Baker McKenzie FenXun
奋迅 · 贝克麦坚时

Data Protection and Privacy/
Technology, Media &
Telecommunications
China

Client Alert

June 2019

Baker McKenzie FenXun
A Leading Chinese and International Law Joint Platform

For further information, please contact:

Zhenyu Ruan
+86 21 6105 8577
zhenyu.ruan@bakermckenziefenxun.com

China proposes more stringent rules on security assessment of export of personal information

As part of the Cyberspace Administration of China (CAC)'s recent push to accelerate formulation of the implementation rules of the China Cybersecurity Law (CSL), it published the draft ***Measures for Security Assessment of Export of Personal Information (for public consultations)*** on 13 June 2019 ("**Draft Security Assessment Measures**").

Unlike the draft *Measures for Security Assessment of Outbound Provision of Personal Information and Important Data* released by CAC in April 2017 and the subsequent draft security assessment guidelines (collectively the "**2017 Draft Measures**") whereby outbound provision of personal information and important data was intended to be subject to the same set of security assessment rules, CAC has now opted to apply two separate sets of security assessment requirements for the outbound provision of personal information and important data. In the *Draft Measures for the Administration of Data Security* ("**Draft Data Security Measures**") released by CAC a week before the release of the Draft Security Assessment Measures, it is proposed that network operators intending to transfer important data[1] overseas must conduct security assessment and obtain the approval from the competent industry regulator or (in the absence of the competent industry regulator) the provincial counterpart of CAC, but CAC remains silent on the security assessment requirement specifically applicable to transfer of personal information overseas. The Draft Security Assessment Measures not only address the security assessment of outbound provision of personal information[2] but also (surprisingly) introduce sweeping requirements which, if implemented as currently drafted, will capture all outbound flow of personal information from network operators in China without any trigger that is quantity or risk impact based.

Security assessment applicable to export of any personal information by network operators

The general rule proposed under the Draft Security Assessment Measures is that in order to transfer any personal information overseas, a network operator must conduct security self-assessment and then file the self-

[1] The term "important data" is proposed to be defined under the Draft Data Security Measures as the data, if leaked, that may directly have impact on national security, economic security, social stability or public health and safety. Examples of important data given in the Draft Data Security Measures include unpublished government information, large scale / coverage of population data, genetic and health data, geoinformation and mineral resource data. For the firs time, the Draft Data Security Measures proposed to exclude personal information and network operators' production and operation related information and internal management information from the scope of "important data".

[2] The term "personal information" is proposed to be defined under the Draft Security Assessment Measures to mean information, recorded in electronic or other forms, that can by itself or in combination with other information be used to identify a natural person, including but not limited to a natural person's name, birthdate, identification number, physical data, address, phone number, etc.

assessment report with the provincial counterpart of CAC for its security assessment review.

Unlike the 2017 Draft Measures under which government-administered security assessment will be triggered only if specific thresholds (such as the quantity of the personal information and the nature of and the risk impact on the information and data being transferred) are crossed, the Draft Security Assessment Measures propose to apply both security-self assessment by network operators and CAC's security assessment review as the mandatory formalities for export of any personal information by network operators, irrespective of the quantity of the personal information being transferred or the potential risk impact to be entailed by the proposed transfer.

The Draft Security Assessment Measures also provide that:

- security assessment must be conducted separately in respect of transfer of personal information to each foreign data recipient; and

- multiple transfers or continuous transfer of personal information to the same foreign data recipient would not trigger separate security assessment, provided that a new assessment would still be required (a) once every two years or (b) where there is any change in (i) the purpose of export of personal information, (ii) the types of exported personal information or (iii) the retention period by the same foreign data recipient during the ongoing export of the relevant personal information.

As no specific threshold (such as the quantity of the data subjects concerned, the volume of the personal information proposed to be exported and/or the nature of the personal information being exported (whether such personal information is sensitive or not) is contemplated for triggering CAC's security assessment review and no distinction is introduced in respect of the purpose of export of personal information, the proposed requirements would literally mean that even responding to an email or a call from a foreign counterparty for the very first time (which would involve the use of email address or phone number of a data subject resident in China) would require the relevant network operator to undergo the two-step security assessment process. The rather inflexible security assessment formalities introduced by the Draft Security Assessment Measures would conceivably create very cumbersome administrative and operational burden and even pose unreasonable operational challenges to both Chinese domestic companies conducting international business or engaging in any dealing or communications with overseas counterparties and foreign-invested companies who would inevitably share personal information with overseas parents and affiliates (such as employees' personal information) on a daily basis.

