Hogan Lovells

The dust has finally settled – the long journey of China's new Personal Information Security Specification

April 2020

More than one year after the release of a draft amended version of the GB/T 35273-2017 Information Security Technology – Personal Information Security Specification (the 2017 Specification) for public comments in January 2019, the National Information Security Standardization Technical Committee (commonly known as TC260) released the final amended version on 6 March 2020 (the 2020 Specification), which will come into force on 1 October 2020. In between the issuance of the January draft and the 2020 Specification, there were two further draft amended versions issued on 25 June 2019 and 22 October 2019, respectively (together with the January draft, the Previous Draft Specifications).

As noted in our earlier briefing on the 2017 Specification (please see the briefing here), although the 2017 Specification is not a mandatory standard, it is highly influential and useful as a compliance tool for businesses active in China, as the Chinese authorities appear to be using it as a compliance yardstick in practice. 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 and granular requirements set out in the 2017 Specification (and now the 2020 Specification) serve an important role in bridging the gap between principles and practice, providing organizations with useful guidance on how to align their Chinese data protection programs with the increasing demands of international data protection practice.

One of the most striking features of the 2020 Specification is how far its guidelines seek to move China's data protection landscape towards the accountability requirements seen under the European Union's (EU) General Data Protection Regulation (the GDPR). The 2020 Specification recommends internal governance structures that resemble those typical for EU compliance and recommends, where specific materiality thresholds have been met, the appointment of data protection officers. It also establishes a model for privacy impact assessments, data breach incident response programs, and joint controllership.

Perhaps even more significantly, in some respects the 2020 Specification threatens to exceed GDPR requirements. Of particular focus here is the 2020 Specification's movement towards a forced "unbundling" of consents, requiring separate, explicit "opt-in" consents to each purpose

for which personal data is being processed, with a specific focus on third party access, biometric personal information, advertisement personalization, and other forms of digital marketing.

The 2017 Specification: the beginning of the great "unbundled" consent

Consent to the collection and processing of personal data is the fundamental concept underpinning the 2017 Specification.

Clause 5.3 of the 2017 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 rules on collection and use.

Clause 5.5 of the 2017 Specification requires that information controllers who intend to collect sensitive personal information must obtain voluntary, specific, and unambiguous consent from information subjects after

i. Informing them of how the information will be processed as part of:

- The core functions of the information controller's product or service.
- Any ancillary processing purposes.

ii. Explaining the consequences of the information subject withholding consent.

The 2017 Specification goes further than simply recommending unbundled consents for sensitive personal information collection, it also provides 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, a measure that is intended to reduce the scope organizations have to provide a lower standard of service to individuals who have exercised their rights in respect of unbundled consents.

As it stands then, the 2017 Specification already requires unbundling of consent in respect of the processing of sensitive personal information.

Fully unbundled – the 2020 Specification

The 2020 Specification further develops the guidance in respect of unbundling by extending it to all types of personal information, not just sensitive personal information.

Under the 2020 Specification, information controllers must provide unbundled consents for the collection of personal information relating to each separate business function offered to the individual.

This is a forced "unbundling" of consents for different business functions, meaning that one consent will not suffice for the collection of personal information serving multiple business functions, and any refusal by a data subject to the collection of certain personal information required for one business function does not necessarily mean the data controller can refuse to provide another business function to the data subject.

"Business functions" are defined as the types of service that meet the specific needs of personal information subjects, including map navigation, ride hailing, instant messaging, social networking, online payments, news information, online shopping, express couriers, and transport ticketing. The examples cited in the definition make clear that the focus of the unbundling requirements is on the collection of personal information in the context of mobile apps and other online services, where functionality is often bundled, both with respect to service offerings and

with respect to ancillary use of personal information for purposes such as profiling and retargeted advertising.

Annexure C of the 2020 Specification recommends that a distinction be drawn between "basic" and "extended" processing purposes. A single consent is sufficient for processing for all "basic" purposes of the service, 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. Though not expressly defined, extended purposes should be taken to mean any other purposes not based on such primary needs and expectations, such as profiling and retargeting.

