COVINGTON

China Releases Draft Amendments to the Personal Information Protection Standard

February 11, 2019

Data Privacy and Cybersecurity

On February 1, 2019, China's National Information Security Standardization Technical Committee ("TC260") released a set of amendments to *GB/T 35273-2017 Information Technology – Personal Information Security Specification* ("the Standard") for public comment. The comment period ends on March 3.

Although not legally binding, the Standard has been highly influential since becoming effective in May 2018, as it set out the best practices expected by Chinese regulators (see our previous blogpost on the Standard here). The Standard has been widely used by companies to benchmark their compliance efforts in China.

The draft amendments reflect Chinese regulators' evolved thinking on a number of important topics that are hotly debated around the world, such as enhanced notice and consent requirements and requirements for target advertising. The draft amendments would also introduce new requirements for third party access to data and revise notification requirements for data beaches, among other proposed changes.

Enhanced Notice and Consent Requirements

The existing wording of the Standard requires that the collection of personal information and its subsequent use should be subject to prior consent of data subjects, with further informed consent being required for any processing activity exceeding the scope of the original consent (existing Article 5.3). For the collection of sensitive personal information, explicit consent that is freely given, specific and unambiguous is required (existing Article 5.5). Consent for the collection of sensitive personal information also needs to distinguish between the "core functions" of the products or services being provided, and "other products or services, such as those that provide additional capabilities." If an individual refuses to consent to the ancillary uses of their sensitive personal information, the collector/controller may decline to provide the additional services, but may not cease or degrade the provision of core business products and services to that individual.

The draft amendments propose to enhance the notice and consent requirements in three significant ways to address the issues of bundled consent and data over-collection.

Prohibition on Forced Consent and Bundled Consent

The draft amendments prohibit data controllers from forcing data subjects to consent to functions provided by a product/service and the associated data collection (proposed Article 5.4). This includes a number of scenarios:

- controllers should not force data subjects to consent to a bundle of services/functions;
- unless affirmatively opted in by data subjects (by filling in personal information, clicking through, or ticking checking boxes), data controllers shall not activate services/functions or start to collect personal information;
- data controllers are required to provide opt out mechanisms for data subjects and such opt out mechanisms should be as easily accessible and friendly to use as opt-in mechanisms;
- if a data subject refuses to opt in to certain services/functions, the data controller is also prohibited from (i) frequently requesting consent or (ii) suspending or downgrading services/functions to which the data subject has provided opt-in consent.

Also, to address the issue of bundled consent, the proposed amendments introduce the concept of "basic" and "extended" functions for the first time in a new Annex C. This distinction is significant as it implies different consent requirements for different categories of functions.

Annex C explains that the categorization of "basic" functions should be based on core expectations or demands of data subjects, when they opt in for a service/function (proposed Article C.1). The core expectation can be created from, for example, the name and description provided by the data controllers (such as those they create for descriptions of apps in app stores), and the commercials run by controllers. "Basic" functions may need to be redefined once the product or service is upgraded. New notices should be provided, and new consent should be obtained, after the redefinition of "basic" functions. Also, the draft amendments specify that improvement of customer experience and research and development of new products cannot be defined as "basic" functions.

For "basic" functions, the draft amendments allow controllers to obtain a combined consent for all "basic" functions through affirmative actions by data subjects. If a data subject refuses to consent to such collection of personal information, a data controller can refuse to provide basic functions.

For "extended" functions, the consent requirements for collection are higher: consent is required for each extended function, and a request for that consent can only be sent once in a 24-hour period. If a data subject refuses to consent to the collection of extended functions, a data controller cannot refuse to provide or downgrade basic functions.

The proposed changes no longer highlight the difference in consent requirements between the collection of sensitive and non-sensitive personal information. As a result, explicit consent will likely become the *de facto* requirement for any collection of personal information in China, with narrowly defined exceptions discussed below.

Enhanced Notice Requirements

In addition to the prescriptive requirements already laid out in existing Article 5.6, the draft amendments add more information that is required to be included in a data controller's privacy policy.

Under the newly proposed Article 5.6, data controllers shall notify data subjects of the types of personal information that each function/service will collect, distinguishing the information collected by "basic" functions and "extended" functions. If sensitive personal information will be collected, the description of such collection shall be highlighted in the privacy policy.

A data controller's privacy policy also needs to state the data protection principles that the controller is following and the measures taken to protection personal information collected. Data subjects have to be reminded of the risks involved in providing their personal information to the controller and the consequence of not providing such information.

