HAN KUN
汉坤律师事务所
Han Kun Law Offices

Han Kun Newsletter

Issue 162 (10th edition of 2020)

Legal Updates

1. PBoC Releases Guidelines for Financial Data Classification

Authors: TieCheng YANG | Yin GE | Ting ZHENG | Virginia QIAO

On 23 September 2020, the People's Bank of China ("**PboC**") issued the *Financial Data Security - Guidelines for Data Security Classification (JR/T 0197-2020)* (《金融数据安全 数据安全分级指南(JR/T 0197-2020)》) (the "**Financial Data Classification Guidelines**"). Based on the *Cybersecurity Law of the People's Republic of China*(《中华人民共和国网络安全法》) (the "**Cybersecurity Law**") and the existing data protection rules, the Financial Data Classification Guidelines put forward systematic and specific requirements in the field of data classification for financial institutions. In this legal commentary, we will analyze the key points of the Financial Data Classification Guidelines from the perspective of corporate compliance, with a focus on how the new requirements under the Financial Data Classification Guidelines overlay existing regulations and standards.

Background and principle of "data classification" - *What is the purpose for issuing the Financial Data Classification Guidelines?*

"Data classification" has been one of the key regulatory principles in the field of cybersecurity and data protection. In 2016, the Cybersecurity Law imposed a data classification requirement on network operators, among other security protection obligations. According to Article 21 of the Cybersecurity Law, enterprises, as network operators, are required to take data classification and other security protection measures to prevent data from being disclosed, stolen or tampered with. Furthermore, on 3 July 2020, the Standing Committee of the National People's Congress released a consultation draft of the *Data Security Law of the People's Republic of China* (《中华人民共和国数据安全法(草案)》), which proposed that an overall data protection system be established at the national level, in which data classification and classified protection requirements were specified.

In addition, PRC regulators released a series of consultation drafts which also defined compliance requirements for data classification, e.g., the *Regulations on Classified Protection of Cybersecurity (Consultation Draft)* (《网络安全等级保护条例(征求意见稿)》), the *Measures for Administration of Data Security (Consultation Draft)* (《数据安全管理办法(征求意见稿)》), the *Regulations for Security Protection of Critical Information Infrastructure (Consultation Draft)* (《关键信息基础设施安全保护条例(征求意见稿)》), the *Information Security Technology - Implementation Guides for Data Security Classification (Draft)* (《信息安全技术 数据安全分类分级实施指南(草案)》), etc. There are separate industry-specific data classification guidelines formulated in manufacturing industry and other sectors.

In the financial sector, "data classification" is also a regulatory focus of financial regulators. In September 2018, the China Securities Regulatory Commission issued the *Data Classification Guidelines for Securities and Futures Industry (JR/T 0158-2018)* (《证券期货业数据分类分级指引(JR/T 0158-2018)》) (the "**Securities and Futures Data Classification Guidelines**") which mark the first data classification requirements for the financial sector. However, the applicable scope of the Securities and Futures Data Classification Guidelines only covers securities firms, futures companies and fund management companies.

On 13 February 2020, PBoC and the China Financial Standards Technical Committee issued the *Personal Financial Information Protection Technical Specification (JR/T 0171-2020)* (《个人金融信息保护技术规范(JR/T 0171-2020)》) (the "**Specification**"). The Specification adopts the regulatory principle of "data classification", and classifies the sensitivity of personal financial information into three types: C3, C2 and C1. We provided a detailed analysis on the Specification in our previous Han Kun Legal Commentary, Key Analysis on the Personal Financial Information Protection Technical Specification.

With the development of financial technology and the digital economy, financial data has demonstrated tremendous social and commercial value with increasing complexity. In this context, PBoC issued the Financial Data Classification Guidelines to provide detailed and practical guidance for data classification of financial institutions, helping them to better clarify the subjects of classified data protection, optimize resources and costs for data security protection, and further establish a sound financial data lifecycle management framework.

Expanded scope of "financial industry institutions" - *What is the scope of application of the Financial Data Classification Guidelines?*

The Financial Data Classification Guidelines define the scope of application as "institutions engaging in the financial industry" (collectively, "**Financial Industry Institutions**"), as defined in the *Industrial Classification for National Economic Activities (GB/T 4754-2017)* (《国民经济行业分类(GB/T 4754-2017)》).

