HANKUN
汉坤律师事务所
Han Kun Law Offices

Han Kun Newsletter

Issue 155 (3rd edition of 2020)

Legal Updates

1. Key Analysis of the Personal Financial Information Protection Technical Specification
2. Key Developments in the Revised Personal Information Security Specification

1. Key Analysis of the Personal Financial Information Protection Technical Specification

Authors: Kevin DUAN | TieCheng YANG | Kemeng CAI | Fangfei LI | Virginia QIAO | Minzhe HU

On 13 February 2020, the People's Bank of China (**"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"**). 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 **"PRC Cybersecurity Law"**) and the regulatory rules previously issued by PBoC on personal financial information protection, the Specification puts forward systematic and specific requirements covering the whole life-cycle of personal financial information processing from the perspectives of security technology and security management. Compared with the existing laws and regulations, the Specification is more practical and thus can play an important guiding role in compliance practices for financial institutions and relevant enterprises in the financial industry. In this commentary, we will analyze the key points of the Specification from the perspective of corporate compliance, with a focus on how the Specification's new requirements overlay existing regulations and standards.

Expanded scope of application: from "banking financial institutions" to "financial industry institutions"

The Specification defines its scope of application as "licensed financial institutions supervised and regulated by the financial regulatory authorities in China, and the relevant institutions involved in the personal financial information processing" (collectively, **"Financial Industry Institutions"**), 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 be licensed or not), such as third-party payment companies, financial technology companies (**"Fintech Companies"**), etc. Additionally, due to the correlation between industries and the flexible room for interpreting the scope of Financial Industry Institutions, the Specification may also have an indirect impact on industries involved in personal financial data processing, such as e-commerce.

In addition, for private fund managers (including institutions such as PFM, QDLP and QDIE), although not licensed financial institutions in a strict sense, they are required to register and make filings with the Asset Management Association of China and accept its supervision. If a private fund manager obtains, stores or processes any customer's personal information[1] in providing the customer with financial products, services or in other channels, the private fund manager should observe by reference the security

[1] Examples: client's account information, identification information, financial transaction information, personal identity information, property information, lending information, and other information that reflect certain circumstances of a particular individual.

technology and management requirements as set out in the Specification.

Comparatively, there have been a series of regulatory provisions on personal financial information protection promulgated by PBoC and the China Banking and Insurance Regulatory Commission (**"CBIRC"**), which mainly include the *Circular of the People's Bank of China on Fulfilling the Work of Protection of Personal Financial Information by Banking Institutions* (《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》) (effective as of 1 May 2011) (the **"PBoC Circular"**), the *Circular of the People's Bank of China on Further Fulfilling the Work of Protection of Clients' Personal Financial Information by Financial Institutions* (《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》) (effective as of 27 March 2012), the *Implementing Measures of the People's Bank of China for Protection of Financial Consumer Rights and Interests* (《中国人民银行金融消费者权益保护实施办法》) (effective as of 14 December 2016) (the **"PBoC Measures"**), and the *Circular of the China Banking and Insurance Regulatory Commission on Printing and Issuing the Guidelines for the Data Governance of Banking Financial Institutions* (《中国银行保险监督管理委员会关于印发银行业金融机构数据治理指引的通知》) (effective as of 21 May 2018). Most of the above-mentioned regulatory provisions only directly apply to banking financial institutions and, in practice, are only applied as a reference by non-banking financial institutions such as wealth management subsidiaries of commercial banks, financial asset management companies, trust companies, auto-financing companies, consumer finance companies and credit agencies.

It should be noted that the Specification is only a voluntary standard for the financial industry, rather than a mandatory standard. While at the current stage the Specification is not compulsory in its application and retains 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 Specification an important reference when conducting relevant supervisory inspections or law enforcement actions, and may deem the Specification as practical guidance or operating guidelines for Financial Industry Institutions in the field of personal financial information protection. Therefore, we recommend that Financial Industry Institutions comply with the relevant standards and requirements as set out in the Specification to minimize any legal or compliance risks in relation to personal financial information protection.

