China Finalises Rules on Cross-Border Transfer of Personal Information and Important Data

Important Clarifications Included; Basic Structure Unaffected

Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data

Revised Text Released

On 19 May, the Cyberspace Administration of China (“CAC”) released to industry players and market participants the revised text (“Revised Rules”) of the Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (“Measures”), which incorporates comments received from market participants on the consultation draft of the Measures and is expected to be published shortly in substantially similar form. We reported on the consultation draft of the Measures (“Draft”) in our earlier alert.

We attach to this alert the unofficial English translation of the Revised Rules received from the CAC, and summarise below the key changes made to the Draft, followed by some key principles which market participants should bear in mind from the Revised Rules. We also relay certain informal comments made by the CAC officials in explaining the thinking behind the Revised Rules.

Key changes

Consent to transfer of personal information

Compared to the Draft, additional operational flexibility in implementing cross-border transfers of personal information is provided by Article 4 of the Revised Rules. This clarifies that in the absence of express written consent, the personal information subject’s consent to the transfer (a mandatory requirement of the Revised Rules) may be deemed or implied from “acts initiated by personal information subjects” such as international telephone calls, sending e-mails or instant messages overseas and cross-border online transactions. In obtaining the consent, an account of the type (rather than the specific content), together with other criteria, of information transferred is

Contents

Revised Text Released .... 1
Key changes .................. 1
Consent to transfer of personal information ..... 1
Prior assessment .......... 2
Assessment by regulators ................................ 2
Annual assessment not required .................. 2
Not applicable to physical transfers ............... 2
Transitional period ...... 2
Key principles ............... 2
Application of the Revised Rules ............... 2
Not an approval process3
Key assessment considerations ............... 3
Mechanism for obtaining consent............... 3
Important data .......... 4
China finalises rules on cross-border transfer of personal information and important data

sufficient to satisfy the requirement of disclosure to the personal information subject, and the provision of the Draft for the recipient's identity to be disclosed has been removed.

Prior assessment
In Article 6 of the Revised Rules, the Draft’s requirement that the transferor's assessment take place “prior to the transfer” is replaced by a requirement to base the assessment on “type, volume and sensitivity”. This is welcome clarification that an assessment can be made on a once-off basis for a given type and volume of data, as opposed to an assessment made each time a transfer takes place (which could potentially be unworkable). Another useful clarification is the removal of the Draft's requirement to consider the implications of an agglomeration of data overseas in making the assessment.

Assessment by regulators
The Revised Rules have significantly reduced the list of circumstances in which an assessment must be carried out by the regulators (as used in this alert and as explained by CAC, “regulators” means the industry regulators at central government level coordinated by CAC as appropriate). First, the blanket principle in the Draft requiring regulators to assess all transfers by critical information infrastructure (“CII”) operators has been removed; such assessments are still required, however, if the information relates to CII security (Article 7(2)). Second, the requirement for all transfers of over 1000GB to be reviewed by the regulators has been removed from the Revised Rules.

Annual assessment not required
The requirement of the Draft for data transfers to be assessed on an annual basis has been removed, reducing the compliance burden.

Not applicable to physical transfers
It is clarified in the definition of “cross-border data transfer” in Article 15 that only transfers of personal information and important data in electronic form will require assessment.

Transitional period
To enable network operators to adequately prepare for the new regime, the Revised Rules will take effect on 1 June 2017 at the same time as the Cyber Security Law, but network operators will have until 31 December 2018 to comply with the new rules. In the meantime, the National Information Security Standardisation Technical Committee is expected to issue a draft of the standards for the conduct of cross-border data transfer security assessments for public consultation. The CAC also stated that it may consider issuing industry-specific guidance on how to conduct such security assessments.

Key principles
Application of the Revised Rules
The Revised Rules apply to all network operators, not just CII operators (as is the position in the Draft). The CAC clarified that the rules defining CII,
expected to be released shortly, are intended to limit CII to infrastructure and networks of national strategic importance (for example, the mere fact that a network is operated by a bank does not necessarily make it CII). Accordingly, it would not be appropriate to limit the scope of the Revised Rules to CII.

