HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

February 8, 2018

GSP of Personal Information Security Arrived

David TANG | Min ZHU | TieCheng YANG | Ying HUANG

Many industries, such as food, pharmaceuticals and medical devices, focus on quality management and have their own management practices, such as GMPs (Good Manufacturing Practices) and GSPs (Good Sales Practices). There is no doubt that the newly released *Information Security Technology – Personal Information Security Specification (GB/T 35273-2017)* (the "**Specification**") is the "GSP" (Good Security Practices) of personal information protection in terms of its structure and content. In the financial industries, financial regulators have their own rules protecting personal financial information. Promulgation of the Specification will help financial institutions to give more protection to their customers.

On December 29, 2017, the General Administration of Quality Supervision, Inspection and Quarantine of the PRC and the Standardization Administration of the PRC jointly released the Specification in the form of a national standard. The full text of the Specification was officially published on the national standards public system on January 24, 2018, and will be effective on May 1, 2018. The Specification establishes a framework for personal information protection in accordance with requirements of the Cybersecurity Law, providing comprehensive and detailed compliance obligations for all aspects of the personal information processing life cycle.

Distinguish Functions + Qualitativeness and Quantitativeness + Process Management

Upon analyzing the content of the Specification in its entirety, we believe that the overall internal logic of the Specification can be summarized as "distinguish functions + qualitativeness and quantitativeness + process management." Specifically, the Specification first distinguishes core and additional business functions, since there may be different basic compliance obligations for different functions. Next, the Specification qualitatively and quantitatively puts forward different requirements for personal information which may be involved in the business, such as stipulating the clear purpose principle (legitimate, justified and necessary) and

minimum sufficient use principle (minimum quantity and lowest frequency) etc., and also stipulates the collection methods, storage area, and storage period, etc. Third, the Specification stipulates specific standardization requirements for each stage of the personal information life cycle, which involves collecting, storing, using, commissioned processing, sharing, transferring, public disclosure, and mergers and acquisitions, etc.

In order to illustrate the above framework more intuitively and clearly, we have provided the following table. We believe that this table will not only aid in understanding the overall structure and content of the Specification, but also be instructive for enterprise personal information compliance practices.

Table 1

Information / Function	Qualitativeness and Quantitativeness			Process Management						
	Type	**Quantity**	**Frequency**	**Collect**	**Store**	**Use**	**Commissioned Process**	**Share / Transfer**	**M&A and Reorganization**	**Public Disclosure**
Applicable Principles	Clear purpose, minimum sufficient use			Selective consent, transparency, guarantee of security, participation of subject						
Core Business Function 1 (Ex.: Payment)	Identity information, bank account etc.	1	1	Explicit consent	Minimized time, de-identification, encryption	-	-	Explicit consent, security impact assessment, informing sharing information	-	-
Core Business Function 2										
…										
Additional Business Function 1 (Ex.: location)										
Additional Business Function 2 (Ex.: money management)										
…..										

The Specification Clearly Answers Some Pending Questions in Practice

i. Ownership of Personal Information

The Specification creatively puts forward the concept of "personal data controller" ("**Controller**"), and defines it as "an organization or individual that has the right to decide the purpose and method of personal information processing." From this term, we can observe that the Specification continues to gloss over the issue of ownership of personal information, in line with many previous documents dealing with the protection of personal information. At this point, we believe that the personal information ownership issue is actually a false proposition, or at least that a clear and definite definition of ownership cannot be established at this stage due to the balancing between personal information protection and the economic development of big data. The expression "personal data controller" in the Specification emphasizes that this entity or person is the actual controller of personal information rather than the owner. In fact, the Specification cleverly handles the ownership issue at this stage by not influencing the creation of a set of rules for the protection of personal information. Remaining silent as to the ownership of personal information may be conducive to promoting the overall process of personal information protection without this issue creating a prerequisite obstacle.

ii. Consent Rules at the Collection Stage

In practice, use of consent terms inconsistent with the consent rules is a common industry phenomenon. For many network operators, it is common to efficiently and at low cost obtain users' consent by allowing users to accept the operator's privacy policy when registering for the operator's services. However, the general and ambiguous wording of these types of privacy policies is often used to obtain general user authorizations, so as to lessen or even exempt network operators of their own obligations. The Specification stipulates in detail specific compliance requirements for informed user consent rules.

Article 5.3 of the Specification provides general requirements for personal information collection, namely that personal information subjects ("**Subjects**") must be clearly informed of the circumstances related to the collection and that authorized consent be obtained from the Subject. We believe that "authorized consent" includes both "explicit consent" and "implied consent." Article 5.5 of the Specification distinguishes functions of network products into core functions and additional functions, and further stipulates special consent requirements for personal sensitive information.

With respect to the collection of personal sensitive information, for example, Article 5.5 of the Specification provides that if the collection is necessary for core business functions, network operators should inform the Subjects of specific types of personal sensitive information to be collected, clearly inform them of consequences of refusal to provide information or consent, and allow the Subjects to choose whether to provide the information or agree to automatic

collection. If the collection is for other additional business functions, network operators should explain each item of personal sensitive information necessary for each additional business function separately, and allow the Subjects to choose whether to provide or agree to the automatic collection of personal sensitive information. Where the Subject refuses to provide personal sensitive information for the additional functions, those functions may not be provided, but the core functions should not be terminated due to this refusal, and the quality of the services should still be guaranteed. Because additional business functions are inherently not essential to the service, the compliance requirements for collecting personal sensitive information for such functions is clearly more demanding.