Grading and "scenario-based": differentiated regulatory requirements for personal financial information

The Specification adopts the supervisory principles of "classification and grading" and "scenario-based", dividing the sensitivity levels of personal financial information into three types, C3, C2 and C1, in descending order according to the degree of harm caused in the event of information leakage or tampering to the information security and property security of personal financial information subjects:

- C3 information mainly refers to user authentication information, the leakage of which may result in direct property damage. C3 information includes but is not limited to: account passwords, bank magnetic track data, chip information, card verification codes, card validity periods, and personal biometric identification information for user authentication (e.g., facial recognition, fingerprint recognition);

- C2 information mainly refers to personal financial information that can be used to identify a specific personal financial information subject and his or her financial status, as well as key information used for financial products and services, the leakage of which may result in indirect property damage, discriminatory treatment or harm to information security. C2 information includes but is not limited to: account information, ID card information, auxiliary user identification information (such as text message verification codes), personal property information, transaction information, KYC information, home addresses; and
- C1 information mainly refers to personal financial information used internally by Financial Industry Institutions, including but not limited to: account opening time, account opening institution, payment token information, etc.

Family member information provided by a personal financial information subject should be classified according to the above sensitivity levels. A variety of information in a lower sensitivity level may be combined, correlated, or analyzed to further become information in a higher sensitivity level. The Specification also puts forward, for the first time, requirements for determining the information sensitivity level based on service scenarios. An enterprise should identify and classify information according to the specific service scenarios and the role of the relevant information in such scenarios, and take targeted protection measures.

Please note that C3 and C2 information is generally classified as "personal sensitive information" in the *Information Technology - Personal Information Security Specification* (《信息安全技术 个人信息安全规范》) (the **"Personal Information Security Specification"**), which was promulgated by the National Information Security Standardization Technical Committee (**"NISSTC"**, also known as **"TC260"**) on 30 November 2017, and was last revised on 6 March 2020. However, the Specification, on the basis of various financial service scenarios, puts forward higher protection requirements for C3 and C2 information than those for personal sensitive information under the Personal Information Security Specification:

- 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;
- 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;
- in principle, Financial Industry Institutions should not retain C3 information which such institution does not own. Where there is a specific need, such retention should be authorized by the information subjects and the account management institutions;
- 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;

- C3 information or auxiliary user identification information among C2 information should not be shared, transferred or disclosed; and
- outsourcing service institutions and external cooperation institutions should be prohibited from retaining C3 and C2 information by contract or agreement.

Legitimacy and necessity: personal financial information collection rules with both stringency and flexibility

The lawful collection of data is a prerequisite for the subsequent processing of data in accordance with law. Thus, the Specification focuses on the process of collection in respect of collection methods, data sources and collection scope, etc.

For the direct collection of personal information, Financial Industry Institutions should avoid compelling or misleading personal financial information subjects to provide information through authorization by default or "bundling" of functions. In order to avoid undisclosed collection of personal financial information, the Specification provides that Financial Industry Institutions should conduct technical tests before products or services are released online, to ensure that personal financial information is collected, used, and shared in accordance with laws and regulations, with proper disclosure through relevant privacy policies.

For the indirect collection of personal information, Financial Industry Institutions should require information providers to indicate the sources of personal financial information and ensure the traceability of such information sources through technical measures. Financial Industry Institutions are obliged to confirm the legitimacy of the information sources and understand the authorized contents that the information providers have obtained. Financial Industry Institutions need to undertake higher review obligations, and will find it difficult to exempt themselves from their liability by solely relying on the written contracts or guarantees with information providers.

With respect to the scope of data collection, the Specification explains the "minimization requirement" for data collection, allowing Financial Industry Institutions to collect personal financial information in direct connection[2] with the realization and optimization of financial products or services, and the prevention of the risks of financial products or services. Compared with the common expression of "information unrelated to business must not be collected" in the previous relevant regulatory provisions, the preceding provisions of the Specification are more flexible, retaining a certain degree of flexibility for the collection of personal financial information for the purpose of optimizing financial products or services, and cater to the special needs of risk control in the financial industry.

