China's first Data Protection Measures lifting its veils

June 2019

Hogan Lovells

China's first Data Protection Measures lifting its veils

On May 28, 2019, the Cyberspace Administration of China ("**CAC**") released the draft *Measures on the Administration of Data Security* ("**Data Security Measures**", see our in-house English translation here) for public consultation. This Data Security Measures will be a great leap forward in China's current data protection landscape, which mainly consists of scattered provisions contained in various pieces of legislations and standards, such as the *Cyber Security Law, the E-Commerce Law*, the *Consumer Rights Protection Law* as well as the *Personal Information Security Specification* ("**Specification**"), the most comprehensive yet non-binding national standard with respect to data protection. The Data Security Measures, once officially promulgated, will be the first binding administrative regulation in China to specifically and systematically set out explicit protection for personal data and important data collected and processed through the use of cyber technologies, following the effectiveness of the *Cyber Security Law* in 2017 (see our briefings here).

The scope of application of the Data Security Measures

Article 2 of the draft Data Security Measures states that the provisions therein govern all private sector data processing activities, including but not limited to data collection, retention, transfer, processing and use, by the use of cyber technologies within the territory of the People's Republic of China. The data covered by the Data Security Measures includes personal data and important data. Data so processed for the purpose of "pure family and personal affairs" is, however, explicitly exempted from the provisions of the draft Data Security Measures.[1]

The draft Data Security Measures appear to mainly target the data processing activities of "network operators", which under these draft measures has the same definition as is used in the *Cyber Security Law*, namely, including the owner or administrator of a network or a network service provider. As such, the definition is so broad and vague that it would likely capture all businesses with network infrastructure and operations in China.

Requirements for personal data collection statements

In common with the current requirements set out in the Specification, the draft Data Security Measures require network operators, who collect personal data via cyber tools such as websites or mobile applications ("**Apps**"), to formulate and publish a personal data collection statement (which is typically a privacy notice) in a specific, reader-friendly and readily accessible manner.

Similar to the Specification, a personal data collection statement should include the following items:

- Basic information of the network operator;
- Name and contact information of principal and data protection officer of the network operator;
- The purpose, type, frequency, quantity, method and scope of data collection;
- The location and term of data retention as well as how will the personal data be disposed after the expiration of the data retention term;
- Rules about providing personal data to third parties (as needed);
- Information regarding personal data protection strategies;
- The rights of data subjects, such as right to access, correct, delete personal data, right to

[1] Although the term "pure family and personal affairs" needs to be further clarified, it seems to be generally aligned with "domestic purpose exemption" typically seen in comparable foreign jurisdictions. This mechanism assures that people holding personal data of their family, friends and acquaintance for non-commercial purposes should be exempted from China's data protection requirements. It is therefore comforting that the use of, for instance, social network sites by an individual to hold contact information of his or her friends will not give rise to any privacy related non-compliance concerns to such individual.

withdraw consent as well as methods to fulfil the foregoing rights;

- The channels and mechanisms for lodging complaints; and
- Other items required by laws and administrative regulations.

In relation to the obligation to formulate a personal data collection statement, network operators, especially those who operate via Apps, should also pay close attention to the draft *Methods for Identification of Illegal Collection and Use of Personal Information in Apps* ("**Methods**") released on May 5, 2019. The draft Methods set out a set of practical requirement on data collection via Apps. Specifically, App operators are required to (i) formulate a personal data collection statement; (ii) display the statement at the time of instalment or use of the Apps by way of interactive interface or designs (such as pop-up windows, tooltips and links); and (iii) limit the number of clicks or swipes users need to make before they can reach the page of the statement down to four.

Stricter consent requirement

As one of the fundamental concepts underpinning China's data protection landscape, consent to the processing of personal data has always been of upmost significance to business operators in China. Under current data protection rules, China adopts an "implied consent plus explicit consent" model which generally requires at least implied consent by data subjects to collecting general personal data (such as names, birthday and address) and explicit consent to collecting sensitive personal data (such as telephone number, financial data and biometric data)[2]. **Article 9** of the draft Data Security Measures appears to require data controllers to seek *explicit consent* in *all* circumstances before personal data can be collected. The draft is silent with respect to the acceptable forms of explicit consent. Making reference to the Specification, the typical forms of explicit consent include data subjects giving a written affirmative statement, ticking an empty checkbox, and clicking buttons such as "I agree" / "submit" / "register" / "continue".

