A new model for obtaining data protection consents: unbundling the proposed amendments to China's *Personal Information Security Specification*

May 2019

Hogan Lovells

A new model for obtaining data protection consents: unbundling the proposed amendments to China's Personal Information Security Specification

On February 1, 2019, the National Information Security Standardization Technical Committee (the "**Committee**") issued an amended version of the *GB/T 35372-2017 Information Technology – Personal Information Security Specification* (the "**Specification**") for public comment, with the period for making comments having closed on March 3, 2019.

In common with the version currently in force (which was officially issued on December 29, 2017 and took effect from May 1, 2018 which we discussed in our earlier briefing *here*), the amended draft Specification (the "**Draft Specification**") would still be a "GB/T" national standard, i.e., recommended (but non-binding) national standard. However, given that the Draft Specification is the most comprehensive embodiment of China's personal information protection regime, its significance is its ability to influence Chinese regulators in terms of setting personal information protection benchmarks.

The fact that the Specification is being reviewed and amended so soon after its promulgation demonstrates the extent to which organizations have turned to it for detailed data protection compliance guidance and its high profile within the business community. Most Chinese laws of general application which address data protection, such as the *Cyber Security Law* and the *Protection* of *Consumer Rights Law*, only do so in very general terms. The more detailed requirements set out in the Specification serve an important role in bridging the gap between principles and practice.

China moves a step closer to GDPR

The introduction to the Draft Specification states that the proposals are developments of the Specification based on observations of industry practice, the aim of which is to provide more comprehensive and practical guidance.

However, the most striking feature of the Draft Specification is how China's data protection landscape is tracking requirements under the European Union's *General Data Protection Regulation* (the "**GDPR**") and moving towards a forced "unbundling" of consents, requiring separate, explicit "opt-in" consent to each purpose for which personal data is being processed, with a specific focus on advertisement personalization and other forms of digital marketing, which are clearly areas of particular concern.

Stricter consent requirements

Consent to the collection and processing of personal data is the fundamental concept underpinning the Specification.

Clause 5.3 of the Specification requires that information controllers who intend to collect personal information must obtain consent after having expressly notified information subjects of the types of personal information being collected in relation to each business function of the product or service in question, and the purpose and rules of collection and use.

Clause 5.5 requires that information controllers who intend to collect *sensitive* personal information must obtain voluntary, specific and unambiguous consent from information subjects after informing them of how the information will be processed as part of:

(i) the core functions of its product or service; and

(ii) ancillary processing purposes, as well as explaining the consequences of the information subject withholding consent.

The Specification goes on to provide that where information subjects have opted out of providing their sensitive personal information for ancillary purposes, information controllers must not suspend or degrade the performance of core functions.

As it stands then, the Specification already requires unbundling of consents in respect of the processing of *sensitive* personal information.

Move to require unbundled consent in all contexts

It is important to note that the scope of "sensitive personal information" under the Specification is broader than the concept typically seen in comparable international jurisdictions, and is defined as "information that may cause harm to personal or property security or is very likely to result in damage to an individual's personal reputation, physical or mental health or give rise to discriminatory treatment if it were misused." Examples given in the Specification include identification card numbers, biometric information, bank account details, communications records, property details, credit reference information, location data, health and medical information, transaction data and personal data of children under the age of fourteen. Those familiar with other jurisdictions with similar legislation will recognise that this is a broader definition of "sensitive personal data" than is typically seen in the international context.

The Draft Specification further develops consent requirements by extending unbundling to *all types* of personal information, not just sensitive personal information, and re-orienting the scope of unbundling around "basic" and "extended" processing purposes. A single consent is sufficient for processing for "basic" purposes; however processing for "extended" purposes would need to be unbundled and separate consent obtained for each use case. "Basic" processing purposes are defined based on the data subject's primary needs and expectations of using the products or services .

Information controllers may refuse to provide their products and services to information subjects that refuse to consent to the collection of personal information for "basic" purposes.