In addition, the Specification also stipulates exceptional circumstances where the consent of information subjects is not required, i.e., the collection of the personal financial information necessary for the safe and stable operation of financial products or services (such as the information used to identify or manage fraud or misappropriation in financial products or services), or the personal information relevant to the performance of obligations provided by national laws and regulations, as well as the requirements as set

[2] "Direct connection" means that the aforesaid purpose cannot be achieved without the participation of such personal financial information.

out by the relevant industry authorities. This provision leaves more room for Financial Industry Institutions to collect personal financial information for the purpose of conducting risk control or performing obligations in relation to anti-money laundering, anti-terrorist financing, etc.

Desensitization, deletion and destruction: clearer rules for the application and storage of personal financial information

In practice, many Financial Industry Institutions often face the compliance challenge of using personal financial information in product development. Considering the sensitivity of personal financial information, the Specification requires Financial Industry Institutions to effectively segregate the development and testing environment from the production environment. In the actual development and testing, personal financial information should be fictionalized or de-identified and, in principle, actual personal financial information should not be used. Notably, the Specification particularly gives examples of information masking technologies in the appendix, stating that Financial Industry Institutions may apply the masked information in product development and testing activities.

In addition, the Specification also provides that the storage period of personal financial information should follow the requirements of laws and regulations and the industry authorities, and meet the minimum time requirements which are necessary for the authorized use. If the time limit has been exceeded, or if the personal financial information subject requests deletion in accordance with law, Financial Industry Institutions should delete the personal financial information or anonymize such information. Deletion means "the process of making personal financial information unavailable for search and access". In practice, it is worth exploring how to handle personal information once the service relationship has come to an end and the purpose required for authorization has reached expiration, but the institution is still required to retain the information according to the law[3]. In this regard, while Financial Industry Institutions must continue to retain the personal information if legally required to do so, we believe they should avoid use of such information for other purposes.

In addition to deletion, the Specification also provides for the destruction of information, which means "the process of removing personal financial information and making it unrecoverable". Therefore, destruction is stricter than deletion and mainly applies to delegated processing scenarios, i.e., where a third-party institution is appointed to process personal financial information, if the appointment is terminated, the appointed party should be obliged to destroy the personal financial information and continue to assume the corresponding confidentiality responsibilities as required by the Financial Industry Institution. The Financial Industry Institution should also supervise the process of destroying the storage medium and require preservation of the destruction record.

[3] For example, the *Measures for Administration of Verifying Clients' Identities and Preserving Data on Clients' Identities and Transactions Records by Financial Institutions* (《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》) explicitly require the Financial Institutions to preserve client identity information and transaction records for at least five years.

Impact of the Specification on outsourcing activities of Financial Industry Institutions

I The Specification and information technology outsourcing of Financial Industry Institutions

Due to business needs for providing financial products or financial services, Financial Industry Institutions may appoint or authorize third-party institutions such as service providers to handle information technology activities for which they are responsible ("**IT Outsourcing**"). In practice, the IT Outsourcing of Financial Industry Institutions typically covers the following types:

- outsourcing of research and development advisory: outsourcing of advisory and design for technology management and technology governance, and outsourcing of planning, demand, system development and testing;
- outsourcing of systems operation and maintenance: including outsourcing of operation and maintenance of data centers (disaster recovery center), server room support facilities, networks and systems, and outsourcing of operation and maintenance of remote terminals and office equipment such as self-service equipment, POS terminal, etc.; and
- information technology activities in business outsourcing: systems development, operation and maintenance, and data processing activities in outsourcing of market expansion, business operation, enterprise management and asset disposal, etc.

Among the above three types of IT Outsourcing scenarios, the first type "outsourcing of research and development advisory" mainly focuses on technology management framework design and system construction for enterprises; the second type "outsourcing of systems operation and maintenance" mainly aims toward the overall operation and maintenance of information technology systems and facilities. Generally speaking, the above two types of outsourcing activities do not delve deeply into actual business activities of the enterprise, in which Financial Industry Institutions usually do not allow outsourcing service institutions to specifically participate in processing personal financial information.

Compared with the above two types, the third type "information technology activities in business outsourcing" is more closely related to the actual business activities of Financial Industry Institutions. In such IT Outsourcing activities, Financial Industry Institutions should pay special attention to whether the scope of outsourcing services involves appointing third-party institutions to participate in the collection, transmission, storage, use, deletion, destruction, etc. of any personal financial information.

