Updates
September 16, 2020
China's New Personal Information Protection Specifications

After undergoing several rounds of revisions to the 2019 draft specifications, the new *Information Security Technology-Personal Information Security Specifications (GB/T35273-2020)* (New Personal Information Specifications) were released jointly by the State Administration of Market Regulation and the Standardization Administration of China on March 6, 2020. The New Personal Information Specifications will take effect and replace the 2017 version of the *Information Security Technology-Personal Information Security Specifications (GB/T35273-2017)* (Current Personal Information Specifications) on October 1, 2020.

Both the current and new versions of the Personal Information Specifications provide voluntary standards regarding the collection, use, storage, processing, transfer, and sharing of personal data as well as rights of personal data subjects. The New Personal Information Specifications added and highlighted the requirements of voluntary choice of multiple business functions of a product or service; collection, storage, and sharing of personal biometric information; restrictions on data aggregation and commercialization; as well as protection of data subject rights. The New Personal Information Specifications are applicable to personal information processing activities conducted by entities operating in China as well as supervision, administration, and assessment activities conducted by the regulatory bodies. The following update provides a more detailed discussion of these new requirements.

Voluntary Choice of Multiple Business Functions

Under the New Personal Information Specifications, Personal Information Controllers (PICs) will not be allowed to obtain overall consents from users to collect and use personal information for multiple business functions of a product or service by bundling different business functions together. Instead, PICs must obtain explicit consents from users for each specific business function. In addition, PICs must provide ways to opt out of business functions that are as easy as those used to opt in. They also must stop collecting personal information after the users opt out of the business function.

In the design of specific business functions and user interfaces, companies should make sure explicit consents are collected for each business function of a product or service and provide options for users to opt out of a business function. Companies should also be mindful of the frequency of obtaining consents from users after the users refuse to grant authorization for the same function. It is noteworthy that PICs are not allowed to force consents from users solely on the grounds of improving service quality, enhancing user experience, and developing new products.

Collection, Storage, and Sharing of Personal Biometric Information

Personal biometric information includes genes, fingerprints, voiceprint, palmprints, auricle, iris, and facial features of an individual. The New Personal Information Specifications establishes rules regarding the collection, storage, and sharing of personal biometric information in addition to personal information and sensitive personal information due to the extensive collection of personal biometric information under various scenarios such as identity verification and payment.

- **Collection:** Before collecting personal biometric information, a PIC shall separately disclose rules of collection and use to data subjects and obtain their explicit consents. The rules shall include the purpose,

method, and scope of collection and use of personal biometric information as well as storage rules.
- **Storage:** Personal biometric information shall be stored separately from personal identity information. Summaries rather than raw personal biometric information can be stored by a PIC. A PIC can directly use personal biometric information on terminals where such information is collected to achieve business functions and shall delete the raw images where personal biometric information can be generated after achieving the business functions.
- **Sharing/Transfer:** The general requirement is that PICs can only share or transfer personal biometric information when there is a business necessity. The PICs must separately disclose to data subjects the purpose of sharing, type of personal biometric information, and identity and data security capability of the data receiving party, and obtain explicit consents from the data subjects.

Companies must create a separate statement for collecting or sharing of personal biometric information and disclose to data subjects that the purposes listed above, and obtain explicit consents before collection or sharing. Companies should only store summaries of personal biometric information and delete raw images after using such information on terminals of collection.

Restrictions on Data Aggregation and Commercialization

The New Personal Information Specifications provide restrictions on data aggregation, user profiling, and personalized display to enhance the protection of personal information.

- **Data Aggregation:** A PIC shall not use the personal information collected beyond a reasonable scope related to the purpose of collection. To do so, the PIC must again obtain explicit consents from users for such purposes. PICs are also required to conduct a security assessment of the aggregated personal information based on the purpose of use and take effective protection measures.
- **User Profiling:** Certain descriptions of the features of data subjects are prohibited in user profiling, such as obscenity, pornography, gambling, superstition, violence, and discrimination based on nationality, race, religion, disability, and disease. Also, a PIC shall not infringe upon legal rights of individuals and entities or harm national security interests when utilizing user profiling in its internal/external business. A PIC shall also avoid using direct user profiling in its business.
- **Personalized Display:** When using personalized display during the process of providing a business function to data subjects, a PIC shall distinguish between personalized display and non-personalized display by clear labelling them as such. Also, the PIC shall create a control mechanism where data subjects can control the degree and extent to which their personal information can be used to generate a personalized display. An e-commerce company shall, at the same time, provide search results without considering a customer's hobbies and interests when it provides a personalized display to the customer. Media companies shall provide options for users to exit the mode of personalized display and allow users to delete relevant personal information after the users choose to exit.

Companies may need to adjust their business methods to comply with these requirements when exploring plans to enhance commercial value from the data collected by various business functions.

Protection of Data Subject Rights

Under the Current Personal Information Specifications, data subject rights of access, correction, deletion, consent withdrawal, and account cancellation are provided under the Section of Use of Personal Information. The New Personal Information Specifications highlight the protection of such data subject rights by creating a new section for these rights.

Regarding the right of account cancellation, the New Personal Information Specifications provide more detailed requirements as follows:

- Account cancellation requests must be processed within a period not exceeding 15 working days.
- Personal information specifically required for identity verification in the process of account cancellation shall be limited to the personal information collected during registration process.
- PICs shall not set unreasonable conditions for account cancellation.
- If sensitive personal information is required for identity verification in the process of account cancellation, a PIC shall disclose to data subjects the measures, such as deletion, after the cancellation has been completed.
- Upon cancellation of data subject accounts, a PIC shall immediately delete relevant personal information and shall not use personal information in its business if the retention of such information is required by law.

Companies shall provide easy options for account cancellation and shall respond to an account cancellation request as soon as possible. Companies should also pay attention to the process of collecting personal information and sensitive personal information for the purpose of identity verification in the account cancellation process. After the account cancellation, companies should be careful to delete or preserve relevant personal information as required by law.

Takeaways

Even though the New Personal Information Specifications are not mandatory, they provide detailed guidance for relevant business operators regarding the collection, use, storage, processing, transfer, and sharing of personal data in China. The New Personal Information Specifications are also considered by regulatory authorities as an important reference. Therefore, foreign-invested companies engaged in activities related to personal data in China should review their current practices and make necessary adjustments to comply with the New Personal Information Specifications.

Explore more in

Corporate Law Privacy & Security

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law