In order to restrict information controllers from unreasonably expanding the scope of "basic" purposes, the Draft Specification clarifies that what determines the data subjects' primary needs and expectations is not what the information controllers deem those needs and expectations to be. As such, upgrading services, enhancing the user experience and the research and development of new products are not "basic" processing purposes. Instead, such needs and expectations should be determined with reference to the data controller's promotional materials and the name, type and descriptions of its products and services (for example, the content found in an app store in the case of mobile apps).

Consents for "extended" processing purposes must be unbundled by informing the personal information subject, on a case-by-case basis, of the "extended" business functions offered, the personal information which needs to be collected, and permitting the personal information subject to grant or withhold consent for each "extended" business function on a case-by-case basis.

It is recommended that prior to the initial use of both the "basic" business functions and "extended" business functions, consent is obtained by way of interactive interfaces or designs (such as pop-up windows, text-based instructions, filling in boxes, tooltips, audio-based alerts and other such forms).

In additional to the unbundling requirement, the Draft Specification sets out further requirements on consent:

- Consent must be based on the information subject's positive action (such as proactively filling in personal information, ticking or clicking on a checkbox), and controllers must provide an easy-to-follow opt-out mechanism to allow information subjects to opt-out at any time;

- Where information subjects refuse to opt-in or decide to opt-out from a specific processing purpose, information controllers must not disturb information subjects by sending consent requests on a frequent basis. Annex C of the Draft Specification provides

that in the event that an information subject refuses to consent to certain extended business functions, no repeat consent request can be sent within 24 hours; and

- Where information subjects refuse to opt in or decide to opt out from a specific processing purpose, information controllers must not suspend or downgrade business functions that information subjects have consented to. In particular, if an information subject refuses to opt in or chooses to opt out from "extended" purposes, the information controller must not cease or downgrade basic business functions.

Removal of the exemption for contractual necessity

Clause 5.4 of the Specification sets out circumstances in which the processing of personal information may be carried out without obtaining consent from information subjects.

Critically, Clause 5.7 of the Draft Specification removes the exception previously made for processing required for the performance of a contract. By removing the exemption for processing required by contract (which was, in practice, by far the most commonly relied upon exception), the Draft Specification exponentially expands the impact of the move to greater unbundling of transactions, as the scope of processing transactions requiring use-case-by-use-case unbundled consent will become much broader.

New requirements for personalized display and targeted advertising

Apart from the developments in relation to "unbundled" consents, the other key feature of the Draft Specification is its specific addressing of "personalized displays" and targeted advertising.

"Personalized displays" are defined under the Draft Specification to include features of digital interfaces such as personalized research results and other displays based on the information subject's web browsing history, personal interests, consumption records and habits. The Draft Specification adds a new Clause 7.4 imposing requirements on information controllers:

- Information controllers that push personalized news or information services are required to:
    - clearly mark the content as "personalized display", "targeted push" or similar; and
    - provide a straightforward opt-out method so that the user may receive unpersonalized content instead.
- E-commerce operators that provide personalized recommendations or targeted search results for goods and services based on an information subject's personal interests or consumption records are required to provide a means of opting out.
- Information controllers may enable greater transparency by establishing mechanisms for information subjects to understand and control the personal information upon which personalized displays rely. At the time an information subject opts out from a personalized display, the information controller may also provide the information subject with an option to delete or anonymize personal information used for targeted advertising. This provision however, is only a recommendation and appears to be a counsel of perfection that few information controllers will want to follow voluntarily.

Information security requirements for integration of personal information

The Draft Specification also adds a broadly-drafted provision requiring information controllers who integrate personal information collected from various sources to carry out a personal information security impact assessments, based on the purpose of integrating the personal information, and to adopt appropriate protective measures.

