中倫律師事務所
ZHONG LUN LAW FIRM
北京市朝阳区金和东路 20 号院正大中心 3 号楼南塔 23-31 层，邮编：100020
23-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing 100020, P. R. China
电话/Tel：+86 10 5957 2288 传真/Fax：+86 10 6568 1022/1838
网址：www.zhonglun.com

Another Stripe on China's Data Compliance Latticework? -- Highlights of the Draft PRC Data Export Security Assessment Measures*

Information (data) flow has become the lifeblood of enterprises in the increasingly digitalized global economy. However, given its privacy concerns and importance to national security, governments have become more vigilant in regulating the cross-border movement of data. In China, the *Cybersecurity Law* (hereinafter "**CSL**"), the *Data Security Law* (hereinafter "**DSL**") and the *Personal Information Protection Law* ("hereinafter "**PIPL**") have sketched out a framework for data export security assessment (hereinafter the "**DESA**"), with focus on the protection of important data and personal information.

On 29 October 2021, the Cyberspace Administration of China (hereinafter the "**CAC**") released an exposure draft of *Measures of Security Assessment for Data Export* (hereinafter the "**Draft Measures**"), with the aim of fleshing out the DESA scheme. The Draft Measures lay out the substantive and procedural requirements for PRC data export (formally termed "cross-border data transfer") through a tiered security assessment system, and prescribe obligations for China-based companies which transfer data abroad (whether to affiliates or to unrelated third parties as part of business transactions), as well as overseas recipients of China-originated data (e.g. data from internal operations of Chinese subsidiaries or data acquired from Chinese trade counterparties). Therefore, it is prudent for companies to familiarize themselves with the upcoming DESA scheme and be ready to deploy compliance measures in anticipation of its official implementation. To that end, we highlight the key provisions of the Draft Measures, and share our brief observations on proactive actions by data exporters.

To receive a complete bilingual version of the Draft Measures, or to receive our follow-on analysis on China data export compliance issues, please click the following link: request form.

I. Highlights of Key Provisions

* Prepared by John Jiang, Rachel Li and Jason Jia at Zhong Lun Law Firm (Compliance & Regulatory Practice) with assistance from Daisy Xu, for reference purpose only. For more detail, please contact Rachel Li at lirui@zhonglun.com or +86 10 5957 2143.

- **Highlight 1: Types of Data Export Subject to the DESA Scheme**

  According to the Draft Measures, data processors should comply with DESA when engaging in cross-border transfer of (i) important data collected or generated through operations within the border of China; or (ii) personal information which is subject to security assessment under relevant laws (Article 1).

  It further specifies the circumstances where the data processor engaging in cross-border transfer shall apply for an organized security assessment (hereinafter "**OSA**") coordinated by the CAC (Article 4). Such circumstances include:

  1. Personal information and important data collected or generated by a critical information infrastructure operator;
  2. The dataset concerned contains important data;
  3. The export of personal information by a processor who processes the personal information of **over 1 million** people;
  4. On a cumulative basis, export of the personal information of **more than 100,000** people or the sensitive personal information of more than **10,000 people**; and
  5. Other circumstances prescribed by the CAC.

- **Highlight 2: DESA Lifecycle: Ex Ante DESA Followed by Ongoing Supervision**

  As the Draft Measures indicate, the DESA shall integrate ex-ante assessments and ongoing supervision (Article 3). Hence, in its business operation, a data exporter needs to adequately monitor data cross-border transfers and post-transfer activities relating to the data concerned. The Draft Measure also provides for a whistleblowing system, which enables employees, customers, suppliers, and business partners etc. to file complaints or reports. (Article 15).

  Failure to effectively monitor post-transfer activities can create significant compliance exposure. If the CAC has found that a previously cleared data export activity no longer meets the relevant security management requirements, it will revoke the security assessment result. In such case, the data processor shall terminate the data export activity, conduct rectification as required, and re-apply for OSA after the completion of such rectification (Article 16).

- **Highlight 3: Relationship between Risk Self-Assessment (hereinafter "RSA") and Organized Security Assessment**

  The DESA envisages two prongs: self-assessment by the data exporter and organized assessment coordinated by the CAC. The Draft Measure requires the data exporter to integrate RSA and OSA when applicable (Article 3).

  If a cross-border data transfer is subject to DESA, the data exporter should firstly conduct an RSA, and under prescribed circumstances (*See* Highlight 1), the data exporter should apply for OSA after completing the RSA (Article 4).

The RSA covers the following aspects (Article 5):

1. The legality, propriety and necessity of the purpose, scope, manner, etc., of the cross-border transfer and the overseas recipient's data processing activities;
2. The volume, scope, category, and sensitivity level of the data concerned, as well as the risks that the data export may impose on national security, public interest, and the lawful rights and interests of individuals or organizations;
3. Whether the data processor's management and technical capabilities could prevent risks, such as data leakage, damage, etc. that might occur in the course of transfer;
4. Whether the overseas recipient's committed accountability, its management and technical measures, capabilities etc. could safeguard the security of the data exported;
5. The risks of leak, damage, tampering, and abuse, etc., after the data export or the subsequent transfers, and whether there are effective channels for individuals to enforce their personal information rights and interests, etc.; and
6. Whether the data export contract concluded with the overseas recipient adequately provides for data protection obligations.