Where the processing of personal financial information is delegated, Financial Industry Institutions should ensure that both themselves and the outsourcing service institutions not only comply with existing regulatory provisions on personal information protection and requirements for security management and security technology in the national standards, but also meet the new requirements for the delegated processing of personal financial information as set out in the Specification.

II Specific requirements in the Specification for the delegated processing of personal financial information

Prior to the promulgation of the Specification, national standards such as the Personal Information Security Specification have set specific security management and technology requirements for

delegated processing of personal information. In light of the industry characteristics of financial products and financial services, the Specification puts forward more detailed security management and technical requirements for Financial Industry Institutions' delegated processing of personal financial information on the basis of applicable laws, regulations and national standards. Please refer to the following table for more detailed information:

Type	Specific requirements in the Specification on the delegated processing of personal financial information
Scope of delegated activities	Delegated activities should not go beyond the scope of authorization and consent of the personal financial information subject (other than exceptional circumstances where authorization is not required).
Scope of delegated information	C3 information or the auxiliary user identification information in C2 information should not be delegated to a third-party institution for processing.
Desensitization of delegated information	The information delegated for processing should be desensitized by methods such as de-identification (not only using encryption technology) to reduce the risk of personal financial information being leaked, misused and abused.
Personal financial information security impact assessments of the delegated activities	Financial Industry Institutions should conduct personal financial information security impact assessments (at least once a year) of delegated activities, and ensure that the delegated party has sufficient data security capabilities and provides adequate security protection measures.
Supervision of delegated parties	Financial Industry Institutions should supervise the delegated institutions such as third-party institutions. The methods include but are not limited to: ■ stipulating the responsibilities and obligations of the delegated party by means of contracts, etc.; and ■ conducting security inspections and assessments of the delegated party (at least once a year).
Technical reviews and audits of externally embedded automation tools	Financial Industry Institutions should conduct technical reviews of the externally embedded or intervened automation tools (such as codes, scripts, interfaces, algorithm models, software development kits, etc.), to ensure that their personal financial information collection and usage behaviors meet the agreed requirements; and conduct audits on activities of financial information collection and cut off access in a timely manner if any activities are found to be beyond the agreement.
Delegated processing records	Financial Industry Institutions should accurately record and preserve the circumstances of the delegated processing of personal financial information.

III Impact of the Specification on big data and Fintech Companies

The stringent standards in the Specification on the delegated processing of personal financial information can be regarded as an extension of the recent PBoC and CBIRC rules which aim to strictly regulate Financial Industry Institutions, big data companies, and Fintech Companies. A presently common practice may face restrictions, whereby Financial Industry Institutions appoint big data companies and Fintech Companies to obtain and verify the information of the borrower's behaviors, e-commerce shopping and living characteristics for loan provisions, anti-fraud, credit review and collection. Before big data companies and Fintech Companies provide such services to Financial Industry Institutions, they may undergo security assurance capability reviews and face qualification restrictions or entry thresholds uniformly set by the regulatory authorities. The provision of data

services and the scope of services may also be narrowed.

Impact of the Specification on cross-border transfers of personal financial information

I Overview of the regulatory system for the cross-border transfer of personal financial information

Data localization and related supervision of cross-border transfer of data have always been a compliance focus for Financial Industry Institutions, especially for multi-national financial group operations in China. In this section, we will briefly review the key regulatory requirements related to the cross-border transfer of personal financial information.

A. The PRC Cybersecurity Law

On 7 November 2016, the Standing Committee of the National People's Congress adopted the PRC Cybersecurity Law which, for the first time, puts forward requirements for data localization and security assessments of cross-border transfers of data by critical information infrastructure operators (**"CIIOs"**):

- the personal information and important data collected and generated by CIIOs during operations within the territory of the PRC shall be stored within the territory of the PRC; and
- where it is truly necessary to provide the information offshore due to business needs, a security assessment shall be conducted in accordance with the measures jointly formulated by the cyberspace administration authority and the relevant departments under the State Council.

In addition, the PRC Cybersecurity Law specifies that, without the consent of the person whose information is collected, network operators shall not provide the personal information to others, which means that network operators must obtain the consent of personal information subjects before transferring their personal information offshore.