The following three steps should be considered when network products or services involve personal information collection:

- Step 1: determine whether it is a collection activity. Local access to users' information via some network products or services may not be a collection activity, and therefore there would be no need for authorization from the Subject.
- Step 2: if it is confirmed to be a collection activity, distinguish whether the business functions belong to core or additional functions of products or services. For core functions, privacy policies may still be used for general authorized consent, while separate authorizations should be used to obtain explicit consent for additional functions.
- Step 3: distinguish whether the information belongs to general personal information or personal sensitive information. For general personal information, enterprises may obtain general authorizations, including "implied consent" (Opt-Out) and "explicit consent" (Opt-In); as for personal sensitive information, enterprises should only adopt the method of "explicit consent," that the Subjects should make written statements or affirmative actions, for example by affirmatively ticking a box and clicking "Agree."

Table 2: types of authorized consent

Information / Function	Personal Sensitive Information	General Personal Information
Core Business Function	Explicit consent	Explicit or implied consent
Additional Business Function	Separate explicit consent	Explicit or implied consent

Four departments, including the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology, the Ministry of Public Security, and the Standardization Administration jointly launched a special program for the privacy policies of 10 network products and services during the period from August 24, 2017 to September 24, 2017. The results of the program indicated that the privacy policies for the products and services had all improved to various degrees. Subsequently, the companies offering the ten products and services also jointly signed the *Proposal for Personal Information Protection*, which includes "respecting the user's right to know" and "complying with user authorization and strengthening self-restraint." It is noteworthy that the Specification also provides the main content of and compliance requirements for privacy policies in detail, and displays privacy policy templates in a 9-page appendix. This appendix provides an important reference guide for platforms and apps to develop their own privacy policies.

iii. Limited Due Diligence in Indirectly Obtaining Personal Information

As for sources of personal information, besides being voluntarily or automatically collected from Subjects, there is the possibility that a Controller will indirectly obtain personal information from third parties. The Specification stipulates specified regulations for third-party sources.

a. Personal information providers ("**Providers**") are required to indicate the sources of personal information and to verify the legitimacy of those sources.

b. Controllers should understand the scope of authorized consent to process personal information which Providers have obtained, including the purpose of use, and whether the Subjects consented to the transfer, sharing, or public disclosure of the information. If the organization processes personal information for business beyond the scope of the authorization, explicit consent of the Subjects should be obtained within a reasonable time after obtaining the personal information or prior to processing the personal information.

These rules present the diligence and care obligations for Controllers which indirectly obtain information via third-party channels. In order to satisfy these compliance requirements, the relevant enterprises should conduct limited but necessary due diligence on the relevant business activities of the Providers, review the relevant policy documents of the Providers, and examine their personal information protection activities to maximize the protection of the enterprise's own interests.

iv. Information Preservation and Processing after Termination of Services

For the storage stage of the personal information life cycle, the Specification provides specific requirements for minimizing the time for saving and de-identifying the information in accordance with the minimum sufficient use principle and the ensure security principle. As for the storage of personal sensitive information, Controllers should use security methods such as

encryption, and technical measures should also be employed in advance to handle personal biometric information.

Subjects are relatively concerned in practice regarding Controllers' handling of personal information following the termination of products or services. The Specification clarifies a solution to this issue by requiring Controllers to stop collecting information, notify Subjects individually or in the form of an announcement, and to delete or anonymize the personal information held when the Controller's product or service is no longer being offered.

v. Tripartite Relationship Rules in the Personal Information Life Cycle

The previous discussion involved the bilateral relationship between the Controllers and the Subjects, but the Specification also regulates tripartite relationships in handling personal information. In this section, the Specification focuses on the regulatory requirements for personal information processing involving third parties and clearly distinguishes the stages and applicable rules for commissioned processing, sharing, transferring, public disclosure, common control, mergers and acquisitions involving personal information.

For Controllers commissioning others to process users' personal information, the Specification provides that the Controller should not exceed the scope of authorization, and that the Controller should conduct a personal information security impact assessment on the commissioned activity. In accordance with the Specification, personal information should in principle not be shared, transferred or publicly disclosed, and prior consent of the Subjects should be obtained when it is necessary to perform such actions. The consents should be explicit if personal sensitive information is involved. In addition, receivers of personal information should be subject to personal information security impact assessments, and Controllers should inform the Subjects of the specific details relating to sharing, transferring and publicly disclosing the information.

Section of "Personal Information Sharing and Transfer" in Article 8.2 of the Specification, item e) is of particular note by requiring "the undertaking of corresponding liability for causing damage to the legitimate rights and interests of Subjects due to the sharing and transfer of personal information." We understand that, the liability here includes not only the Controller causing adverse consequences, such as through information leakage or damage during the process of sharing and transferring information, but also the Controller failing to carefully investigate the information receiver and sharing or transferring personal information to a receiver which lacks appropriate information security capabilities. Potential liability due to a failure to investigate information receivers should be of note to Providers, because in this case the personal information is beyond the Provider's control, and presents a broadening of potential risk.

