Legal Commentary

June 13, 2019

漢坤律師事務所
HAN KUN LAW OFFICES

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

# Draft Personal Data Export Rule Released for Public Comments

**Authors: Kevin DUAN | Kemeng CAI | Wen HE**

The Cyberspace Administration of China ("**CAC**") released a new draft of the long-halted Measures on Security Assessment on Personal Data Export ("**Draft Measures**") on June 13, 2019, almost two years after the publication of the controversial draft cross-border data transfer rules. While excluding important data[1] from the Draft Measures, likely in wake of the intrinsic difference between the two types of data, the draft again expands the security assessment obligation for export of personal data from Critical Information Infrastructure Operators ("**CIIOs**") to ordinary network operators, and indiscriminately requires prior government assessment for data export of onshore and offshore entities. Both will likely spur strong reactions from companies heavily relying on cross-border data transfers for their daily operations, in particular MNCs, or offshore internet/data companies without domestic presences. Further, despite its enhancement of data subject rights, implementation and enforcement of such rights under the Draft Measures may be difficult and at the same time, pose much burden on domestic data controllers.

## I. Expanded Entity Scope and Prior Government Assessment

Like the previous draft, the Draft Measures requires all network operators, rather than CIIOs as stipulated in Article 37 of the Cybersecurity Law, to complete security assessment before transferring personal data outside of China. One step further, the Draft Measures explicitly requires offshore operators who collect personal data from users within China to bear the same obligation through a domestic representative. [2]

Also, the Draft Measures mandate all network operators to apply for security assessment to provincial CAC authorities before transferring personal data abroad. This is a significantly stricter version compared to the previous one, where network operators shall perform self-assessment periodically and are only required to submit self-assessment report for government assessment if volume of data reaches certain threshold or certain sensitive data are involved.

[1] Under the draft of the *Data Security Protection Measures*, important data is defined as "data the divulgence of which may endanger national security, economic safety, social stability, public health and safety, such as unpublished government data, large volume of demographic, genetic health, geographic, mining, resources and other data."

[2] Article 20 of the Draft Measures.

## II. Contract-Oriented Approach and Enhanced Data Subject Rights

The Draft Measures adopts a contract-oriented approach for security assessment.

In addition to a security impact assessment report with respect to data export, a security assessment application filed by network operators subject to the Draft Measures shall include contracts between domestic operator and overseas receivers ("**Transfer Contract**").

Specifically, the Transfer Contract should include the following terms:

- Data subjects are the beneficiary of the clauses concerning the data subject rights, and can directly resort to the domestic operator or the overseas receiver or both, in case of right infringement;
- The security protection obligations towards personal data should survive the termination of Transfer Contract, unless the data has been destroyed or anonymized;
- The domestic operators are obliged to obtain informed consent from the data subjects with respect to the particulars of the data transfer, and provide a copy of the Transfer Contract upon the request of data subjects;
- The overseas receivers are obliged to respond to data subjects' right request promptly;
- In case of any change to the receiving country's legal regimes causing the receiver's difficulty to perform its the contractual obligations, the contract should be terminated. Otherwise the receiver should promptly notify the domestic operator and apply for government reassessment through the latter; and
- In principle, the personal data may not be further transferred to any third party unless the domestic operators and overseas receivers provide certain required safeguards to rights of data subjects.

On the merits, the Draft Measures put the focus on data subject rights when evaluating the Transfer Contract. In particular, the Draft Measures provides that the government assessment should focus on:

- Compliance with laws, regulations and policies;
- The lawfulness and appropriateness of data collection;
- Whether the Transfer Contract provide sufficient safeguards to data subjects and their enforceability; and
- Whether the domestic operator or receiver has any record of damage to the right and interest of data subjects, and whether major cybersecurity incidents have occurred.

## III. Continuous Report and Supervision

Instead of incident-by-incident evaluation, the Draft Measures intend to set up an assessment mechanism that requires continuous reports from network operators and imposes constant supervision thereon from the authorities. At the same time, such mechanism will spare repeated assessment for transfer of similar

data between same parties within a certain period.

In particular, once a network operator passed the security assessment, it does not need to apply for re-assessment for multiple or continuous transfer to the same receiver within two years. However, re-assessment is required if there is any change to the purpose of transfer, types of data concerned and the period of storage of such data abroad. Moreover, network operators are required to preserve records on data export for at least five years, report the particulars with respect to personal data export and performance of Transfer Contract to the provincial CAC authorities annually, and promptly notify provincial CAC authorities in case of occurrence of serious data breach incident.

On the other side, CAC authorities may ban the data export in case the domestic operator or overseas receiver (1) has serious data leakage or data abuse incidents on, or (2) is unable to safeguard the personal interest of data subjects or the security of these personal data.

## IV. Unsolved Puzzle for MNCs and Offshore Entities

The Draft Measures would pose significant challenge for the operation and management of MNCs.

A contract-oriented approach may draw experience from GDPR, which allows MNCs to transfer personal data to overseas party 1) *within the group* under the binding corporate rule (BCR) once authorized by a data protection authority; and 2) outside the group under standard contract clauses (SCC) issued by the European Commission.

However, assessment mechanism contemplated by the Draft Measure significantly deviates from the GDPR, as network operators need to seek separate assessments for transferring to multiple receivers and reassessments in case there is material change to approved transfers. Such burden may be overtaxing the MNCs, and eventually force them to opt for data localization.

The Draft Measures also require offshore services providers directly collecting data from data subject and providing their services on cross-border basis to seek for government assessment through onshore representative, which may be an onshore affiliate or a contact agency. As many provisions under the Draft Measures are tailored to the “domestic operator to overseas receiver scenario” (such as the requirements on Transfer Contract), it is unclear how such provisions would apply to the offshore services providers which directly collect data from data subjects. Last but not least, such assessment obligation may be deemed as creation of a *de facto* license requirements for offshore providers, and it is questionable how the CAC authorities would extend its jurisdiction to such offshore services providers except for cutting off connection thereto.

## V. Enforcement of Data Subject Rights

Under the Draft Measures, data subjects are endowed with third party beneficiary rights under the Transfer Contract, who may exercise their data subject rights and raise compensation claims either towards the domestic operator or directly against the overseas receivers. However, considering the high cost, direct recourse to overseas receivers may be less meaningful in practice. In light of this, the Draft Measures requires the onshore operator to claim against the offshore receiver on behalf of the data subjects, and

compensate the data subjects first in lieu of the offshore receiver in case of the breach of the latter. Such requirement would significantly aggravate the responsibilities of the onshore operator. It is questionable whether such draconian requirements is fair to the onshore operator, considering it may lack effective control and enforcement mechanism towards the offshore receiver.

## VI. Our Comments

The Draft Measures propose unprecedented restrictions on cross-border transfers of data from China and may lead to profound implications on data-related operations. For those whose business now rely on oversea data processing or centralized storage, data localization will be an expensive yet inevitable solution to avoid lengthy assessment procedures and uncertainties arising therefrom. Also, a universal requirement of prior government assessment for network operators collecting personal data may be difficult to implement, and sometimes unnecessary. A more flexible assessment mechanism with parallel compliance approaches like standard contract clauses, binding corporate rules, and adequacy decision or consent, together with ex-post enforcement, is likely more practical, and will not compromise both data subjects' rights and national securities, as already proven in other jurisdictions.

## *Important Announcement*

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

**Kevin DUAN**

Tel: +86-10-8516 4123
Email: kevin.duan@hankunlaw.com

© 2019 Han Kun Law Offices. All Rights Reserved.