Although the Draft Security Assessment Measures stipulate that CAC security assessment review must be completed within 15 days which may be extended if the circumstance is complicated, it is also questionable if provincial counterparts of CAC would have sufficient manpower and bandwidth (even with assistance from external experts and institutions designated by CAC) to handle the vast volume of security assessment applications that companies within their respective provincial jurisdictions will submit in accordance with this 15-day timeframe.

Personal information export contract required between the network operator and the foreign data recipient

Under the Draft Security Assessment Measures, before a network operator is able to file for CAC's security assessment review of proposed export of personal information, it must:

(a) enter into a contract or other forms of legally binding document with the foreign recipient concerning export of personal information (collectively "**Contract**"); and

(b) conduct self-assessment of security risks associated with the intended export and the security safeguards and measures to be adopted to address such risks, and prepare a security assessment report.

The requirement on concluding a Contract between the network operator exporting personal information and the foreign data recipient is akin to the concept of the data transfer agreement (between data controller and data processor) or the binding corporate rules or BCR (as the internal rules for data transfers within multinational companies) stipulated under the EU General Data Protection Regulation (GDPR). Instead of providing model data transfer clauses to be incorporated into or referenced in the Contract (which is EU's approach under GDPR), the Draft Security Assessment Measures provide that the Contract must contain the following contents and information:

- the purpose of personal information export, the types pf exported personal information and the period of retention of exported personal information by the foreign data recipient;
- the relevant data subjects shall be the beneficiaries of the provisions concerning rights and interests of data subject contained in the Contract;
- when the legitimate rights and interests of the relevant data subjects are infringed, they shall be able to, by themselves or through an attorney, seek indemnity from the network operator exporting their personal information, the foreign data recipient or both of them who shall then indemnify the data subjects in the absence of evidence that they are not responsible for the infringement;
- the Contract shall be terminated or new security assessment should be conducted where the legal environment of the jurisdiction where the foreign data recipient is located has changed and resulted in the Contract not capable of being performed;
- unless the foreign data recipient has destroyed the exported personal information or otherwise anonymized such personal information, the responsibilities and obligations of the network operator and the foreign data recipient shall not be exempted as a result of termination of the Contract.

The Draft Security Assessment Measures also provide that the respective responsibilities and obligations of the network operator exporting personal information and the foreign data recipient shall be specified in the Contract in accordance with the Draft Security Assessment. For instance, insofar as the network operator is concerned, it must inform the relevant data subjects of

the basic information of the network operator itself and the foreign data recipient and the intended personal information export and even provide a copy of the Contract upon request by the data subjects. In the case of the foreign data recipient, it would need to enable the data subjects to access their personal information received by it and accommodate the requests (including correction and deletion of personal information it received) by the data subjects. The foreign data subject would also need to undertake in the Contract that it will only use the exported personal information for the agreed purposes and retain such information within the agreed time period and that it will inform the network operator in a timely manner of any change in the legal environment of its jurisdiction that may have impact on performance of the Contract so that the network operator can inform the competent provincial counterpart of CAC accordingly.

The Draft Security Assessment Measures further provide that the Contract must explicitly state that the foreign data recipient must not transmit the personal information it receives to third parties, unless the following conditions are met:

- the network operator has informed the relevant data subjects by way of email, instant message, mail or facsimile of the purpose of transmitting their relevant personal information to third parties, the identity and nationality of such third parties, the types of personal information being transmitted, and the period of retention of the relevant personal information by such third parties;

- the foreign data recipient undertakes that when the data subject requests to cease the transmission to third parties, it will cease the transmission and requests such third parties to destroy the personal information already received;

- where sensitive personal information[3] is involved, advance consent has been obtained from the data subjects; and

- the network operator agrees to indemnify the data subjects first when transmission to third parties impaired the legitimate rights and interests of such data subjects.