- **Highlight 4: Substantive and Procedural Aspects of OSA**

Step 1: Applying for OSA

When a data export triggers the OSA (*See* Highlight 1), the data exporter should submit the following materials through the local counterpart of CAC (Article 6):

1. An application letter;
2. An RSA report;
3. The contract to be concluded between the data processor and the overseas recipient, or other legally binding documents with the same legal effect;
4. Other materials necessary for conducting OSA.

Step 2: CAC Confirming the Docketing of the Application

The authority shall inform the data exporter with written notice **within 7 working days** upon receiving the application materials, determine whether to docket the DSEA application (Article 7). If the materials are not complete or are not in order, the docketing time will likely be prolonged.

Step 3: Carrying out the OSA

The authority shall complete the OSA **within 45 working days** from the date of issuing the written docketing notice; if the circumstances are complicated or supplementary materials are needed, the OSA period may be extended, but

generally not exceeding **60 working days** (Article 11). The OSA result would be notified to the data processor in writing.

It is worth noting that the Draft Measures provide that the data processor shall submit OSA materials strictly in accordance with the applicable rules. If submitted materials are incomplete or non-compliant, the data processor shall timely supplement or rectify the materials. Where the data processor refuses to supplement or rectify the materials concerned, the CAC may terminate the organized security assessment. The Draft Measures also emphasizes that if false materials are submitted intentionally, the data export shall be deemed to have failed to pass the organized security assessment (Article 13).

As the Draft Measures have not come into force, PRC authorities have not officially implemented the OSA scheme. Once implemented, as Article 8 of the Draft Measures stipulates, OSA would assess the legality, propriety, and necessity of the purpose, scope, manner, etc. of the data export, the impact of data security protection policies and statutes of the host country or region of the overseas recipient, etc. Specifically, the CAC will organize the industry regulatory authority, the relevant State Council departments, provincial-level cyberspace administration departments, and professional agencies, etc., to conduct the OSA. In connection with assessing important data export, the CAC will also solicit opinions from the relevant industry regulatory authorities (Article 10).

- **Highlight 5: Data Export Contract: Mandatory Provisions and Forms**

The contract entered into by the data processor and the overseas recipient in connection with the data export plays a critical role in both the RSA and OSA. It is noteworthy that Article 38 of the PIPL has raised the concept of "standard contract published by State cyberspace administration authority", which appears to echo the Standard Contractual Clause scheme under the GDPR. Even though the standard contract hasn't yet been issued, the Draft Measures provides a glimpse of the likely contents of such contract.

According to the Draft Measure, the data export contract shall include, but not be limited to, the following contents (Article 9):

1. The purpose, manner and scope of data export, the overseas recipient's intended usage of the data exported, and data processing means;
2. The overseas storage location and duration of the data exported, as well as the measures for disposal of the transferred data upon storage period expiration, the accomplishment of the stipulated purpose, or the termination of the relevant contract;
3. A constraining provision which restricts the overseas recipient from transferring exported data to any other organization or individual subsequently;

4. The security measures to be taken by the overseas recipient in the event of any substantial change in its actual control or scope of business, or any change in the legal environment of the host country or region, thereby rendering it difficult to ensure data security;

5. The contractual liability for breach of data security protection obligations, as well as a binding and enforceable dispute resolution provision; and

6. In the event of data leakage and occurrence of any other risk, proper emergency response and assurance of effective channels for individuals concerned to seek redress regarding rights and interests in their personal information.

- **Highlight 6: OSA Validity Period and Change of Circumstances**

  The OSA result is valid for **2 years**. During the validity period, in addition to noncompliance events which lead to rectification order by the CAC (Article 16) (*See* Highlight 2), when the following condition occurs, the data exporter also needs to re-apply for OSA (Article 12):

  1. There is a change in the purpose, manner, scope, or category of cross-border data transfer, or a change in oversea recipient's intended usage or means of data processing, or there is an extension of the oversea storage period;

  2. Any circumstance that may affect the security of the data concerned, such as a change in the legal environment of the host country or region where the overseas recipient is located, a change of actual control of the data processor or the overseas recipient, a change in the relevant contract between the data processor and the overseas recipient, etc.;

  3. Any other circumstance that may affect the security of the data concerned.

II. Our Observations

The core objective of the DESA scheme is for the competent authority to assess enterprises' data export activities to safeguard national security and ensure personal information protection. Therefore, the application scope of DESA can potentially be fairly broad.

Upon the official enactment of the Draft Measures, fulfilling the regulatory requirements will be more challenging to data processors (especially multinational companies) who are not adequately prepared. Thus, we suggest that companies with existing or potential data export scenarios be ready to take appropriate compliance steps in advance. Key actions for data exporters include:

- Conduct internal review of the company's data export flows and scenarios, and subsequently identify corresponding compliance requirements;

- For multinational companies (hereinafter “MNC”), it is prudent to consider establishing a localized storage system for personal information and important data, so as to mitigate non-compliance risks;
- MNCs should also further review its cross-border data transfer policy, with the focus on satisfying the strictest requirements at a global level, namely the PIPL and the GDPR;
- MNCs may conduct embed-testing and incorporate the DESA requirements into the current procedure and process;
- Proactively carry out RSA in accordance with the likely requirements, and review and adjust data security protection obligations in contracts concluded with overseas recipients, etc.;
- For companies whose data export activities may trigger OSA, it is important to start improving the internal data export compliance system as soon as possible. After the official implementation of the DESA scheme, the company can promptly apply for OSA as required and shorten the assessment time.