention expires or the purposes of processing are achieved; (2) the PI Processor stops providing products or services; (3) individuals withdraw their consent; (4) the PI Processor processes personal information in violation of laws, administrative regulations, or agreements; and (5) other circumstances provided by laws and administrative regulations. However, PI Processors need only to stop processing such personal information if the retention period prescribed by laws and administrative regulations has not expired or deletion of personal information is technically infeasible;
- The Draft Law for the first time proposes the right of explanation, which means that individuals have the right to request that PI Processor explain their rules of personal information processing.

To address controversies in practice, such as those regarding personalized displays and price discrimination, the Draft Law provides special rules for "automated decision-making". "automated decision-making" refers to analyzing, evaluating, and making a decision by automated means with that individual's information in respect of an individual's behavior, habits, hobbies or economic, health, credit status, and so forth:

- Automated decision-making shall ensure transparency in decision-making and the fairness and reasonableness of the processing results;
- Where individuals believe that automated decision-making has a significant impact on their rights and interests, they have the right to request an explanation from the PI Processor and have the right to refuse the PI Processor's decisions solely through automated decision-making;
- Where commercial marketing and information push are conducted through automated decision-making, the PI Processor shall provide options not to target individuals' specific personal characteristics.

In current practice, most companies have not yet established a comprehensive mechanism to allow for the exercise of individual rights. Therefore, if the relevant provisions of the Draft Law come into effect, it will pose a significant challenge for corporate compliance. Meanwhile, the Draft Law does not provide more details on the conditions, time limit, fees charged, and means of information subject rights, which will need further clarification by regulatory authorities in their enforcement activities.

Cross-border data transfer compliance: multiple mechanisms for different scenarios

The cross-border transfer of personal information is the area in the Draft Law that attracts the greatest attention of multinationals. The Draft Law provides an array of mechanisms based on different levels of risk relating to national security under different transfer scenarios.

- The Draft Law provides the same requirements as the CSL for critical information infrastructure operators ("**CIIOs**"). CIIOs are required to apply for a security assessment organized by CAC before exporting the personal information abroad;
- Similar to previous provisions of the *Measures on Security Assessment of Personal Information and Important Data to be Exported (Draft for Comment)*, PI Processors are required to fulfill the same requirements as CIIOs if the volume of data they process reaches certain quantitative thresholds set by CAC;
- In other circumstances, if it is necessary for PI Processors to provide personal information outside of China due to business needs, they can choose one of the following ways: (1) completing a CAC security assessment; (2) passing certification on personal information protection conducted by qualified certification institution; (3) entering into an agreement with the overseas recipient to specify the rights and obligations of both parties and supervising the recipient's personal information processing activities; (4) other conditions provided by laws, administrative regulations, or provisions of CAC. It is apparent that PI Processors under the Draft Law have more convenient choices available in addition to prior security assessments compared with the *Measures on Security Assessment of Personal Information to be Exported (Draft for Comment)* and other draft rules;

- The Draft Law clearly states that prior approval of relevant regulatory departments shall be obtained before providing personal information for international judicial assistance or administrative law enforcement assistance. This provision reiterates the emphasis on the importance of data sovereignty and rebuts some countries' access to overseas data based on their national laws.

In short, we believe that the Draft Law proposes multiple mechanisms for cross-border data transfers that are more aligned with the international mainstream. While ensuring national security and personal information security, the Draft Law would also reduce the cost of data cross-border transfers, promote orderly and efficient flows and use of personal information, and we expect the Draft Law will be affirmed and welcomed by industry.

Application to public authorities: regulation and restraint

The Draft Law for the first time stipulates the basic requirements for personal information processing by government authorities, which include:

- **Necessary for duties:** Government authorities shall only process personal information to the extent necessary for fulfilling their statutory duties and responsibilities and not exceed the limits of their power and procedures set forth in the laws and regulations;
- **Informed consent and exceptions:** In principle, government authorities shall notify the information subject and obtain their consent when processing personal information, except where notification and consent will impede government authorities' fulfilment of their statutory duties and responsibilities (e.g. where there is a secrecy protection obligation);
- **No disclosure or provision:** government authorities shall not disclose the personal information they process or provide it to other persons, except where laws or regulations provide otherwise or the individual's consent is obtained;
- **Data localization:** Personal information processed by government authorities shall be stored within China. If it is necessary to provide such information abroad, the government authorities shall complete a security assessment.

These government information processing provisions would curb the excessive collection and abuse of personal information by public authorities, which is particularly important in the context of excessive data collection by government authorities during the COVID-19 pandemic. We expect to see in the future more detailed laws and regulations that refine the specific rules for the processing of personal information by public authorities to protect the legitimate rights and interests of citizens.

Punishment and relief: severe penalties and class action lawsuits

The Draft Law imposes significant increases in punishment for violations, which include rectification orders, warnings, and the confiscation of illegal income. Refusal to rectify may lead to a fine of not more than 1 million RMB and, if the violation is serious, and regulatory authorities may impose a fine of not more than 50 million RMB or 5% of annual revenue, order the suspension or cessation of business, and revoke relevant business permits or license. Meanwhile, the person in charge and other personnel directly

responsible may be imposed with a fine from 10,000 to 1 million RMB.

Individuals are usually granted minimal compensation in lawsuits with respect to infringement of personal information and thus lack the incentive to bring civil actions. The Draft Law therefore stipulates that if a PI Processor's violations infringe the rights and interests of a large number of individuals, a lawsuit may be filed on behalf of aggrieved individuals by procuratorates, regulatory authorities in charge of personal information protection, and other organizations designated by CAC (e.g. consumer protection associations). These rules would provide a clear legal basis for procuratorates and consumer protection organizations to bring class actions against violation of personal information.

Summary and perspective

In summary, we take the view that the Draft Law draws on experiences from mainstream foreign laws on personal information protection, absorbs wisdom derived from recent enforcement activities, and effectively responds to practical challenges and difficulties. The Draft Law basically reaches a balance between the protection of personal information, national security, and public interest and the efficient use and flow of personal information.

Although domestic companies have significantly enhanced their personal information compliance, there still exist noticeable compliance gaps in meeting protection requirements under the Draft Law, particularly in terms of informed consent, information subject rights, risk assessment, and cross-border transfers of personal information.

Multinationals may have established more robust personal information protection policies in accordance with GDPR or other foreign laws or regulations. However, their domestic entities may not have fully implemented such policies, or, even if fully implemented, may still need to be adjusted and localized in light of special requirements proposed under the Draft Law. We recommend that, before the Draft Law comes into effect, companies should utilize this time to prepare for the forthcoming *Personal Information Protection Law*, including conducting gap analyses, mapping compliance risks, adopting and adjusting compliance schemes and improving current levels of protection, so as to avoid the risk of administrative punishment, civil compensation, or even criminal penalties.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com