For network operators that have already signed data transfer agreements or BCRs for the purpose of compliance with GDPR, they may rely on such existing documents with their overseas affiliates or counterparties and make specific amendments or China law addendum to such documents in order to in conformity with the Contract requirements stipulated under the Draft Security Assessment Measures. For network operators that adopt data transfer agreements or BCRs which cover cross-border transfers of personal information to group companies and affiliates, while such collective approach would still satisfy the Contract requirement, they would still need to follow the two-step security assessment requirement with respect to the transfer of personal information to each of the group companies and affiliates covered under the data transfer agreements or BCRs.

[3] The term “sensitive personal information” is proposed under the Draft Security Assessment Measures to mean personal information that, once leaked, stolen, or tampered with, can be used to impair a data subject’s bodily or property safety or a data subject’s reputation or mental health.

Again, as the Contract requirement is intended to be applicable without any quantitative trigger, the practical challenge lies where export of very limited amount of personal information by a network operator is involved. Concluding a Contract with the specific contents and information required by the Draft Security Assessment Measures (and going through the two-step security assessment process) would be inherently at odds with how businesses will communicate with overseas counterparties in business reality.

The requirements proposed to restrict transmission of personal information received by the foreign data recipients to third parties could also be practically cumbersome, as many companies typically engage data centres and/or make use of cloud applications or services (SaaS or PaaS) to store and manage their data including personal information generated, collected or received from their business activities. Since the CSL and the other Chinese laws and regulations do not explicitly make distinction between data controller and data processor, the Draft Data Security Measures do not provide for an exception for transmission of personal information received by foreign data recipients to third party vendors who act in the capacity of data processors for the foreign data recipients. Accordingly, the requirements to allow data subjects to opt out of transfer of their personal information to third parties and to obtain their consent for transfer of sensitive personal information to third parties could result in a situation where foreign data recipients have to (a) either store and manage the personal information of the data subjects who request to opt out or withhold their consents (on processing of their sensitive personal information) on their own (without the use of the data centres or cloud services of third parties) or (b) not receive such personal information at all . In the latter case, the network operator in China would be forced to put in place replicate data centre or cloud services in order to manage and process the personal information of such data subjects within China, which could not be operationally efficient and effective for the business.

Security self-assessment by network operators

According to the Draft Security Assessment Measures, the following focus areas should be covered by a network operator in its security self-assessment (which would also be the focus areas of the security assessment review conducted by the provincial counterparts of CAC):

- whether the intended personal information export conforms to laws, regulations and policies of the State;
- whether the Contract sufficiently safeguard the legitimate rights and interests of the relevant data subjects;
- whether the Contract can be effectively performed;
- whether the network operator exporting personal information or the foreign data recipient has any track record of infringing upon rights and interests of data subjects or experiencing major cybersecurity incident; and
- whether the personal information to be exported was legally and properly obtained by the network operator.

Based on the security self-assessment, the network operator shall formulate a security assessment report detailing:

- background, scale of operation, business(es), financial situation, reputation and credibility, and cybersecurity capability;
- plan of personal information export such as timeframe for export, quantity of data subjects involved, scale of personal information to be exported, and whether exported personal information will be provided to third parties;
- risk analysis and proposed measures to safeguard the relevant the relevant personal information.

In its application for the security assessment review by the provincial counterpart of CAC, the network operator would need to submit an application letter, the Contract and the security assessment report.

Under the 2017 Draft Measures, in circumstances where government-security assessment is not triggered, security self-assessment is not a pre-condition for a network operator to export personal information. Although this could be administrative cumbersome for businesses, this is still a more practical requirement if compared with the two-step security assessment requirement stipulated by the Draft Security Assessment Measures.

Security assessment review by CAC

Upon receipt of a security assessment application, the provincial counterpart of CAC shall conduct and conclude its security assessment review within the proposed 15-day timeframe which may be extended in complicated situations. Following conclusion of its security assessment review, the provincial counterpart of CAC shall notify the network operator applying for its review and concurrently inform CAC of the same. If, as a result of the security assessment review, the provincial counterpart of CAC concludes that the proposed export of personal information would have impact on national security, impair public interest or implicate insufficient safeguard of the exported personal information, it may decide that the proposed export of personal information cannot be conducted.