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, Annexure C of the 2020 Specification clarifies that what determines the data subjects' primary needs and expectations is not what the information controllers subjectively 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 whether needs and expectations are primary or not, are to 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 also recommended that prior to the initial processing for 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).

Manufacturing consent – recommendations for implementing consents under the 2020 Specification

In addition to the unbundling requirement, the 2020 Specification sets out further recommendations as to how organizations should obtain requirements on consent from data subjects:

- **Affirmative action**: Consent must be based on the information subject's affirmative action (such as voluntary clicking, ticking, entering the relevant information, or otherwise opting in), as the condition for commencing the provision of specific business functions in relation to products or services. Information controllers may only initiate or commence the collection of personal information after the information subject initiates such business functions.
- **Opting out**: Information controllers must provide means or methods through which business functions can be turned off or allow opting out. The means or methods for turning off or opting out of business functions must be as simple as the means or methods through which information subjects opt in to such business functions. Once an information subject turns off or opts out of a specific business function, the information controller must cease collecting personal information through such business function.

- **Requests to reconsider opt-outs**: Where information subjects refuse to opt-in or decide to opt-out from any specific business function, information controllers must not disturb information subjects by sending consent requests on a frequent basis. Annexure C of the 2020 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 48 hours.

- **No reduction in quality**: Where information subjects refuse to opt-in or decide to opt-out from any specific business function, information controllers must not suspend other business functions for which the information subject has opted in, or lower the service quality of such business functions.

- **No forced participation in research and development**: Information controllers must not mandatorily require an information subject to agree to the collection of his/her personal information for the sole purposes of improving service quality, enhancing user experience, developing new products, increasing security, or other such purposes.

New requirements for personalized display and targeted advertising

Apart from the developments in relation to unbundled consents and highly granular specifications in relation to how consents should be obtained, another key feature of the 2020 Specification is its specific addressing of "personalized displays" and targeted advertising.

"Personalized displays" are defined under the 2020 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 2020 Specification adds a new clause 7.5 imposing requirements on information controllers specifically targeting tailored results:

- Information controllers that provide business functions must prominently differentiate personalized displays and nonpersonalized displays (for instance, by indicating words such as "pushing", or offering separate displays in the form of different columns, sections, or web pages).

- 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 of such recommendations.

- Information controllers that push personalized news or information services are required to provide a straightforward opt-out method so that the user may receive generic content instead. At the time an information subject opts out from a personalized display, information controllers are also required to provide the information subject with an option to delete or anonymize personal information used for targeted advertising.

- Information controllers may enable greater transparency by establishing mechanisms for information subjects to understand and control the personal information upon which personalized displays rely. This provision is, however, only a recommendation and appears to be a counsel of perfection that few information controllers will want to follow voluntarily.

New requirements for access to platform data

The runaway success of China's digital economy has been fueled in part by early adoption of platforms enabling businesses to operate applications and mini-programs within platform ecosystems.

If an information controller includes third-party products or services with personal information collection functions in its products or services, the new requirements under clause 9.7 of the 2020 Specification will apply. These requirements include requirements to:

- Establish procedures for enabling secure access to data and access conditions, such as conducting security assessments when necessary.
- Specify, by way of a contract with the third-party product or service provider, the security responsibilities of both parties as well as the personal information security measures to be implemented.
- Clearly indicate to information subjects that such products or services are provided by a third party.
- Duly preserve contracts and management records relating to third-party platform access and ensure such information is made available to the relevant parties.
- Require third parties to obtain consent from information subjects and when necessary, verify the methods through which said third parties satisfy this requirement.
- 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.
- Where a product or service is embedded in, or connected to, third-party automated tools (such as codes, scripts, interfaces, algorithm models, software development kits, mini programs, and so forth), it is advisable that technical inspections and audits are carried out, and access should be disabled if third party activities exceed the scope of what has been agreed.