B. The Cyberspace Administration of China ("CAC")

Regarding the cross-border transfer of personal information, CAC has issued for public comment the *Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Consultation Draft)*(《个人信息和重要数据出境安全评估办法（征求意见稿）》) and the *Measures for Security Assessment of Cross-border Transfer of Personal Information (Consultation Draft)*(《个人信息出境安全评估办法（征求意见稿）》) on 11 April 2017 and 13 June 2019, respectively, which aim to stipulate the application scope, assessment content and assessment procedures for the security assessment of cross-border transfers of personal information, etc.

C. NISSTC

NISSTC issued the Personal Information Security Specification on 30 November 2017 and, in a subsequent revision on 6 March 2020, recommends overall requirements for the cross-border transfer of personal information where personal information collected and generated during operations inside the territory of the PRC is provided offshore, the personal information controller should comply with the requirements of relevant national regulations and standards.

Additionally, NISSTC issued for public comment in May 2017 and August 2017 respectively the *Information Security Technology - Guidelines on the Security Assessment for Cross-border Data Transfer(Consultation Draft)* (《信息安全技术 数据出境安全评估指南（征求意见稿）》), which aims to further refine the key points and procedures for the security assessment of cross-border transfers of personal information and important data, etc.

D. PBoC

In the financial sector, PBoC has adopted a more cautious approach to the protection of personal financial information by Financial Industry Institutions. PBoC issued the PBoC Circular on 21 January 2011. According to the PBoC Circular, banking financial institutions must comply with the following requirements:

- personal financial information collected within the territory of the PRC shall be stored, processed and analyzed

within the territory of the PRC; and

- unless otherwise prescribed by any law or regulation or PBoC, the banking financial institution shall not provide any domestic personal financial information to an offshore party.

Five years after the PBoC Circular was issued, PBoC promulgated the PBoC Measures on 14 December 2016, which propose stricter requirements for cross-border transfers of data by banking financial institutions established in the PRC in accordance with law, to provide financial products and services to financial consumers, other financial institutions that provide cross-market and cross-industry financial products and services and non-bank payment institutions:

- where, for the purpose of developing a cross-border business, a domestic financial institution, as authorized by the parties concerned, transfers relevant personal financial information collected in the PRC to an offshore institution (including its headquarters, parent company or any of its branches, subsidiaries and other affiliates necessary for the completion of such business), it shall comply with the laws, administrative regulations and the provisions of the relevant regulatory authorities; and
- the domestic financial institution shall require offshore institutions to keep confidential the personal financial information obtained by taking effective measures such as signing an agreement or conducting on-site inspections.

II Specific requirements of the Specification for the cross-border transfer of personal financial information

Based on relevant applicable laws and regulations and national standards (as summarized in Section (1) as above), the Specification puts forward more detailed management requirements for Financial Industry Institutions for the localization and cross-border transfer of personal financial information. Please refer to the following table for specific requirements:

Type	Relevant requirements in the Specification for the cross-border transfer of personal financial information
Principled requirements	The Specification stipulates that personal financial information collected and generated during the provision of financial products or services within the territory of the PRC should be stored, processed, and analyzed within the territory of the PRC.
Requirements for cross-border transfers of personal financial information	The Specification provides that a Financial Industry Institution may provide personal financial information to an offshore institution (including its headquarters, parent company or any of its branches, subsidiaries and other affiliates necessary for the completion of such business), provided that the following requirements are met: ■ due to business needs, it is truly necessary to provide the information to an offshore institution; ■ the explicit consent of the personal financial information subject should be obtained; ■ a security assessment of the cross-border transfer of personal financial information should be carried out to ensure that the data security protection capability of the offshore institution meets relevant security requirements; ■ the Financial Industry Institution should ensure and supervise the offshore institution to effectively perform its duties and obligations such as confidentiality of personal financial information, data deletion, and cooperation with case investigations, by signing of an agreement with the offshore institution and conducting on-site inspections, etc.; and ■ the national laws and regulations and relevant rules, measures and standards of industry regulatory authorities should be followed.