The Revised Rules are intentionally widely drafted to catch all electronic transmissions of personal information and important data out of the PRC, with no specific exceptions for purpose (e.g. internal transfers between affiliates) or type of information (e.g. employee information, customer information, and information relating to PRC nationals as well as foreign nationals would be caught by the Revised Rules), and regardless of whether the information and data is transferred from a server in the PRC to a location outside the PRC, or is accessible to a remote operator located outside the PRC.

**Not an approval process**

A transfer cannot proceed if a prohibited element is discovered in the course of an assessment (Article 9). For this purpose, the assessment could be carried out by the transferor or by the regulators. If the regulators discover an element of a prohibited transfer, a prompt demand is to be made for the transfer to be stopped (Article 10). The Revised Rules thus reflect the view (also consistent with but not as explicit in the Draft) that the intention is not to disrupt a data transfer pending completion of an assessment.

**Key assessment considerations**

The redefined criteria of regulatory assessments and prohibited transfers (Articles 7 and 9) shows that the concern of the regulators in assessing and preventing data transfers is national security (broadly defined to include political, economic, culture, social, technological, informational, ecological, resource and nuclear factors as well as defence). This also means that when conducting an assessment, it should be possible to define the “legitimacy, propriety and necessity” of a transfer in accordance with Article 8(1) by reference to commercial factors affecting the transferor (such as transfers of data to a low-cost processing jurisdiction); such commercial factors should, however, be reasonably necessary to justify the type and volume of data transferred.

**Mechanism for obtaining consent**

The Revised Rules continue to require the network operator that seeks to transfer or provide personal information out of the PRC to obtain the information subject’s consent (Article 4). This structure fails to take into account the information flows of a modern business operation, where the entity transferring the information (such as a third-party processor, or a reinsurance company obtaining information from its insurance company clients) may be different from the entity which obtained the information and has direct contact with the information subject. We understand the CAC is still thinking through the possibilities, and hope that further clarification will be forthcoming.
Important data
This remains undefined, and is to be the subject of subsequent rules. The CAC clarified that “importance” is likely to be measured with reference to the state and the general public, not from the standpoint of particular interest groups.
China finalises rules on cross-border transfer of personal information and important data

Authors: Richard Gu, Bryan Chan, Luna Yang

This publication is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here or on other areas of law, please contact one of your regular contacts, or contact the editors.

© Linklaters LLP. All Rights reserved 2017

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com.

This firm is not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services to clients because we are regulated by the Law Society of England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

We currently hold your contact details, which we use to send you newsletters such as this and for other marketing and business communications.

We use your contact details for our own internal purposes only. This information is available to our offices worldwide and to those of our associated firms.

If any of your details are incorrect or have recently changed, or if you no longer wish to receive this newsletter or other marketing communications, please let us know by emailing us at marketing.database@linklaters.com.

A34084650
Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data
(Revised Draft)

Article 1.
These Measures are formulated in accordance with laws and regulations such as the P.R.C. National Security Law and the P.R.C. Cybersecurity Law, in order to safeguard the security of personal information and important data, to uphold national sovereignty in cyberspace, national security, social and public interests, and to protect the lawful interests of citizens.

Article 2.
Network operators providing personal information and important data overseas collected and generated in the course of their operations within the territory of the People’s Republic of China (hereinafter referred to as “cross-border data transfer”) shall be assessed in accordance with these Measures. Where laws and regulations provide otherwise, such provisions shall prevail.

Article 3.
Security assessment for cross-border data transfer shall adhere to the principles of fairness, impartiality, objectivity and transparency, assure the security of personal information and important data, and promote lawful, orderly and free flow of data over networks.

Article 4.
If a network operator is to provide personal information overseas, it shall account for the purpose, scope and type, as well as the country or region in which the recipient is located, to the information subject and acquire the subject’s consent. A network operator shall not be bound by this rule when the transfer is necessitated by an emergency that endangers the life and property of citizens. Acts initiated by personal information subjects, such as making international phone calls, sending emails or instant messages to individuals or organizations overseas, and making cross-border transactions online shall be deemed as implied consent by the subjects.