If the abovementioned third parties do not obtain separate authorizations and consents from information subjects for collecting or using their personal information, then information controllers providing third-party access to such third parties will be deemed as joint controllers with such third parties, in which case the following requirements will apply:

- The personal information controller must confirm with the third party, by way of a contract or otherwise, the personal information security requirements to be met, their respective responsibilities and duties in relation to personal information security, and expressly inform personal information subjects of the same.
- If an information controller fails to expressly inform the information subjects of the above required information, the information controller must assume liability for any personal information security issues created by the acts or omissions of such third party.

New requirements on information controllers regarding processing by a third party, data sharing and transferring

Under the 2020 Specification, an information controller is responsible for taking immediate action against a third-party processor (which is processing data on its behalf) if it becomes aware or discovers that the third-party processor has failed to process personal information in accordance with its requirements, or has failed to effectively perform its duties to protect the security of personal information.

Also, if an information controller discovers that a data recipient (which has received shared or transferred data) has processed the personal information in violation of laws and regulations or in violation of agreements entered into between the parties, the information controller must take immediate action as well. To be more specific, the information controller must:

- Require the third-party processor or data recipient to discontinue the relevant conduct.
- Make or require the third-party processor or data recipient to remedy the position (such as changing its password, refraining from gaining access, and disabling the network connection) to mitigate or eliminate security risks faced by such personal information.
- When necessary, terminate its business relationship with the third-party processor or data recipient and require them to delete personal information obtained from the information controller in a timely manner.

Simplifying certain consent requirements

The 2020 Specification simplifies the disclosure requirements, for instance, the frequency of collection and place of storage are no longer required to be disclosed.

Furthermore, there is a note in the 2020 Specification to clause 5.4 explaining that if the product or service offers a single business function requiring the collection and use of personal information (single business function), the information controller may fulfill its disclosure requirements through its personal information protection policy (i.e., privacy policy). If, on the other hand, the product or service offers multiple business functions that collect or use personal information (multiple business functions), then in addition to the privacy policy, the information controller should ideally indicate to information subjects the purpose, method, and scope for which the personal information is collected and used at the time of actual collection of specific personal information, such that the information subject may consider any specific impact before giving the specific authorization and consent.

Revising the list of examples of sensitive personal information

It is important to note that the scope of "sensitive personal information" under the 2020 Specification is broader than the concept typically seen in the international context. Examples given in the 2020 Specification include identification card numbers, biometric information, bank account details, communications records, property details, credit reference information, location data, transaction data, and personal data of children under the age of 14.

Some of the previous draft Specifications removed "personal phone numbers" and "email addresses and related passwords" from the examples of sensitive personal information that were listed in Annexure B of the 2017 Specification. The 2020 Specification further removed online identity information (including personal information subjects' accounts, passwords, answers to security questions, information subject's personal digital certificates, and so forth and combinations thereof) and information relating to personal health from the list of sensitive personal information.

"Address books, friends lists, lists of groups" are new additions to the examples of sensitive personal information in Annexure B.

Separate requirements on collection, storing, sharing, transferring, and public disclosure of biometric personal information

With the development of technology these days, people can unlock their smart phones or even pay a bill by using their fingerprints or face print data. However, should one's biometric data be accessed and misused by others, the ramifications could be immeasurable. This is because an individual's biometric data is permanent and uniquely identifies its owner. After all, you can change your password, but not your facial contours. Therefore, like many other jurisdictions, the use of biometric data has been the focus of attention in China.

TC260 released a consultation draft of Protection Requirements on Biometric Identification Information on 25 June 2019, the consultation period for which ended on 8 August 2019. Coincidently, the 2020 Specification also added a set of new requirements (which were not included in any of the previous draft specifications) regarding biometric personal information.