III Cross-border transfers of personal financial information and anti-money laundering compliance

It is worth noting that the Specification allows Financial Industry Institutions to provide personal financial information to offshore institutions, provided that the provision of such information complies with national laws and regulations and relevant rules, measures and standards of industry regulatory authorities. This means that when Financial Industry Institutions provide personal financial information to offshore institutions, they must also observe the regulations and requirements for anti-money laundering and anti-terrorist financing of the PRC financial regulatory authorities.

Under the PRC anti-money laundering regulatory system, in addition to the *Anti-Money Laundering Law of the People's Republic of China* (《中华人民共和国反洗钱法》) officially adopted by the Standing Committee of the National People's Congress on 31 October 2006, financial regulatory authorities such as PBoC and CBIRC have also issued a series of anti-money laundering and anti-terrorist financing provisions and requirements, two points of which are worth noting:

- According to the *Measures for Administration of Verifying Clients' Identities and Preserving Data on Clients' Identities and Transactions Records by Financial Institutions* (《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》) jointly promulgated by PBoC and other financial regulatory authorities:

  the "basic identity information" of a natural person client includes names, gender, nationality, occupation, domicile address or business address, contact info, and type, number and period of validity of the identity card or other identity document; and

  the "transaction records" of a customer includes data, business vouchers, accounting books for each transaction, and contracts, business vouchers, receipts, business correspondences and other materials that reflect the circumstances of the actual transactions required by relevant regulations.

- The PRC financial regulatory authorities have also imposed strict restrictions in view of the confidentiality and external provision of customer identity data and transaction information. According to anti-money laundering rules such as the *Measures for Administration of Anti-money Laundering and Anti-terrorist Financing for Banking Financial Institutions* (《银行业金融机构反洗钱和反恐怖融资管理办法》), the *Measures for Administration of Anti-money Laundering and Anti-terrorist Financing by Internet Finance Service Institutions (for Trial Implementation)* (《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》), and the *Measures for Administration of Anti-money Laundering and Anti-terrorist Financing of Payment Institutions* (《支付机构反洗钱和反恐怖融资管理办法》), relevant financial institutions and their personnel must keep confidential the client identity data and transaction information obtained by performing anti-money laundering and anti-terrorist financing obligations in accordance with law; they must not provide such information to any entity or individual unless otherwise stipulated by laws.

  We note that the "client identity data and transaction information" obtained by financial institutions when engaging in business activities under the current PRC anti-money laundering regulatory regime largely overlaps with the "personal financial information" as defined in the Specification, which will also

present certain challenges for the data compliance of Financial Industry Institutions under the personal information protection regime and the anti-money laundering regulatory regime.

In view of this, we suggest that Financial Industry Institutions, when complying with relevant requirements related to personal financial information protection and cross-border data transfers, also observe the relevant anti-money laundering rules and regulatory requirements issued by PBoC, CBIRC and the China Securities Regulatory Commission, and other financial regulatory authorities. Meanwhile, with the continuous development of the personal information protection and anti-money laundering regulatory regimes in China, we will also pay further attention to the revisions of the relevant systems and share our views with readers in a timely manner.

2. Key Developments in the Revised Personal Information Security Specification

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU

On March 7, 2020, the State Administration for Market Regulation and the Standardization Administration of China jointly released a revised version of the *Information Security Technology – Personal Information Security Specification* (the "**2020 Revision**"), which will come into force on October 1, 2020 and replace the currently effective 2017 version (the "**Specification**"). The 2020 Revision generally incorporates the changes proposed in previous consultation drafts released in 2019 and other regulatory demands government authorities have imposed in recent enforcement campaigns. The 2020 Revision contains the following key revisions compared to the Specification:

- Optimizes the readability of privacy policies.
- Provides a function-based approach to regulate excessive collection of personal information.
- Enhances notification-consent requirements and security protection obligations for processing biometric information.
- Strengthens products and service providers' responsibility to supervise personal information processing by embedded third-party plugins (such as SDKs and APIs).
- Enhances user control over personalized push (including targeted advertising).
- Provides for obtaining consent and conducting security assessments when integrating personal information from different sources for secondary uses.
- Streamlines the account deregulation process.