Article 11 of the draft Data Security Measures prohibits network operators from forcing or misleading data subjects to give consent to certain data processing activities in an implied manner or via a bundled consent, under the excuse of upgrading services, enhancing user experience, sending targeted push advertising or researching and developing new products.

Currently, the Specification (see our briefings here) and its proposed amendments released on February 1, 2019 (see our briefings here) require data controllers to distinguish core business functions from extended business functions of products and services they offer. Generally speaking, core functions are basic and fundamental functions of a product or service, without which users would not choose to use the product or service. The Specification allows a product or service provider to suspend its service in the event data subjects refuse to consent to the processing of his or her personal data necessary to achieve core functions. However, a data subject's refusal to provide personal data for the purpose of extended functions must not be grounds for service providers to cease the provision of services. Echoing requirements under the Specification, the draft Data Security Measures do not allow discriminatory treatment. For example, network operators must not suspend or degrade the performance of core functions of their service merely because a data subject refused to consent to the processing of his or her personal data for purpose of extended functions. In addition, network operators are not allowed to practice price and service discrimination based on the scope of consent granted by the data subject.

Filing of personal data collection statements

Article 14 of the draft Data Security Measures requires network operators who collect important data and sensitive personal data for "business operations purposes" to file the personal data collection statement and other information such as purpose, scale, method,

[2] Please see Sections 5.3 and 5.5 of the Specification.

scope, type and term of the collection etc. with the local cyberspace administrators (which may include the local branches of the CAC, the Ministry of Industry and Information Technology, the Ministry of Public Security and etc.). This is the first time that such a filing requirement has been imposed. At this stage, no details on the filing procedure or any nature of review by the authorities have been provided. We expect to see implementing details in working guidelines that may be published by the supervising authorities at a later stage.

One essential flaw of this record-filing mechanism is the lack of clarity as to what constitutes "business operations purposes". It is unclear whether this term intends to capture all businesses that are engaged in personal data processing in order to perform services, deliver products or to achieve other business goals, or only those in relation to which data processing is their primary business (e.g., credit information companies)

There are also inconsistencies with respect to the definition of "important data" compared with other Chinese legal sources. The draft Data Security Measures define "important data" as data that, once leaked, may *directly impact* on national security, economic security, social stability and public health and safety, such as undisclosed governmental information, a large scale of data relevant to population, genetic health, geography, mineral resources etc. The draft provides some comfort by excluding manufacturing and operations information and organizations' internal management information from the scope of "important data". As a result, it appears that the scope of important data will be narrower than that provided in the draft *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment* ("**Data Cross-Border Transfer Guidelines**") issued on August 25, 2017, whose Annex A "*Guidance on Identification of Important Data*" attached a non-exhaustive and lengthy list of samples of important data among 26 sectors, covering telecommunications, finance, pharmaceuticals, e-commerce sectors and so forth.

The draft Data Security Measures do not define "sensitive personal data". Based on the Specification, sensitive personal data is data 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 is misused. Examples given in the Specification include identification card numbers, biometric information, bank account details, communication records, credit reference information location data, health and medical information, transaction data, and personal data of children under the age of fourteen.

Personalized display and targeted advertising

Corresponding to the proposed amendments to the Specification, **Article 23** of the draft Data Security Measures also include certain requirements in relation to personalized displays and targeted advertising. Network operators that make targeted pushes are required to:

- clearly mark the content as "personalized display", "targeted push" or similar;
- provide a straightforward opt-out method so the user may receive non-personalized content instead; and
- delete personal data such as MAC address and IMEI numbers used for targeted pushes.

Note that as required under **Article 11**, the sending of targeted pushes cannot rely on implied or bundled consent by data subjects. This may require network operators wishing to send targeted pushes to seek a separate and explicit consent from the data subject.

Prior approval for publishing, sharing, trading and international transfer of important data

Article 28 of the draft Data Security Measures require that before publishing, sharing, trading or internationally transferring important data, network operators to seek prior approval from its industrial supervising authority (for example, the industrial supervising authority for

telecommunication companies would be the Ministry of Industry and Information Technology) or the provincial level CAC if the supervising authority is unclear.