- **Definition of biometric personal information**: Biometric identification information is defined as "personal genes, fingerprints, voice prints, palm prints, auricle, iris, facial recognition features, and so forth" under the 2020 Specification.
- **Collection of biometric personal information**: Compared with the collection of personal information and sensitive personal information, more stringent requirements are imposed on information controllers for the collection of biometric personal information, including (i) separately informing the information subject regarding the purpose, method, scope, and the storage period for which the biometric personal information is collected and used, and (ii) obtaining explicit consent prior to collection and use.
- **Storing, sharing, transferring, and public disclosure of biometric personal information**: Biometric personal information must be stored separately from identification information. In principle, raw biometric personal information (e.g., samples, images, and so forth) must not be stored and the measures which may be taken to process such information are: (i) storing summaries of biometric personal information only, (ii) using biometric personal information directly in the collection terminal to achieve purposes such as identification and authentication, and (iii) deleting the original image that may be used to retrieve biometric personal information after achieving purposes such as identification and authentication using facial recognition features, fingerprints, palm prints, iris, and so forth. Furthermore, biometric personal information must not be shared or transferred unless it is necessary to do so due to business needs and explicit consent has been obtained from personal information subjects after informing them the purpose for such sharing and transfer, the types of biometric personal information to be shared or transferred, and the specific identity, data security capabilities, and other such details of the data recipients. Lastly, no biometric personal information may be publicly disclosed.

Elevating the position of data protection officer and the status of the personal information protection department

Under the 2017 Specification, data controllers were required to appoint a head of personal information protection in cases of organizations principally engaged in the processing of personal information and employing more than 200 individuals, or organizations (with or without its personal information processing being their principal businesses) processing the personal information of more than 500,000 individuals. Such an individual was required to be dedicated

to this role. The 2020 Specification increases this processing threshold to one million individuals. In addition, it expands the circumstances requiring such a dedicated individual to organizations which process sensitive personal information of more than 100,000 individuals, which is quite a significant and potentially onerous expansion, given the need for an additional employee to take up the position, or moving an existing employee away from other duties to dedicate himself/herself to the role.

The 2020 Specification also requires the head of personal information protection (DPO) posts 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

China's progress on standards for data protection compliance in recent years has been extraordinary. The rapid sequence of consultation drafts in respect of the 2017 Specification has now run its course, providing some hope that the "dust" may have settled on this area (for now, at least).

The key changes made to the 2017 Specification in the previous draft specification remain: of particular note the forced unbundling of consents to the collection and use of all types of personal information serving different business functions, regulating "pushed" personalizations and empowering information subjects to opt out in certain circumstances.

Overall, what emerges from the 2020 Specification is that China appears to see some value in "hitching a ride on the GDPR train," but with heavier emphasis on certain "hot button" issues which are perceived as particularly problematic in China, like "pushed" personalizations and on empowering information subjects to opt out, presumably based on complaints from, and concerns raised by, data subjects in China. In that sense China may have partially decoupled from the GDPR train, pursuing its own agenda for data protection that reflects the particular needs of its internet economy.

The direction of travel is clear from the 2020 Specification. The amendments in relation to unbundled consents seem to be largely directed at online data collection, striving to seek a balance between allowing China's massive internet economy to continue to grow and innovate and at the same time provide transparency and security to internet users. These changes raise the stakes for data protection in China significantly, particularly in the context of online business models that derive commercial benefit from data analytics and data sharing, such as the online advertising industry, 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 thriving ecosystems based on these technologies, and for the brands and marketers seeking to extract data-driven business value from platform interactions. The amendments in this area to the 2020 Specification have raised a significant debate in China and in this area in particular is one to watch.

Contacts

Andrew McGinty
Partner, Hong Kong
T +852 2840 5004
andrew.mcginty@hoganlovells.com

Philip Cheng
Partner, Shanghai
T +86 21 6122 3800
philip.cheng@hoganlovells.com

Sherry Gong
Partner, Beijing
T +86 10 6582 9516
sherry.gong@hoganlovells.com

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Maggie Shen
Senior Associate, Shanghai
T +86 21 6122 3883
maggie.shen@hoganlovells.com

Jing Wang
Associate, Shanghai
T +86 21 6122 3839
jing.wang@hoganlovells.com

www.hoganlovells.com