New requirements for access to platform data

The runaway success of China's digital economy is fuelled in part by platforms enabling businesses to operate applications and mini-programs within the platform ecosystem. The Draft Specification requires information controllers operating such platforms to:

- establish procedures for enabling secure access to data and access conditions, such as conducting security assessments when necessary;
- incorporate specify information security responsibilities and measures to be taken to ensure the security of personal information in contracts with businesses using the platform;
- notify information subjects where products and services are provided by third parties;
- retain records of third-party access;
- require third parties to obtain consent from information subjects and verify these consents;
- require third parties to establish procedures for responding to requests for information and complaints made by information subjects;
- monitor third party information protection practices, require remediation where necessary and (when necessary) disable platform access if the third party fails to implement the information security requirements; and
- conduct technical inspections and audits on embedded automatic tools (such as codes, interfaces, mini applications and so forth) and disable access if third party activities exceed what has been agreed.

Notification and reporting requirements for personal information breaches

The Specification currently requires information controllers to notify information subjects of *all* security incidents. The Draft Specification relaxes this requirement by limiting the notification requirement to security incidents that may have a relatively significant impact on information subjects, such as breaches involving sensitive personal information.

In addition, the Draft Specification clarifies that only security incidents that involve personal information of more than one million information subjects, or that involve sensitive personal information that may affect the national security and social public interest of China, must be reported to the cyberspace administration, which may include the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security and the local arms thereof.

New information log and processing recording requirements

The Draft Specification adds a new recommendation in Clause 10.2 that information controllers establish and maintain logs of personal information processing activities, including:

- type, volume and source of personal information (for example collected from

information subjects directly or through third parties);

- purposes of processing, application scenarios, third party data processing arrangements, information sharing / transfer / disclosure, and cross-border transfers; and
- systems, departments and personnel involved in each step of personal information processing.

Elevating the position of Data Protection Officer and the status of the personal information protection department

The Draft Specification requires the personal information protection officer ("**DPO**") posts must be filled by persons having the relevant managerial experience and professional knowledge relating to the protection of personal information; such officers shall be involved in important decision-making relating to the processing of personal information, and will directly report to the chief person-in-charge of the organization.

It also requires information controllers to provide its DPO and the DPO's department with the necessary resources, and to ensure that they can independently perform their duties.

Conclusions

Although legally speaking the Specification is not binding 'hard' law, experience demonstrates that Chinese regulators and law enforcement officials consider it to be much more than just 'recommended' good industry practice. We have seen significant movement towards working practices and policies across industry sectors incorporating elements of the Specification, as well as regulators using the Specification as a legal yardstick to measure the compliance of ecosystem platform industry participants, and we expect this trend to continue.

The introduction of the Draft Specification raises the stakes significantly, particularly in the context of online business models that derive commercial benefit from data analytics, data sharing and "data lake" arrangements that combine data collected from across a range of sources. Forcing an unbundling of consents for these types of "extended" processing models and mandating an opt-out from advertisement personalization will have a significant impact on China's internet economy, both for the leading platforms who maintain the thriving ecosystems based on these technologies, and for the brands and marketers seeking to extract data-driven business value from platform interactions.

The consultation on the Draft Specification comes at the same time as the first decisions on profiling and advertisement personalization come to the fore under GDPR, meaning that there is much more focus internationally on how far lawmakers and regulators will go towards making data protection consents more granular, and towards putting increasing optionality back in the hands of data subjects. Overall, what emerges from the Draft Specification is that China appears to see some value in 'hitching a ride on the GDPR train' in terms of unbundling consents, but with heavier emphasis on certain issues which are perceived as particularly problematic in China, like 'pushed' personalization and on empowering information subjects to opt out.

Contacts

Andrew McGinty

Partner, Hong Kong
andrew.mcginty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
mark.parsons@hoganlovells.com

Sherry Gong
Partner, Beijing
sherry.gong@hoganlovells.com

Maggie Shen
Senior Associate, Shanghai
maggie.shen@hoganlovells.com

Lan Xu
Junior Associate, Beijing
lan.xu@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

www.hoganlovells.com