Provisions on Regulating and Facilitating Cross-Border Data Flow

(Draft for Comment)

In order to ensure national data security, protect the rights and interests of personal information, and further regulate and promote the free flow of data in a lawful and orderly manner, in accordance with the relevant laws, the following provisions (referred to as "the Provisions") are established for the implementation of regulations related to outbound data flow such as Outbound Data Security Assessment Measures and Provisions on the Standard Contract for Cross-Border Transfer of Personal Information.

Article 1: Outbound data flows generated from international trade, academic cooperation, multinational manufacturing and marketing activities, which do not involve personal information or important data, do not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification.

Article 2: If relevant departments or regional administrations have not notified or publicly announced that the data is important data, the data processors are not required to submit outbound data security assessment applications for the data they processed as important data.

Article 3: Personal information that is not collected and generated within the country does not need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification when being exported abroad.

Article 4: In any of the following circumstances, there is no need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification.

1) It is necessary to provide personal information to foreign entities for the purpose of fulfilling a contract in which an individual is involved as a party, such as cross-border shopping, cross-border remittances, reserving flight and hotel, and visa processing.
2) It is necessary to provide the personal information of internal employees to foreign entities for the purpose of implementing human resources management that is based on relevant labor regulations and lawful labor contracts that are signed collectively.
3) In emergency situations where it is necessary to provide personal information to foreign entities in order to protect the life, health, and property safety of natural persons.

Article 5: If it is anticipated that the personal information of fewer than 10,000 individuals will be transferred outside of the country within one year, there is no need to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained.

Article 6: If it is anticipated that the personal information of more than 10,000 individuals but less than 1 million individuals will be transferred outside of the country within one year, there is no need to apply for outbound data security assessment if a standard contract for cross-border transfer is established with the foreign recipient and registered with the provincial-level cyberspace administration department of personal information, or if a certification of personal information protection is obtained. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained. If it is anticipated that the personal information of more than 1 million individuals will be transferred outside of the country within one year, it is required to apply for outbound data security assessment. However, when the outbound transfer of personal information is based on individual consent, the consent of the personal information subject should be obtained.

Article 7: Free Trade Pilot Zones may independently formulate a list of data (referred to as the “Negative List”) that needs to be included in the applicable scope of outbound data security assessment, standard contract for cross-border transfer, and personal information protection certification within the jurisdiction of the Pilot Free Trade Zone. The Negative List needs to be approved by the provincial-level cyberspace administration department and then registered with the Cyberspace Administration of China. Outbound data flows that are not included in the Negative List do are not required to apply for outbound data security assessment, enter a standard contract for cross-border transfer of personal information, or obtain a personal information protection certification.

Article 8: Government agencies and operators of critical information infrastructure that transfer personal information and important data to foreign entities should comply with relevant laws, administrative regulations, and departmental rules. When sensitive information related to the Party, government, military, and confidential units, as well as sensitive personal information are provided to foreign entities, relevant laws, administrative regulations, and departmental rules should be followed.

Article 9: Data processors that transfer important data and personal information outside of the country shall comply with the provisions of relevant laws and administrative regulations, fulfilling their obligations of data security protection, and ensure the security of outbound data flows. In the event of security incidents of outbound data or when there is an increased risk to outbound

data security, data processors shall take remedial measures, and report to the cyberspace administration department in a timely manner.

Article 10: Local cyberspace administration departments should strengthen their guidance and supervision over data processors' outbound data transfer activities. Local cyberspace administration departments should enhance both proactive and reactive monitoring, and if they identify significant risks in outbound data transfer activities or if a security incident occurs, they should require data processors to rectify and eliminate the underlying issues. In cases where data processors refuse to correct their behaviors or if their behaviors lead to serious consequences, they should be legally ordered to cease data export activities to ensure data security.

Article 11: In cases where relevant regulations such as Outbound Data Security Assessment Measures and Provisions on the Standard Contract for Cross-Border Transfer of Personal Information are inconsistent with the Provisions, the Provisions should be followed.