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.