Finally, the new Article 5.6 specifically requires the privacy policy to provide information on cross border data transfers, if personal information collected is transferred outside of China.

Narrowed Scope of Exception for Notice and Consent Requirements

The existing version of the Standard provides certain exceptions to the requirement of obtaining consent at the point of collection (existing Article 5.4). In addition, existing Article 8.1(a) provides that processing can rely on consent or rely on Article 5.4. So for data collected based on Article 5.4 (that is, data collected without consent), processing is not restricted.

The draft amendments move Article 5.4 to Article 5.7 and add "complying with legal obligations imposed on data controllers by laws and regulations" as an exception. However, the new Article 5.7 removes the exception for performance of contract. In practical terms, data controllers can no longer rely on contracts with data subjects as a ground for collection and processing. This is a significant change, and is narrower than GDPR. If adopted as proposed, neither the execution of an agreement with a data subject nor meeting a company's "legitimate interests" would be valid grounds for processing in China.

New Requirements on Personalized Recommendations and Target Advertising

The draft amendments add a new article on "personalized display," which imposes specific requirements on two types of data controllers serving personalized recommendations based on data subjects' browsing history, interests, consumption record or habits (proposed Article 7.4):

- controllers that provide personalized news or information services (including for example search engines) are required to:
  - mark the news or information as "personalized display" or "targeted push," and
  - provide a user friendly opt-out mechanism.
- e-commerce platforms or merchants providing personalized recommendations or targeted search results based on data subjects' interests or consumption records are required to provide options that do not involve personalized recommendations available to data subjects at the same time.

The draft amendment also recommends that data controllers establish a portal allowing data subjects to manage their preferences for receiving personalized advertisement. Once a data subject opts out from targeted marketing, the data controller is recommended to delete or anonymize the personal information used for targeted promotions.

Requirements on Access by Third Parties and Data Integration

When a data controller allows third parties to collect personal information through their products or services (for example, though Application Programming Interfaces), the new Article 8.7 requires the controller to:

- implement a third-party access management process and set up conditions on access such as conducting security assessments, if necessary;

- specify security responsibilities and measures in the contracts with third parties;
- notify data subjects that certain products or services are provided by third parties;
- retain third-party access records;
- require third parties to obtain consent from data subjects and verify consent collection mechanisms adopted by third parties;
- require third parties to establish procedures for responding to data subject requests;
- monitor data protection practices of third parties and disable third party access if issues are spotted; and
- conduct technical inspections and audits on APIs and other embedded applications and cut off access if the data collection goes beyond the agreed terms.

Note that this article applies only when the third parties are not acting as a processor for the controller (defined by Article 8.1) or a co-controller (defined by Article 8.6).

Separately, if a data controller plans to integrate data collected from different sources, the controller will be required to (i) ensure that the use of data is still within the purposes that are directly related to or compatible with the purposes stated at the point of collection and consented to by data subjects; and (ii) conduct security impact assessments and take appropriate measures to protect the security of integrated data.

Revised Notification Requirements for Incident Response

Under existing Article 9.1 of the Standard, data controllers are required to notify data subjects of all security incidents. The draft amendments, however, limit such notification requirements to security incidents that may impact the rights and interests of data subjects, such as the breach of sensitive personal data. It remains unclear how this proposed change can be reconciled with Article 42 of the Cybersecurity Law, which requires network operators to notify regulators and affected individuals of an incident where actual or potential "leakage, damage, or loss" of personal information is involved.

Also, the draft amendments clarify that a security incident that involves personal information of more than one million data subjects, or that involves sensitive personal information that may affect China's national security and social public interest, must be reported to the Cyberspace Administration of China ("CAC") or its local counterparts (Article 9.1.d).

Data Processing Records

As a new requirement, the draft amendments recommend that data controllers maintain an inventory of their data collection and use in a newly added Article 10.2. The inventory should include:

- types, volume and sources (for example collected from data subjects directly or through third parties) of personal data;
- processing purposes, whether processors are involved and whether the data will be shared, transfer, publicly disclosed or transferred abroad; and
- systems and personnel relating to each steps of the processing activities.

The proposed amendments have been released against the backdrop of the CAC and other government agencies (including the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration of Market Regulation) leading a campaign to audit the collection and use of personal information by mobile applications nationwide (see CAC press release here in Chinese). It signals the enforcement priorities of the government and is likely to significantly impact companies' data protection practices in China.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Yan Luo	+86 10 5910 0516	yluo@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.