[New Legislation] Measures for Assessment of Outbound Data Transfer Security

On July 7th, the Cyberspace Administration of China ("CAC") announced the **Measures for Assessment of Outbound Data Transfer Security** (hereinafter called the 'Measures'), which will come into effect on September 1st.

The Measures are mainly based on the Cyber Security Law, the Data Security Law and the Personal Information Protection Law, reflecting the Chinese government's intention to **regulate outbound data, protect the rights and interests of personal information**, as well as safeguard national security and social public interest, while promoting the safe and free flow of data across borders to create a secure commercial environment for the growth of enterprises in China.

·What areas will the Measures apply to?

When enterprises transfer and store data collected and generated in the course of their operations on the territory of China to an offshore location; also, collecting and generating data that is stored on the territory of China and can be accessed or retrieved by offshore institutions, organizations or individuals, self-assessment and security assessment by CAC shall be required according to the Measures.

·Under what circumstances enterprises must declare a security assessment of outbound data (cases in which outbound data security assessment must be declared to the CAC through local cyberspace administration at the provincial level)?

1. Data processors provide **Important Data** outside of China.
2. Operators of critical information infrastructures and data processors handling the personal information of more than 1,000,000 people provide personal information overseas.
3. Data processors that have cumulatively provided personal information of 100,000 people or sensitive personal information of 10,000 people since January 1st of the previous year for overseas.
4. Other circumstances under which security assessment of outbound data is required as prescribed by the CAC.

Consequently, we suggest that firstly, the enterprises should be aware that "important data" refers to data that may endanger national security, economic operations, social stability, public health and safety if it is tampered with, damaged, leaked or illegally obtained or illegally used. Furthermore, for enterprises that **have provided a cumulative amount of personal information data and sensitive data abroad, since 1st January of last year**, and for enterprises that **operate critical information infrastructures,** as well as **those who will provide a large amount of personal information data abroad, must prepare materials in advance to respond to the security assessment**. Last but not the least, legally the CAC has the power to specify other circumstances in which a data cross-border transfer assessment is required. Nevertheless, **the criteria are still based on national security, public interest or the protection of the legitimate interests of individuals or organizations.**

·What's the process for outbound data security assessment?

Step 1 Pre-assessment Enterprises should **firstly conduct a self-assessment** of outbound data risk **before the declaration of security assessment**.

Step 2 Filing assessment

If the circumstances for declaring outbound data security assessment are met, enterprises shall declare the outbound data security assessment to the CAC through the local cyberspace administration at the provincial level.

Step 3 Carrying out The CAC shall complete the security assessment of outbound data and determine whether to accept the assessment **within 7 working days from the date of receipt of the declaration**; and complete the outbound data security assessment **within 45 working days from the date of issuance of the written notification of acceptance**; if the situation is complex or the additional and corrected materials are required, the time extension **may be appropriately extended** and the enterprises will be informed of the expected extension.

Step 4 Reassessment OR Termination

1)If the validity period of the assessment results expires or if the circumstances for re-assessment stipulated in these Measures arise during the validity period, the enterprises shall re-declare the outbound data security assessment.

2) If the outbound data activities that have passed the assessment no longer meet the outbound data security management requirements in the course of actual processing, the enterprises shall terminate outbound data activities after receiving written notice from the CAC.

3) If the enterprises need to continue to carry out outbound data transfer activities, they shall rectify the situation in accordance with the requirements and re-declare the assessment after completion of the rectification.

·The keys to outbound data self-assessment

Article 5 of the Measures set out the legal conditions under which enterprises are required to carry out a self-assessment. Enterprises shall seriously focus on assessing the following perspectives:

1. Legality, appropriateness and necessity of the outbound data and the purpose, scope and method of the overseas recipient's processing of the data.
2. The quantity, scope, type and sensitivity of the outbound data; risks to national security, public interests, and the legitimate rights and interests of individuals or organizations that may arise from the outbound data.
3. The responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management, technical measures and ability to perform the responsibilities and obligations can ensure the security of the outbound data.
4. Risks of leakage, damage, tampering and abuse of data after the data is transmitted abroad and further transferred, and whether the channels for individuals to maintain their rights and interests in personal information are unblocked.
5. Whether the relevant contract for the outbound data concluded with the overseas recipient fully specifies the responsibilities and obligations for data security protection.
6. Other matters that may affect data exit security.

Even if the Measures set out the circumstances in which self-assessment is required, we advise that when confronted with the circumstances that do not meet or do not fall under the requirements to declare outbound data security assessment to relevant departments such as the CAC, enterprises **ought to maintain a cautious attitude as there is a risk of multiple interpretations of the conditions**.

Therefore, we suggest that enterprises should self-evaluate whether they meet the requirements of data exit security assessment through self-attestation. Additionally, enterprises should be aware that Article 55 of the Personal Information Protection Law also imposes a legal obligation to conduct a personal information protection impact assessment on companies providing personal information abroad. Furthermore, Article 9 of the Measures also details what should be included in a legal document (contract) for data crossing the borders, which presents that the setting of legal document clauses will also form a significant part of the self-assessment and security assessment of the CAC.

·What elements will be assessed by the CAC?

According to Article 8 of the Measures, CAC is mostly concerned with the risks to national security, public interests, and the legitimate rights and interests of individuals or organizations caused by

outbound data, which is also the fundamental judgement criteria of CAC. Specifically, it currently includes the following written matters:

1. Legality, legitimacy and necessity of the purpose, scope and method of transmitting the data abroad.
2. The impact of the policies and regulations on the data security protection and the network security environment of the country or region where the overseas recipient is located on the security of the outbound data; and whether the data protection level of the overseas recipient meets the requirements of the laws and administrative regulations of the People's Republic of China and the mandatory national standards.
3. The quantity, scope, type and sensitivity of the outbound data, and the risks of leakage, tampering, loss, damage, transfer, or illegal acquisition or illegal use of such data when leaving the country or thereafter.
4. Whether the data security and the rights and interests of the personal information can be adequately and effectively protected.
5. Whether the contract between the data processor and the overseas recipient has made sufficient provisions on the responsibilities and obligations for data security protection.
6. Compliance with Chinese laws, administrative regulations, and departmental rules.
7. Other matters that the CAC considers necessary to be assessed.

Distinctively, there is some overlap in the content of assessment between self-assessment and security assessment. However, the security assessment will focus on the risks to national security, the public interest, and the legitimate rights and interests of individuals or organizations arising from outbound data activities, and will additionally consider the impact of the policies, laws, and cybersecurity environment in the country or region **of the offshore recipient** on the security of the cross-border transfer data, as well as the outbound data activities and related parties involved.

In response to the forthcoming Measures, enterprises, **especially multinational enterprises, should begin to gradually form their own data compliance teams** in daily management. The compliance team should systematically and comprehensively manage enterprise data and data resources in accordance with **relevant Chinese and foreign laws**, **regulations and requirements**, as well as the enterprise's **own technical conditions and business needs.** In addition, when drawing up outbound data transfer contracts or other legally binding documents with overseas recipients, enterprises should **give due consideration to their responsibilities and obligations regarding data security protections in the contract.**

Feel free to contact A&Z professionals for advice on any of these matters.

6F, Okura Garden Hotel, 58 Maoming South Road, Shanghai, P.R. China, 200020

中国上海市茂名南路 58 号花园饭店 6 楼 邮编 200020

TEL: (+8621)5466-5477 · FAX: (+8621)5466-5977 · info@a-zlf.com.cn www.a-zlf.com.cn