China Releases Practical Guide for Identifying Sensitive Personal Information

On 14 September 2024, the National Technical Committee 260 on Cybersecurity of Standardization Administration of China ("TC260") released *TC260-PG-20244A Practical Guide to Cybersecurity Standard - Guide for Identifying Sensitive Personal Information (v1.0-202409)* ("Guide").

1. Background

The Guide aims to facilitate companies to identify sensitive personal information by providing relevant identification rules alongside specific examples.

After the formal release of the Guide, the primary legal references for identifying sensitive personal information in practice include the *PRC Personal Information Protection Law* ("PIPL"), the Guide, and the national standard *GB/T 35273-2020 Information Security Technology - Personal Information Security Specification* ("Standard 35273"). Besides, companies may also refer to another national standard *Information Security Technology – Security Requirements for Processing of Sensitive Personal Information (draft for comments)*, which has, however, currently not yet taken effect.

2. Rules for identifying sensitive personal information are established

The Guide adheres to the same definition of sensitive personal information as outlined in the PIPL, i.e. sensitive personal information refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person.

While a definition for sensitive personal information is provided, clear identification rules were lacking. In practice, companies commonly referred to the Standard 35273, which lists certain examples of sensitive personal information. However, even as it lists examples, the Standard 35273 only provides vague identification criteria, affecting companies' judgment on unlisted sensitive personal information. The new Guide bridges this gap, delivering practical and method-driven guidance. Specifically, according to the Guide, the identification of sensitive personal information can be accomplished through the following four-step process:

Step 1 - Determine whether any of the following conditions are met

If any of the following conditions are met, the concerned personal information shall be deemed as sensitive personal information.

- Leakage or illegal use of the concerned personal information that can easily lead to the infringement of a natural person's human dignity, including cyber manhunts, unlawful intrusion into network accounts, telecommunication fraud, and discriminatory differential treatment, etc.

- Leakage or illegal use of the concerned personal information that can easily lead to the harm to the safety of a natural person's life, including the harm caused by disclosure or illegal use of information on a person's movement track information, etc.

- Leakage or illegal use of the concerned personal information that can easily lead to the harm to the safety of a natural person's property, including the harm caused by disclosure or illegal use of financial account information. etc.

Step 2 - Determine whether it falls under any of the sensitive personal information listed in Appendix A of this Guide

The Guide outlines major categories of sensitive personal information consistent with those set forth in the PIPL and builds upon these by listing more specific types for each major category of sensitive personal information in Appendix A. For details, please refer to below Section 3.

The Guide also provides that sufficient reason and proof can justify the non-determination of sensitive personal information, even when it falls under one of the types in Appendix A, provided it does not meet any conditions laid out in the above Step 1.

Step 3 - Determine whether the compilation of multiple pieces of personal information satisfy any of the conditions outlined in Step 1

The Guide regulates that it is necessary to consider not only the identification of a single piece of sensitive personal information, but also the overall influence when multiple pieces of general personal information have been compiled together. For instance, individual pieces of general personal information such as a name, workplace, or phone number might not inherently be considered sensitive. However, once compiled, these details collectively possess enhanced identifiability and potential risks. In such cases, companies must refer back to the conditions outlined in the above Step 1 to evaluate whether the compilation of such information qualifies as sensitive personal information.

Step 4 - Determine whether there are specific laws or regulations designating it as sensitive personal information

If there are laws and regulations stipulating that the concerned personal information is sensitive personal information, such specific laws and regulations shall apply. Therefore, for companies in certain industries, they should pay attention to the specific regulations in the industry. For instance, companies in automobile industry should refer to the *Provisions on Automobile Data Security Management (for trial implementation)*, which came into effect on 1 October 2021. Article 3 of this regulation specifies that vehicle movement tracks, audio, video, images, etc., related to a vehicle owner, driver or passenger or any person outside the vehicle, are typical sensitive personal information in the industry.

3. Scope of sensitive personal information are adjusted

a) Comparison table

The Guide has made considerable adjustments to the scope of sensitive personal information compared to the Standard 35273. Please refer to the comparison table below, where the text in red indicates new additions, the text in blue indicates deletions, and the text in green indicates amendments or further clarifications.

Category	Standard 35273	Guide
Biometric Identification	Personal genes, fingerprints, voiceprints, palm prints, earlobes, irises, facial recognition features, etc.	Personal genes, facial information, voiceprints, walking patterns, fingerprints, palm prints, eye prints, earlobes, irises, etc.
Religious Beliefs	Religious beliefs	Personal religious beliefs, positions held in religious organizations, participation in religious activities, special religious customs, etc.
Identity	ID card, ~~passport, driver's license, work permit, social security card, residence permit, etc.~~	ID card photos
Specific Identity	~~Military ID~~	Information about persons with disabilities, information on occupational identities that are not suitable for public disclosure, etc.
Medical Health	Information generated due to illness or medical treatment, such as symptoms, hospital records, doctor's orders, inspection reports, surgery and anesthesia records, nursing records, medication records, ~~drug and food allergy information~~, fertility information, previous medical history, ~~treatment conditions~~, family medical history, ~~current medical history~~, infectious disease history, etc.	Information related to physical or mental harm, diseases, disease risks, or privacy of an individual's health status, such as symptoms, previous medical history, family medical history, infectious disease history, physical examination reports, fertility information, etc. Personal information collected and generated during disease prevention, diagnosis, treatment, care, and rehabilitation services, such as medical consultation records (e.g., medical opinions, hospital records, doctor's orders, surgery and anesthesia records, nursing records, medication records), inspection and examination data (e.g., inspection reports, examination reports), etc.
Property	~~deposit information (including amount of funds, payment and receipt record), real estate information, credit history,~~ credit reporting information, ~~transaction and consumption records, records of deposit and withdrawal transactions, and information on virtual property such as virtual currencies, virtual~~	credit reporting information