The procedure for applying for an approval, the nature of the review criteria and whether or not any materiality thresholds apply to the obligation to seek approval are, at this stage, unspecified.

For companies that wish to export important data from China to any other jurisdiction, this new rule will aggravate their compliance burden - under the third draft of the *Measures for Security Assessment on Cross-Border Transfer of Personal Information and Important Data* released on August 10, 2017 (which were never finalized), the exporter of important data would only need to make a report of a security assessment if one of a list of materiality thresholds are met, whereas under the draft Data Security Measures, would require organizations to seek approval from their supervising authorities without qualification[3].

App security certification

The voluntary Apps security certification stipulated under Article 34 of the draft Data Security Measures was first adopted in the *Implementing Rules on the Certification of Security of Mobile Internet Applications* released jointly by the CAC and the State Administration for Market Regulation effective March 15, 2019. Network operators may on a voluntary basis apply for a security certification for their Apps at the China Cybersecurity Review Technology and Certification Center. The certification mainly certifies whether the Apps comply with requirements as set forth in the Specification. Those who pass the certification will be granted a certification certificate and a mark "". The CAC encourages App store operators to show the "" mark for the certified Apps and recommend users to use them.

Notification and reporting obligation in the event of data breach

Article 35 of the Data Security Measures requires that in the event of occurrence of possible occurrence of a data disclosure, damage or loss, network operators must: (i) take remedial measures promptly; (ii) notify affected data subjects via phone call, SMS, email or letter etc.; and (iii) make a report to their industrial supervising authority and the CAC. This article imposes much heavier compliance burdens than the proposed amendment to the Specification, which limit notification and reporting obligation to security incidents that may have a relatively significant impact on data subjects, such as breaches involving sensitive personal data.

Conclusion

The draft Data Security Measures clarify some long-standing ambiguities and uncertainties that have been complicating China's approach to data protection regulation. However, the draft still leaves room for improvement. For instance:

- **Traffic routed to overseas – Article 29** of the draft Data Security Measures at a high level prohibits network operators from routing traffic of Internet users in China requesting to visit a Chinese domestic Internet to foreign jurisdictions. It is unclear whether this will impact companies that use private leased lines/VPN to access internet content for internal business needs.
- **Risk assessment on data security** – the draft Data Security Measures require network operators to carry out a so-called "data security risk assessment" before: (i) supplying personal data to third parties; and (ii) publishing, sharing, trading or

[3] The draft Data Security Measures are silent with respect to cross-border transfer of personal data but defer to "relevant regulations", which we believe would be the *Measures for Security Assessment on Cross-Border Transfer of Personal Information and Important Data* (which is also in a draft form). Under the draft *Measures for Security Assessment on Cross-Border Transfer of Personal Information and Important Data*, the cross-border transfer of personal data is conditional upon personal consent by data subjects, security assessment on the transfer activities and reporting obligation to supervising authority (if certain threshold requirements are met).

internationally transferring important data. It is unclear whether such risk assessment is similar to personal data security impact assessment provided under the *Information Security Technology – Security Impact Assessment Guide of Personal Data* (which is still in a draft form) or is intended to be something different.

– **The definitions of "important data" and "personal data"** – the definitions of important data and personal data are somewhat narrower than that in other draft national standards. Such inconsistencies should be addressed in next draft or the finalized version in order to guarantee a unified data protection landscape in China.

The draft Data Security Measures are the latest in a long series of data protection reforms in China and reflect policymakers' increasing focus on advancing the state of data protection compliance in China's thriving online ecosystems, responding to growing demand for stronger data security protection and tracking international trends towards stronger laws, perhaps best exemplified by the European Union's GDPR.

At the same time, some market players are concerned that China's data protection policies may significantly increase their compliance burden, in particular with respect to the need to "unbundle" consents, potentially to the extent of being required to provide data subjects with a long list of separate tick boxes to complete. Using such a detailed basis for consent has been criticized for creating unnecessary barriers for commerce development.

The draft Data Security Measures remain open for comment until June 28, 2019.

Contacts

Roy Zou
Office Managing Partner, Beijing
roy.zou@hoganlovells.com

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

Andrew McGinty
Partner, Hong Kong
andrew.mcginty@hoganlovells.com

Liang Xu
Partner, Beijing
liang.xu@hoganlovells.com

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

Jessie Xie
Senior Associate, Beijing
jessie.xie@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