As compared with the Securities and Futures Data Classification Guidelines, which cover securities firms, futures companies and fund management companies, the Financial Data Classification Guidelines expand to cover other financial institutions such as commercial banks, insurance companies, trust companies, etc. The Financial Data Classification Guidelines also apply to private fund managers (including institutions such as PFM, QDLP and QDIE), third-party payment companies, credit information agencies, etc. Additionally, due to the correlation between industries and the flexibility for interpreting the scope of application, the Financial Data Classification Guidelines may also have an indirect impact on institutions engaging in data security evaluation and assessment, such as third-party data evaluation agencies.

It is noteworthy that although the Financial Data Classification Guidelines and the Specification both apply to "financial industry institutions" from a literal reading, they define this term differently. Under the Specification, "financial industry institutions" include "licensed financial institutions supervised and regulated by the financial regulatory authorities in China, and the relevant institutions involved in the personal financial information processing", which means the Specification directly applies to licensed financial institutions including banking financial institutions, securities firms, fund management companies and insurance companies, as well as related institutions that process personal financial information (which may or may not be licensed), such as third-party payment companies, credit information agencies, etc. Additionally, although PFM/QDLP managers are not "licensed financial institutions" in a strict sense, if they process any customer's personal information in providing financial services, they should also observe the Specification as the "institutions processing personal financial information".

We set out below a table summarizing by different types of institutions the applicability of the Specification, the Securities and Futures Data Classification Guidelines and the Financial Data Classification Guidelines:

Type of institutions	Specification	Securities and Futures Data Classification Guidelines	Financial Data Classification Guidelines
Licensed financial institutions of securities and futures business (i.e. securities firms, futures companies, and fund management companies)	√ (Applicable to "personal financial information" processed by such institution)	√	**Optional** (The Securities and Futures Data Classification Guidelines could be followed instead)
Other licensed financial institutions (including commercial banks, insurance companies, trust companies, etc.)		×	√ (Applicable to "financial data" of institutions)
Private fund managers (including institutions such as PFM, QDLP and QDIE)			
Third-party payment companies			
Credit information agencies			

It should be noted that the Financial Data Classification Guidelines are only voluntary standards for the financial industry, rather than mandatory standards. While at the current stage the Financial Data Classification Guidelines are not compulsory in their application and retain a certain degree of flexibility, provisions of voluntary standards can, in practice, either be directly referenced in or integrated into subsequent compulsory provisions. We also do not rule out the possibility that the financial regulators may consider the Financial Data Classification Guidelines as an important reference when conducting relevant supervisory inspections or law enforcement actions, and may deem the Financial Data Classification Guidelines as practical guidance or operating guidelines for Financial Industry Institutions.

Therefore, we recommend that Financial Industry Institutions comply with the relevant standards and requirements as set out in the Financial Data Classification Guidelines to minimize any legal or compliance risks in relation to financial data classification.

Scope of "financial data" - *What are the financial data to be classified?*

The Financial Data Classification Guidelines focus on the classification of "electronic data" required or generated by Financial Industry Institutions in (i) carrying out business activities; (ii) providing financial services; and (iii) carrying out day-to-day operations and management. The financial data covered by the Financial Data Classification Guidelines include but are not limited to the following four types:

Type 1: Electronic data collected directly (or indirectly) by Financial Industry Institutions during the provision of financial products or services to clients.

Type 2: Electronic data generated and/or stored in the information systems of Financial Industry Institutions, including business information, transaction data, operation and management data, etc.

Type 3: Electronic data generated, transferred and/or stored in the internal office networks of Financial Industry Institutions, including administrative information, internal notices and e-mails, etc.

Type 4: Electronic data generated from the original paper-based documents of Financial Industry Institutions through scanning or other electronic means.

It should be noted that the Financial Data Classification Guidelines do not cover data which constitutes "state secrets". Financial data involving "state secrets" is instead handled in accordance with the relevant national laws and regulations promulgated by the relevant PRC authorities in respect of state secrets' protection, e.g., the *Law of the People's Republic of China on Guarding State Secrets* (《中华人民共和国保守国家秘密法》), the *Regulations for the Implementation of the Law of the People's Republic of China on Guarding State Secrets* (《中华人民共和国保守国家秘密法实施条例》), the *Interim Provisions on Administration of Classifying State Secrets* (《国家秘密定密管理暂行规定》), etc.

Standards on financial data classification - *How will financial data be classified?*

Similar to the Securities and Futures Data Classification Guidelines, the Financial Data Classification Guidelines adopt a multi-level data classification system based on the two key indicators of "impacted areas" and "degree of impact". According to the Financial Data Classification Guidelines, Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, in descending order of importance, by evaluating the "impacted areas" and the "degree of impact" in the event of data leakage or destruction.