Article 5.
The competent regulatory authorities shall guide and supervise the security assessments within their respective sectors, and organize and conduct inspections of the security assessments on a regular basis. The Cyberspace Administration of China shall guide and coordinate nationwide security assessment works.

Article 6.
Depending on the type, volume and sensitivity of the data, network operators shall carry out security assessments of cross-border data transfer to protect public interests and uphold national security.
When there is a substantial change in the purpose, scope, type or volume of cross-border transfer of data, or the data recipient is changed or has experienced a significant security incident, a security reassessment shall be carried out in time.

Article 7.
A security assessment by a competent regulatory authority is required when one of the following circumstance is present in a cross-border data transfer; where the competent regulatory authority is not clear, the security assessment shall be organized by the Cyberspace Administration of China:

1. the data contains personal information of over 500,000 individuals;
2. the data contains information of nuclear facilities, chemistry and biology, national defence and the military, or population and health, or data on megaproject activities, the marine environment or sensitive geographic information, or cybersecurity-related information like security vulnerabilities or specific security measures of critical information infrastructure;
3. the data involves other information likely to affect national security or social and public interests.

Article 8.
A security assessment of cross-border data transfer shall focus on the following matters:

1. the legitimacy, propriety and necessity for the transfer;
2. the personal information involved, including, among others, the volume, scope, type, level of sensitivity and whether the data subjects have consented to the transfer;
3. the important data involved, including, among others, the volume, scope, and type of important data;
4. the security protection capabilities of and the measures taken by the data recipient, and the environment of the nation and region where the data recipient is located;
5. the level of risks of data being leaked, damaged, tampered with or misused after the cross-border transfer or subsequent re-transfer;
6. the risks to national security, social and public interest, as well as lawful interests of individuals.

Article 9.
When one of the following circumstances has been identified by security assessment, the cross-border data transfer shall be prohibited:

1. violating laws, regulations of departmental rules;
2. not consented to by personal information subjects;
3. detrimental to public and national interests;
4. posing risks to the national political system, territory security, military security, economic security, cultural security, societal security, scientific and technological security, information security, ecological security, resource security, security of nuclear facilities, etc.;
5. other situations in which relevant agencies, such as the Cyberspace Administration of China, Ministry of Public Security and Ministry of State Security, have prohibited.
Article 10. A security assessment organized by the competent regulatory authority shall provide timely feedbacks to the network operator. Should any circumstance listed in Article 9 be discovered, the authority shall promptly demand the cross-border data transfer be stopped.

Article 11. Any individual or organization has the right to report the violations of relevant laws or regulations related to cross-border data transfer, or of these Measures, to the relevant agencies such as the Cyberspace Administration of China, Ministry of Public Security and Ministry of State Security.

Article 12. Punishment for violations of the provisions of these Measures shall be imposed in accordance with relevant laws and regulations.

Article 13. When there are treaties or agreements executed by the Chinese government with other nations, jurisdictions or international organizations in relation to cross-border data transfer, the provisions of the treaties or agreements shall prevail.

Article 14. Instance involving information about state secrets shall be carried out in accordance with the relevant regulations.

Article 15. The following terms in these Measures, for the purpose herein, shall have the meanings below:

- **Network operator** refers to network owners, administrators, and network service providers.
- **Cross-border data transfer** refers to the provision of personal information or important data in the electronic form to institutions, organizations or individuals overseas.
- **Personal information** refers to all types of information that is recorded by electronic or other means and that can, on its own or in combination with other information, distinguish the identity or reflect the activities of a natural person, including but not limited to name, date of birth, national identification number, contact details, individual biological identification information, residential address, accounts and passwords, financial condition, location and behaviour information, etc.
- **Important data** refers to data that is closely related to national security, economic development and the societal and public interests. For concrete scope please refer to relevant national standards and the guidance document for the identification of important data.

Article 16. These Measures shall come into effect as of 1 June 2017.

All cross-border data transfers made by network operators shall conform to these Measures starting from December 31st, 2018.