Category	Standard 35273	Guide
	~~transactions, game redemption codes, etc.~~	
Financial Accounts	Bank accounts, authentication information (passwords)	Personal account numbers and passwords for banks, securities, funds, insurance, housing provident fund, provident fund joint account number, payment account number, bank card magnetic stripe data (or chip equivalent information), and payment mark information, personal income details, etc.
Travel Traces	Travel traces	Continuous accurate positioning trace information, vehicle driving trace information, personnel activity trace information, etc.
Personal Information of Minors	Personal information of minors under 14 years old	Personal information of minors under 14 years old
Other Sensitive Personal Information	Sexual orientation, ~~marital history,~~ unpublicized records of illegal and criminal acts, ~~communication records and content, contact list, friends list, group list, webpage browsing history, accommodation information,~~ precise location information, etc.	Precise location information, sexual orientation, sexual life, records of criminal acts, photos or videos showing private parts of the body, etc.

b) Certain information no longer considered as sensitive personal information

(1) Individual ID card numbers, communication records, browsing records, etc.

In the Guide, only photo of ID card is listed as sensitive personal information. ID card numbers, which are often collected and transferred abroad in management of many companies, are no longer considered sensitive personal information.

Besides, the Guide removes communication records and contents, contact list, friend list, group list, webpage browsing history, accommodation information, etc., which are of concern to many mobile application operators.

(2) Identity information

Compared to the Standard 35273, general identity information such as passport, drive license, etc., has been removed from the list. The Guide now lists only two types of specific identity information, i.e. information on the identity of persons with disabilities, and information on occupational identities that are not suitable for public disclosure. In the draft version of the Guide, there were examples of professional identities of military personnels

and police officers. Therefore, specific case-by-case judgments should be made in the practical identification of occupation unsuitable for public disclosure.

(3) Property information

The Guide deletes many types of information referring to property information compared to the Standard 35273. The information of real estate information, credit records, transaction and consumption records, records of deposit and withdrawal transactions, virtual property information, etc., are all deleted. The added types are personal information such as account numbers and passwords of financial accounts as well as payment marking information and personal income details generated based on the account information, that can easily and directly lead to the property loss of the information subject in the event of leakage.

c) New information treated as sensitive personal information

(1) Biometric identification information such as facial information, walking patterns and eye prints

Since the Standard 35273 only stipulates that facial recognition features are biometric information, there was controversy in practice as to whether facial information includes face photos. The Guide clarifies that the concept of face information is data used for face recognition. Meanwhile, the Guide adds walking patterns and eye prints as biometric information.

(2) Medical and health information such as medical opinions and physical examination reports

The Guide categorizes medical and health information into two types, i.e. information on health conditions related to an individual's physical or mental injuries, illnesses, disabilities, disease risks, or privacy, and personal information collected and generated in the course of healthcare services such as disease prevention, diagnosis, treatment, care, and rehabilitation. This information is often collected by organizations such as hospitals, beauty agencies and health insurance companies.

Compared to the Standard 35273, the medical and health information listed in the Guide is relatively broader, involving not only records generated by individuals in illnesses and medical treatments, but also medical opinions, physical examination reports, etc. At the same time, information that needs to be disclosed for an individual to receive better medical assistance and take sick leave is no longer considered as sensitive personal information, such as information on drug and food allergies and current medical history. It is worth noting that basic physical information such as weight, height, blood type, blood pressure, lung capacity, etc., are not considered as sensitive personal information if it is not related to an individual's illness or medical treatment.

4. Conclusion

The release of the Guide refines distinctions between sensitive and non-sensitive personal information, offering clearer criteria and examples. It is also an important guideline for cross-border data transfer, as it is closely aligned with the *Provisions on Facilitating and Regulating Cross-border Data Flow* issued on 22 March 2024. These provisions clearly state that where a data processor other than a critical information infrastructure operator transfers overseas personal information of more than 100,000 but less than one million individuals (excluding sensitive personal information) or the sensitive personal information of less than 10,000 individuals on a cumulative basis starting from January 1 of the said year, it shall conclude a standard contract with the overseas recipient or pass the personal information protection certification pursuant to the law. Companies can use the Guide to further assess their compliance requirements for cross-border data transfers. By providing operational methods for

identifying sensitive personal information, the Guide reduces compliance complexity and costs for cross-border data transfer, and, this helps facilitating a better global data management.

In case you have questions or for further information, please contact the authors of this newsletter:

Panpan Tang
Senior Associate
CMS, China

T +86 21 6289 6363
E Panpan.Tang@cmslegal.cn

Daisy Lv
Junior Associate
CMS, China

T + 86 21 6289 6363
E Daisy.Lv@cmslegal.cn

CMS Hasche Sigle Shanghai
Representative Office (Germany)
3108 Plaza 66, Tower 2
1266 Nanjing Road West
Shanghai 200040, China

CMS Cameron McKenna LLP Beijing
Representative Office (UK)
Room 1909, China Youth Plaza,
No. 19 Dongsanhuan North Road,
Chaoyang District
Beijing 100026, China