Among others, "impacted areas" include national security, public rights and interests, personal privacy, legitimate rights and interests of enterprises, etc. "Degree of impact" could be measured as "serious damage", "ordinary damage", "minor damage" or "no damage". Financial Industry Institutions may carry out data classification by reference to the following matrix:

Minimum level	**Key indicators for data classification**		**Key features and examples**
	Impacted area	**Degree of impact**	
5	National security	Serious damage/ordinary damage/minor damage	■ "Important data" of Financial Industry Institutions. ■ Used for critical business activities of large or ultra-large Financial Industry Institutions and key financial trading platforms. ■ Disclosed to specific personnel on a "need-to-know" basis only.
	Public rights and interests	Serious damage	
4	Public rights and interests	Ordinary damage	■ Used for important business activities of large or ultra-large Financial Industry Institutions and key financial trading
	Personal privacy	Serious damage	

Minimum level	Key indicators for data classification		Key features and examples
	Impacted area	Degree of impact	
	Legitimate rights and interests of enterprises	Serious damage	platforms. ■ Disclosed to specific personnel on a "need-to-know" basis only. ■ **Personal financial information (C3)** under the Specification.
3	Public rights and interests	Minor damage	■ Used for critical and important business activities of Financial Industry Institutions. ■ Disclosed to specific personnel on a "need-to-know" basis only. ■ **Personal financial information (C2)** under the Specification.
	Personal privacy	Ordinary damage	
	Legitimate rights and interests of enterprises	Ordinary damage	
2	Personal privacy	Minor damage	■ Used for general business activities of Financial Industry Institutions. ■ Disclosed to a specific scope for internal use only. ■ **Personal financial information (C1)** under the Specification.
	Legitimate rights and interests of enterprises	Minor damage	
1	National security	No damage	■ Disclosed to or accessible by the public. ■ Voluntarily disclosed by the natural person subjects of personal financial information themselves.
	Public rights and interests	No damage	
	Personal privacy	No damage	
	Legitimate rights and interests of enterprises	No damage	

It is noteworthy that Schedule A (*Table of Data Classification Rules*) of the Financial Data Classification Guidelines further provides a comprehensive summary of data samples and their corresponding levels for data classification. Detailed evaluation standards are further provided in the Financial Data Classification Guidelines.

Process of financial data classification - *How would Financial Industry Institutions carry out data classification?*

Based on overall data classification process set out in the Financial Data Classification Guidelines, Financial Industry Institutions should themselves internally determine and approve data security classifications. The Financial Data Classification Guidelines specify the internal process for data security classifications covering the following five steps:

Step 1 (Formulation of data asset inventory)
■ Review and sort electronic data of the institution ■ Develop a unified inventory of data assets
↓
Step 2 (Preparation for data security classification)
■ Determine the granularity of data classification ■ Identify key data security classification elements
↓
Step 3 (Determination of data security levels)
■ Determine data security levels ■ Formulate separate data inventories at different security levels
↓
Step 4 (Review of data security levels)
■ Check and review the whole process and results of data security classification
↓
Step 5 (Approval of data security levels)
■ Final approval of data security levels by the institution's highest decision-making body

According to the Financial Data Classification Guidelines, a Financial Industry Institution should determine its "highest decision-making body" for data security classification, e.g., set up a data security management committee for the institution. In addition, a Financial Industry Institution should define an organizational structure, with clear roles and responsibilities divided among its departments and staff. No regulatory approval is required for the data classification results at the current stage.

Data protection requirements - *How would Financial Industry Institutions protect their financial data?*

According to the Financial Data Classification Guidelines, Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, in descending order of importance. Comparatively, the Specification divided the sensitivity levels of personal financial information into three types: C3, C2 and C1. Although the Financial Data Classification Guidelines do not directly set data protection requirements for Financial Industry Institutions, it is noteworthy that the Financial Data Classification Guidelines specify correlations with the Specification, namely:

1. C3 data under the Specification should correspond with Level 4 data under the Financial Data Classification Guidelines;

2. C2 data should correspond with Level 3 data; and

3. C1 data should correspond with Level 2 data.

In light of the above, upon determination of the data classification from Level 1 to Level 5, Financial Industry Institutions should observe by reference the corresponding data protection requirements as set out in the Specification, for instance:

1. Financial Industry Institutions should refrain from appointing or authorizing any institutions without the relevant financial licenses to collect C3 or C2 information. To collect C3 information, relevant technical measures such as encryption should be taken to prevent any unauthorized third party from obtaining such information;
2. to transmit sensitive payment information among C3 information, Financial Industry Institutions should adopt relevant control measures that conform to industry technical standards as well as the requirements of industry authorities;
3. in principle, a Financial Industry Institution should not retain C3 information which it does not own. Where there is a specific need, such retention should be authorized by the information subjects and the account management institutions;
4. in principle, Financial Industry Institutions should refrain from appointing third-party institutions to process C3 personal financial information and auxiliary user identification information (such as text message verification codes) among C2 personal financial information;
5. C3 information or auxiliary user identification information among C2 information should not be shared, transferred or disclosed; and
6. outsourcing service institutions and external cooperation institutions should be prohibited from retaining C3 and C2 information by contract or agreement.

Outlook - *What do we expect regarding regulatory trends?*

Compared with the existing laws and regulations, the Financial Data Classification Guidelines are more practical and thus can play an important guiding role in compliance practices for Financial Industry Institutions, which may further lay the foundation for standardized data protection and data lifecycle management in the financial industry. We anticipate that PBoC and other financial regulators may formulate and issue detailed implementing rules in this regard.

In addition, although the Financial Data Classification Guidelines fill the gap in classified data management and mark a further step in the data protection rules, financial regulators have further room for rulemaking. For instance, although Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, the Financial Data Classification Guidelines do not provide data protection requirements for each level of financial data, which may be further specified in subsequent regulatory rules or national/industry standards.

With the continuous development of the regulatory framework on data lifecycle management and personal information protection in China, we will also continue to monitor relevant regulatory updates and share our views with readers in a timely manner.

2. A Great Leap Forward in R/QFII Liberalization

Authors: TieCheng YANG | Yin GE | Ting ZHENG | Flora WEI

China has the second largest stock and bond markets in the world. By the end of June 2020, foreign investment in China's stock and bond markets amounted to US$737.5 billion, accounting for 4.5% of China's stock markets and 2.4% of China's bond markets. With U.S. trade and diplomatic relations remaining strained, Chinese regulators have been determined to make continuous efforts to accelerate and deepen the opening-up of the country's financial markets. On 25 September 2020, the China Securities Regulatory Commission (CSRC), the People's Bank of China (PBoC), and the State Administration of Foreign Exchange (SAFE) jointly released the *Measures for Administration of Domestic Securities and Futures Investment by Qualified Foreign Institutional Investors and RMB Qualified Foreign Institutional Investors* (《合格境外机构投资者和人民币合格境外机构投资者境内证券期货投资管理办法》) (the "**R/QFII Measures**") and CSRC simultaneously published the *Provisions on Issues Concerning the Implementation of the Measures for Administration of Domestic Securities and Futures Investment by Qualified Foreign Institutional Investors and RMB Qualified Foreign Institutional Investors* (《关于实施<合格境外机构投资者和人民币合格境外机构投资者境内证券期货投资管理办法>有关问题的规定》) (the "**CSRC Implementing Provisions**", together with the R/QFII Measures, the "**R/QFII Rules**").[1]

The R/QFII Rules will take effect on 1 November 2020. It has been over a year and a half since the regulators issued consultation drafts of the R/QFII Rules to solicit public comments in January 2019. During this period of time, PBoC and SAFE revised rules in May 2020 relating to R/QFIIs' onshore capital management, which removed R/QFII quotas, simplified repatriation processes, and unified the relevant rules applicable to R/QFIIs.

As the market expected, the R/QFII Rules mark a great leap forward in further liberalizing China's capital markets. The key highlights of the R/QFII Rules include further combining the QFII and RQFII programs, lowering eligibility requirements, simplifying application processes, expanding investment scopes, and removing limits on the number of onshore service providers which R/QFIIs may engage (including local custodians and securities/futures brokers).

Merging QFII and RQFII programs

QFII and RQFII programs have been subject to separate rules and application procedures. The R/QFII Rules consolidate all QFII and RQFII regulations into one set of unified rules to further harmonize the qualification requirements applicable to R/QFIIs and to mitigate regulatory arbitrage by investors. R/QFIIs are encouraged to use offshore RMB to make domestic investments.

