Client Alert

February 2019

China Issues Draft Amendments to the Personal Information Protection Standard

On February 1, 2019, China's National Information Security Standardization Technical Committee issued a set of draft amendments ("the Amendments") to GB/T 5273-2017 Information Security Technology – Personal Information Security Specification (信息安全技术–个人信息安全规范) (the "Specification") for public comments, to be provided by March 3, 2019. The Specification took force on May 1, 2018.

The Specification is defined as a "recommended national standard" and, as such, not legally binding. It is viewed, however, as setting out best practices, and data controllers typically evaluate and adjust their internal policies in relation to the Specification.

The Amendments address, among other issues, forced consent, third-party access and personalized display.

Changes to Consent

The Amendments introduce more stringent consent requirements for collecting personal information.

The Amendments conceptualize the business functions of a data controller as divided into "basic" business functions and "extended" business functions, with distinct consent requirements for the different functions. Annex C of the Amendments, which suggests factors to consider in determining whether a function is "basic" or "extended," indicates that as a general matter, "basic" functions are those integral to the data subjects' demands or expectations regarding a particular product or service. (Another way of imagining this is that, if the data subject would not choose the given product or service if it lacked certain features, such features constitute business functions.) Appendix C points to various elements to consider in categorizing a function as basic or extended, including how the good/service is marketed, the name of the product or service and how it is described in the App Store. The Amendments explicitly state that improvement of service quality, enhancement of user's experience and R&D for new products would not be considered as "basic" functions.

Rules for collecting personal data are articulated in relation to function category. We highlight a few key points regarding these rules under the Amendments:

- For basic functions, the data controller can bundle basic functions into a package, provided that all such basic functions are necessarily activated at the same time. The data controller cannot, however, bundle various functions of products or services into a single package and request the data subject either accept or reject the package if it is not necessary to activate all the basic functions of products or services at a time. For the extended functions, the data subject is entitled to an item-by-item activation of functions.
- The data controller must inform data subjects about basic or extended functions via some sort of interface, such as pop-up windows, written descriptions, notification bars or notification sounds, before activating the basic functions—likely when the data subjects install or use the software or

app for the first time, or register the account—or before use of the extended functions for the first time.

- Consent (either to activate a specific function or relating to personal data collection) can be given only through the data subject's affirmative action, e.g., filling in consent language, clicking an "Agree" bottom or checking a box.
- Data subjects must be given the option to close or opt out of a given function, and doing so must be as easy as activating or opting in to such function.
- The Amendments forbid data controllers from sending data subjects repeated requests for consent to the extended functions if the data subject has declined to do so. Such requests cannot be made more than once in a 24-hour period.
- If a data subject objects to, closes, or opts out of extended functions, the data controller cannot suspend other functions or lower the service quality of other functions.

As indicated above, explicit consent is required for the collection of both sensitive and non-sensitive personal data collection. This is a notable shift away from the sensitive versus non-sensitive distinctions the Specification originally made regarding consent.

Privacy Policies

The Amendments add mandatory material to privacy policy content, including:

- Privacy policies must distinguish personal data collected through basic versus extended functions.
- Any collection of personal sensitive information must be clearly identified or highlighted.
- Privacy policies must disclose any cross-border transfer of personal data.
- Privacy policies must inform data subjects of the potential risks of providing their personal data and of the potential impact if the data subject objects to doing so.
- With respect to using products or services for the first time, or in connection with account registration, the Amendments recommend data controllers employ a pop-up window or comparable notice to proactively display the main or substantial contents of the privacy policy to the data subject.

As a general matter, the Amendments are more protective of data subjects' interests, and specify that in the event multiple interpretations of a privacy policy are possible, the more protective interpretation rules.

No Exception for Consent by Performance of Contract

The Amendments deleted performance of contract as an exception to obtaining consent. If this amendment remains effective, the data controller could not rely on the contract with the data subject to collect the subject's personal information, and would instead be obligated to seek the subject's prior consent.

Personalized Display

The Amendments introduce, for the first time, the notion of "personalized display," and set forth requirements governing two types of data controllers that provide information, merchandise or services based on the data subject's browsing history, personal interests, consumption records, personal habits and other personal information. (The paradigmatic example is targeted advertisement.)

Controllers that provide targeted news or information must mark the material as "personalized display" or "target push" and provide a simple and direct means to opt out. Separately, e-commerce operators providing personalized recommendations or search results must provide the data subject with the option of a non-personalized display. The Amendments also recommend that data subjects be allowed to specify their preferences for receiving targeted marketing. If the data subject opts out of receiving

targeted advertisements, the subject must have the option to delete/de-identify the personal data used for such advertisements.

Integration of Personal Data Collected by Various Functions

For the first time, the Amendments impose restrictions on data controllers integrating data collected from different sources, namely that the use of (integrated) information is compatible with the purposes stated at the time of collection, and that the data controller conduct security assessments and take appropriate measures to protect the integrated data.

Third-Party Access

To the extent third parties can collect personal information through the data controller's service or product, the data controller must adequately supervise and manage the third party. The Amendments impose the following duties in case of third-party access:

- Establishing a management program for the third-party access and, as necessary, establishing access conditions;
- Executing a contract with the third party that specifies each party's security obligations;
- Notifying the data subject that the certain products or services are provided by the third party;
- Adequately maintaining relevant contract and management records properly and making them available for review as necessary;
- As applicable, reviewing consents the third party obtains from data subjects;
- Requiring third parties establish procedures for responding to data subjects' complaints and requests, making and maintaining relevant records, and making such records available for the data subject's review;
- Monitoring the third party's security practices regarding personal information, and, as necessary, cutting off the third party's access to personal information;
- Auditing APIs and other technologies the third party embeds to ensure compliance with the agreement between the parties, and, as necessary, cutting off the third party's access to information.

Data Breach Notification

Under the present cybersecurity-related laws and regulations, it is unclear which of the relevant authorities to whom data breaches should be reported. The Amendments provide two pieces of guidance related to data breach notification, but there are still many unknowns.

Pursuant to the Specification, data controllers must notify the data subject of any incident. Under the Amendments, in contrast, the data controller is not obliged to notify the data subject of all data breach incidents; notification obligations will only be triggered in the event that such incidents substantially impact the data subjects (e.g., if personal sensitive information is disclosed).

In addition, in the case of leakage, damage or loss of the personal sensitive data of more than 1 million individuals, or if related to national economy and people's livelihood or public interests, the data controller must report such incidents to the competent cybersecurity administration. This provision is in line with National Contingency Plans for Cybersecurity Incidents, which became effective on January 10, 2017.

Data Protection Officer

The Amendments raise the threshold requirements for naming a data protection officer, requiring such an officer when the data involved pertains to 1 million (rather than the previous 500,000) individuals. The Amendments also require that the data controller honor the data protection officer's independence.

Records of Personal Data Processing

The Amendments recommend that the data controller establish, maintain and update an inventory of data collection-related records. The contents of the records may include the type, volume and source of the personal data collected; the processing purposes, whether third-party processors are used and the sharing, transfer, disclosure and cross-border transfer of personal data; and the systems and personnel involved in the processing.

Conclusion

The Specification has been important guidance in privacy and data security matters in China, and valued by many companies and relevant authorities. The Amendment will certainly bring heated discussions in the market and we will keep a close eye on its development and finalization.

Contacts

Dora Luo
doraluo@HuntonAK.com

Yanchen Wang
yanchenwang@HuntonAK.com