Optimizing the readability of privacy policies

In response to criticism of the length and ambiguity of privacy policies, the 2020 Revision simplifies policy content and improves notification methods, which is intended to help users better understand how their personal information is processed. On one hand, the 2020 Revision removes from the Specification's privacy policy template explanations of the use of complex terminologies, such as cookies and web beacons. On the other hand, the 2020 Revision recommends data controllers highlight in privacy policies content which relates to the processing of sensitive personal information and provide a summary of key content to new users when they first agree to use the relevant products or services.

Enhancing recommendations for notice and consent

The 2020 Revision adopts a function-based approach to regulate excessive personal information collection and implements the minimization principle. Network products and service providers should categorize business functions as either basic functions or additional functions. Operators may rely on privacy policies to obtain consent to process personal information for basic functions, but should obtain explicit consent for personal information processing for each discrete additional function. Operators should not

bundle additional and basic functions and should allow for information subjects to decide whether to initiate certain additional functions and to consent to the related personal information collection. A personal information subject's refusal to launch an additional function and the related personal information processing should not affect the provision of basic functions. In particular, basic functions do not include improving services, enhancing user experiences, and research and development.

Enhancing protection of biometric information

The 2020 Revision further emphasizes the protection of biometric information, which supplements the existing recommendations regarding personal information and sensitive personal information. When collecting biometric information, data controllers should obtain explicit consent and provide separate and real-time notification to personal information subjects of the collection, specifying the purpose, measures and scope of collection, retention period. Data controllers should process biometric information at the device terminal and avoid uploading biometric information when possible. Moreover, in principle, data controllers should store summary biometric information and not retain raw biometric information.

Adding new recommendations for third-party plug-ins

The 2020 Revision enhances recommendations for data controllers (e.g. apps and websites) to restrict and supervise personal information collection and processing by third-party plug-ins embedded in their products and services. These recommendations include: (i) conducting security assessments before inserting or connecting to third-party plug-ins, (ii) specifying third-parties' security obligations, (iii) disclosing to personal information subjects that their personal information will be processed by a third party and either obtaining their consent or requesting the third party to obtain consent, and (iv) monitoring third parties' personal information processing activities (e.g. through technical monitoring or auditing). When a data controller discovers a third-party has abused personal information or failed to comply with its security obligations, the data controller should notify the third party to make corrections or immediately cut off connectivity.

Strengthening user control over personalized displays

In accordance with the 2020 Revision, data controllers should distinguish personalized and non-personalized displays by clearly labelling with "personalized display" or presenting such content in different columns and provide data subjects a convenient way to opt-out of personalized displays. "Personalized display" is defined as a display of information content or the provision of search results for goods and services based on personal information such as data subjects' browser history, interests, consumption records, habits, etc. Moreover, it is also recommended that personal information subjects be provided with a mechanism to control the degree to which their personal information is used in personalized displays. However, it is worth noting that the 2020 Revision excludes from personalized displays search results based on geographic locations a personal information subject has selected.

Specifying recommendations on integrating personal information from different sources

Data controllers are recommended to conduct security assessments before integrating personal information collected from different sources or purposes and to adopt effective measures to safeguard the security of such personal information. If the purpose of use of the integrated personal information exceeds the original purpose for which the information was collected, data controllers should re-obtain consent from the personal information subjects.

Emphasizing recommendations regarding account deregistration

A focus of the authorities in recent enforcement campaigns has been personal information subjects' rights, particularly the right to deregister accounts. In order to eliminate hurdles for deregistration, the 2020 Revision provides that data controller should not require additional verification information in the account deregistration process beyond those provided during account registration. Once the account is deregistered, users' personal information should be deleted or anonymized. In addition, the 2020 Revision also recommends companies provide convenient deregistration channels to personal information subjects such as in interactive user interfaces, website dashboards, or applications.

Our comments

Compared to the overarching nature of the *Cybersecurity Law of the People's Republic of China*, the Specification serves as an important guideline for both enterprises and law enforcement authorities due to its detailed and specific recommendations. At the same time, the voluntary nature of the Specification makes it flexible enough to balance the demands between privacy protection and business practice. Based on this, we take the view that that the Specification will be revised on a regular basis to address practical needs. Companies should not only pay close attention to the changes, but also maintain effective communications with the authorities to seek mutually appropriate solutions.

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