Lowering eligibility requirements

There is no longer any track record or AUM requirement for R/QFII applicants. The major

[1] The full versions of the R/QFII Rules are available at http://www.csrc.gov.cn/pub/newsite/zjhxwfb/xwdd/202009/t20200925_383649.html (in Chinese) and http://www.csrc.gov.cn/pub/csrc_en/newsfacts/release/202009/t20200925_383652.html (in English).

requirements include that an applicant must have securities and futures investment experience and not have received significant regulatory punishments in the past three (3) years or since its inception. Compared to the consultation draft, the R/QFII Measures impose a new eligibility requirement: the applicant may not have significant impact on the operation of China's domestic capital markets, which leaves more discretion with CSRC in the application review process.

Simplification of application process

The R/QFII application process is further simplified and there are no longer time-consuming notarization or certification requirements; CSRC's review timeline has been shortened from 20 working days to 10 working days.

Expansion of investment scope

In addition to the currently permissible asset classes, which mainly include A-shares, bonds, public securities investment funds and stock index futures, R/QFIIs will be allowed to invest in:

1. depositary receipts, bond repos and asset backed securities traded on securities exchanges;
2. shares traded on the National Equities Exchange and Quotations;
3. private investment funds;
4. financial futures listed and traded on the China Financial Futures Exchange;
5. commodity futures traded on futures exchanges approved by CSRC;
6. financial products traded on the China Interbank Bond Market and PBoC-approved derivatives products related to bonds, interest rates, and foreign exchange (under current rules, R/QFIIs are only permitted to invest in fixed-income products traded on the China Interbank Bond Market);
7. foreign exchange derivatives products permitted by SAFE for hedging purposes;
8. options traded on exchanges approved by the State Council or CSRC; and
9. other financial instruments permitted by CSRC.

For investments in private investment funds, the underlying investment of the private investment funds must fall within the permissible investment scope of R/QFIIs.

RQFIIs will also be allowed to participate in issuance of asset backed securities, margin trading and securities lending on the exchanges, and securities lending to the securities finance company (currently China Securities Finance Corporation Limited).

Engaging affiliated investment advisors

An R/QFII may engage as its investment advisor a controlled or affiliated domestic private investment fund manager. This means an R/QFII may appoint a PFM manager or potentially a QDLP manager within its group as its investment advisor.

Clarifying securities/futures account structure

The R/QFII account naming requirements are further clarified and asset management R/QFIIs are encouraged to adopt “R/QFII + Client Name” or “R/QFII + Fund” format to specify the underlying investors or products. For omnibus accounts in the name of “R/QFII + Client Assets”, the R/QFII will report relevant information about the underlying investors and their assets in accordance with relevant requirements.

Reporting offshore hedging positions

Under the consultation draft, it was contemplated that R/QFIIs would report to CSRC on a quarterly basis their overseas hedging positions related to the domestic securities/futures investments. Now, the R/QFII Rules merely require reporting upon CSRC’s request based on its regulatory needs.

Enhancing ongoing supervision

The R/QFII Rules have also enhanced ongoing supervision on R/QFIIs, including broker account and transaction monitoring, information sharing by exchanges and depositaries, additional information disclosure on offshore hedging positions related to onshore investment, and the “look-through” approach for underlying investors’ compliance with holding limits and disclosure of interest requirements. For example, the CSRC Implementing Provisions specifically require investors that invest in China’s markets via R/QFIIs (i.e. the underlying clients of R/QFIIs) submit through R/QFIIs the information disclosure materials with relevant stock exchanges if the relevant information disclosure obligations are triggered, and R/QFIIs are required to monitor the onshore shareholdings of their underlying clients and urge those clients to strictly perform their information disclosure obligations. The corresponding penalties for violations are also specified.

Outlook

The R/QFII Rules also make some reservations in terms of investment scope expansion. For example, with respect to the financial futures, commodities futures and options available to R/QFIIs, the specific types and trading models are subject to CSRC’s separate approvals based on the relevant exchange’s proposals. Implementing details may also be required as to R/QFIIs’ participation in margin trading and securities lending on the exchanges, securities lending to the securities finance company, etc.

Given the size of China’s securities markets and the current low level of foreign participation in those markets, there remains great potential for China to continue its opening-up policies. Beyond R/QFII, we expect more initiatives to be rolled out to serve China’s agenda to develop more internationalized capital markets.

3. 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 Newsletter 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:

Beijing	**Wenyu JIN**	**Attorney-at-law**
	Tel:	+86 10 8525 5557
	Email:	wenyu.jin@hankunlaw.com
Shanghai	**Yinshi CAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0980
	Email:	yinshi.cao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com