Additionally, to a certain extent, the Specification explicitly gives affiliated companies / affiliates

and authorized partners (such as suppliers, service providers, etc.) limited access to information in the Appendix D "Privacy Policy Templates." For the transfer of personal information in the case of mergers, acquisitions, and reorganizations, the Controllers should undertake the obligation to notify Subjects. And if the purpose of using the personal information changes, the explicit consent of the Subjects should also be obtained again.

vi. Personal Financial Information and Cross Border Transfer of Personal Information

In its preamble, the Specification provides that where there are other requirements in laws and regulations in relation to personal information, those requirements shall prevail. In each of financial instructress (e.g. securities, funds, futures, banking and insurance), there is general requirement that financial institutions must keep their customers personal information confidential. In 2011 the People's Bank of China issued the Circular to Banking Financial Institutions in Protecting Personal Financial Information (the "**PBoC Circular**"). The PBoC Circular focus on protection of an individual's financial information, such as the information of an individual's financial accounts and financial trading. The detailed standards and procedures set out in the Specification (which is lacking in the PBoC Circular) could help financial institutions improve their protections on their customers' financial information.

For cross-border transfer of personal information, the Specification requires the Controller to conduct safety assessment in accordance with the rules and standards issued by CAC and other competent authorities. In the Privacy Policy Templates, there is a template statement on cross-border transfer of personal information and a general requirement that the Controller should specify the type of personal information to be transferred abroad and the standards, agreements and the legal mechanism that it will comply with for the transfer.

vii. Other Highlights of the Specification

Previously, the Cybersecurity Law and other laws and regulations provided a definition of personal information, but they did not clarify the key terms related to personal information processing. The Specification responds to many concepts closely related to the practice of personal information protection and provides clear guidelines, such as for personal sensitive information, Subjects, Controllers, collection, explicit consent, user profiles, deletion, public disclosure, transfer, sharing, anonymization, de-identification.

It is also notable that the Specification concludes by providing informative appendices which include examples of personal information, criteria for personal sensitive information, to protect Subjects' right to selective consent, and privacy policy templates. The first two appendices set out the scope and types of personal information and personal sensitive information, and clearly include the controversial network identity information and personal Internet records as personal information. The latter two appendices display the corresponding functional interface and policy text in the form of templates, which are of high practical reference value.

This is particularly so for privacy policy templates which will be widely referenced and adopted by Internet and platform-based companies.

Advice for Enterprises

The Specification provides detailed provisions for the protection of personal information that is mentioned in the Cybersecurity Law. Some of the provisions are somewhat strict and the compliance requirements for enterprises have also been significantly raised, which in turn will result in the corresponding increase in enterprise operating costs. However, compared with the previous policy blanks, the promulgation of the Specification will undoubtedly provide a more comprehensive guide for the formulation of corporate compliance policies and the protection of personal information.

Therefore, we recommend enterprises to improve their internal compliance systems as early as possible. Enterprises whose scale meet certain conditions should clarify responsible departments and officers, and the position of chief information officer ("**CIO**") will be customary for the enterprises engaged in big data services. In addition, enterprises also need to establish systems, such as personal information management personnel positions and training systems, personal information security impact assessments and auditing systems, personal information security incident handling and reporting systems, and then strictly comply with requirements in the Cybersecurity Law, the Specification and other supporting regulations in all stages of the personal information processing life cycle.

It is worth noting that although the Specification is a recommended national standard, and it is not mandatory for all kinds of organizations to implement, it does not mean that the Specification is without significance. The Specification expresses in the beginning that it "applies to the supervision, administration and assessment of personal information processing by competent authorities or third party evaluation agencies." In addition, a responsible officer of the CAC has also stressed the spirit advocated by the Specification in a recent hot incident. It can be seen that although the Specification is a recommended standard, it may be used as an important reference for the supervision and enforcement of government departments in practice, and thus the Specification should attract adequate attention from network operators. For financial institutions, in addition to their own financial regulatory requirements, they may wish to take into account the detailed standards and procedures of the Specification in order to give their financial customers more protection.

Han Kun Cybersecurity and Data Compliance Series:

I : Big Data Policy and Legal Issues in the Healthcare Industry

II : Comments on the Network Security Law

III: Comments on the Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (for Public Comment)

IV: The Unveiling of Cybersecurity Reviews

V : Personal Information Protection from the Perspective of Criminal Law

VI: Guidelines on Data Export Security Assessments

VII: CII, Core Cybersecurity Law System Issued

● Important Announcement

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

Should you have any questions regarding this publication, please contact **Mr. David TANG （+8621-6080 0905; david.tang@hankunlaw.com ）, Mr. Min ZHU （ +8621-6080 0955; min.zhu@hankunlaw.com ）** or **Mr. TieCheng YANG (+8610-85164286; tiecheng.yang@hankunlaw.com)**.