If a network operator objects to the conclusion of the security assessment review conducted by the provision counterpart of CAC, it could appeal to CAC.

Ongoing compliance requirements on network operator

A network operator transferring personal information overseas will be required under the Draft Security Assessment Measures to establish and maintain records of exporting personal information for 5 years covering the following information:

- when (time and date) outbound provision of personal information is conducted;
- identity (name, address and contact methods) of the foreign data recipient(s);

- type and volume of the exported personal information and level of sensitivity;

- other information that may be required by CAC.

A network operator shall submit an annual report on its export of personal information and the status of performance of the Contract(s) within the relevant calendar year to the provincial counterpart of CAC by 31 December of each calendar year. It shall also report any relatively major data security incident to the provincial counterpart of CAC, although no definition of "relatively major data security incident" can currently be found in the Draft Security Assessment Measures or other published laws and regulations.

CAC's ongoing monitoring of personal information export

Aside from receiving the annual reporting and the ad-hoc reporting submitted by network operators with respect to their respective personal information export, the provincial counterparts of CAC are authorized under the Draft Security Assessment Measures to regularly inspect network operators' actual practices of personal information export and the performance of the Contracts included in their security assessment review applications.

The provincial counterparts of CAC may request network operators (and to cause the foreign data recipients) to take remedial measures when they become aware of circumstances where data subjects' legitimate rights and interests are infringed upon as a result of exporting their personal information or where data breach incidents occur. CAC may also request a network operator to suspend or cease personal information export where:

- an incident of relatively major data breach or data misuse occurs to the network operator or the foreign data recipient(s);

- the relevant data subjects are unable to safeguard or have difficulty in safeguarding their legitimate rights and interests (i.e. they are not able to exercise their rights as contemplated under the applicable Contract or as informed by the network operator exporting their personal information); or

- the network operator of the foreign data recipient is not capable of safeguarding security of the exported personal information.

Network operators failing to comply with the requirements stipulated under the Draft Security Assessment Measures in personal information export activities would be penalized by the relevant laws and regulations.

Foreign companies to follow security assessment requirements?

Article 20 of the Draft Security Assessment Measures provides that where a foreign institution collect personal information of users resident in China through methods such as the Internet during their business activities, they shall designate the legal representative or an institution in China to perform the responsibilities and duties of a network operators as stipulated under the Draft Security Assessment Measures.

While this clause is drafted in a rather vague manner and some parts of this clause are quite confusing (e.g. whose legal representative or which domestic institution should be designated), it literally means that CAC's intention is for foreign companies collecting personal information from data subjects resident in China to also designate a representative in China to undergo the two-step security assessment process. However, it is questionable how CAC and its provincial counterparts would be able to enforce the relevant requirements on foreign companies, especially those that do not have any registered presence in China.

Also, with this Article 20, CAC has effectively abandoned the exception for data subjects resident in China to voluntarily provide their personal information for their cross-border activities as recognized in the 2017 Draft Measures which is a more pragmatic and sensible approach.

Concluding comments

The two-step security assessment process proposed by CAC under the Draft Security Assessment Measures reflects the heightened concern of Chinese government over security of personal information in cross-border activities and to certain extent introduces concepts and requirements that have been implemented in other jurisdictions (such as the requirement on data export Contract). However, the proposal to apply the two-step security assessment process (especially CAC's security assessment review) to any personal information export by network operators seems overly stringent and clearly impractical.

CAC will accept public comments on the Draft Security Assessment Measures until 13 July 2019. It remains to be seen if CAC will consider comments from businesses and update the Draft Security Assessment Measures to adopt requirements and approaches that are more practical and implementable.

www.bakermckenziefenxun.com
www.bakermckenzie.com
www.fenxunlaw.com

Baker McKenzie FenXun (FTZ)
Joint Operation Office
Unit 1601, Jin Mao Tower
88 Century Avenue, Pudong
Shanghai 200121, PRC

Tel: +86 21 6105 8558
Fax: +86 21 5047 0020