TaylorWessing

Data export controls in China: implications for digital business

All digital business in China will need to consider the implications brought by the draft Measures for Security Assessment of Export of Personal Information and Critical Data ("Draft") which were presented by the Cyberspace Administration of China ("CAC") to solicit comments from the public until 11 May 2017 and are expected to take effect in June 2017. This is an important legislative move following the new PRC Cyber Security Law, which will take effect on 1 June 2017 ("CS Law"), and which extends the legal application of the controversial Article 37 under the CS Law. This article generally imposes a local storage obligation on critical information infrastructure operators ("CIIO") with regard to personal information and important data collected and generated out of their operation in China. If transmission of such data out of China is necessary due to business needs, clearance procedures shall be followed according to separate rules to be formulated by the CAC. The Draft is meant to clarify details for further implementation of Article 37 of the CS Law. However, in its current form as presented to the public it appears to go far beyond the CS Law, which will have a substantial impact on all online based business including digital business.

Relevance to your business

The CS Law does not define the term CIIO. Based on a pure literal reading of this law, one will not conclude that it relates to digital business. The exemplary industries mentioned in this law where the term CIIO appears include public communication networks and information services, energy, transport, water conservancy, finance, public services, and e-government affairs. It further covers the areas where a data breach or security compromise could result in serious harm to national security, national economy, peoples' livelihood and the public interest. All these give the impression of a "heavier" infrastructure and facility operator, but not a lighter digital business model, which usually takes the form as a user of the former. However, "information service" under Article 31 of the CS Law - as an exemplary industry where a company may qualify as a CIIO - is quite a broad and vague term, which could potentially be extensively interpreted to cover all business relating to (digital or digitalised) information.

As a newly formed ministerial level agency in charge of cyber security matters, the CAC is supposed to shed light on implementation details of the CS Law including in regards to further interpreting the tricky term "CllO." However, the Draft it presented to the public has come as quite a surprise to the business sector. This Draft does not address CIIOs. Instead, it repeats the local data storage obligation under Article 37 of the CS Law and applies this obligation to "network operators" (not only CIIOs). The term "network operators" is further defined to be those who own networks, manage networks and provide network services. This is a very broad term which in the real world could potentially cover all digital businesses which usually have online features (e.g. cloud based services). On top of this, Article 16 of the Draft stipulates that "other individuals or organisations" shall also handle data export clearance matters by referring to this Draft.

Obviously, by rephrasing and expanding the subjects of the obligation, the Draft now makes local storage of data a more general requirement. As far as your business concerns personal information and important data collected and generated out of your operations in China, you might be caught by this obligation.

Data sensitivity and how to handle the obligations

Generally speaking, two types of data are sensitive under the CS Law and the Draft, namely personal data (i.e. more individual based data) and critical data (e.g. more group based data) collected and generated within the territory of China. The definition of personal data is the same under both the CS Law and the Draft, which means information recorded by electronic or other means that, alone or jointly with other information, can serve to identify a natural person,

including but not limited to a natural person's name, date of birth, identification number, personal biometrics data, address, or phone number. Critical data - a term not defined under the CS Law - is defined under the Draft as data closely related to national security, economic development and public interest, of which the exact scope shall follow relevant national standards and classification guidance. So far no such national standards and classification guidance exist; they are yet to be formulated.

According to the Draft, if export of the above sensitive data becomes necessary due to business demand, an export clearance shall be secured. This is formed of two kinds of exercise, namely a self-assessment procedure and an administrative assessment procedure. The former is a generally applicable procedure for all network operators who shall be responsible for the result of their own assessment. They are obliged to carry out such an assessment on a yearly basis depending on their business development and shall file the assessment result with their respective industrial watchdogs. Such assessment shall focus on aspects such as business demand for export, quantity, scope, category and sensitivity of the concerned data including consent for export where applicable, security level and competence on the data recipient's side including the cyber security situation in the country/region where the data recipient resides, data breach risk and impact after export including re-export. Any change on the recipient side or alteration of purpose, scope, quantity and type of data export or a serious data breach event shall result in a new self-assessment (plus filing).

In case of any of the items listed below, an administrative assessment shall apply, i.e. clearance for data export shall be obtained beforehand from the respective industrial watchdogs that will work under the CAC's guidance and shall complete a review case within 60 working days:

1. personal information involving over 500,000 individuals (including on an accrued basis);
2. data size exceeding 1,000 GB;
3. data concerning nuclear facilities, biochemistry, national defence and military, demographics and health, large-scale project activities, marine environment or sensitive geographic information, etc.;
4. cyber security information about system vulnerabilities and security protection of critical information infrastructures;
5. exporting data by a CIIO; and
6. other circumstances potentially impacting national security and the public interest, of which an assessment is deemed necessary by the regulatory watchdogs.

Compared with Article 37 of the CS Law which only says that export of sensitive data by a CIIO shall require export clearance, the above is again surprisingly a much broader scope of coverage. Considering the fact that more data exporters are already caught by the Draft (see above first section), the Draft indeed substantially expands the circumstances under which a compulsory data export clearance will be triggered. Irrespective of the above data export clearance procedures, the Draft states that the below data are not allowed to be exported abroad:

- personal data of which no prior consent was sought for export or where an export might jeopardise personal interest;
- data of which export brings a risk to national security (e.g. politics, economy, technology, national defence) or may possibly affect national security and damage the public interest; and
- other data of which an export is barred by administrative authorities such as the CAC, the public security authority and the national security authority.

Practitioners' advice

Besides clarifying some implementation details as expected under the CS Law, the Draft actually brings more uncertainties and burdens for digital business. The fact that it regulates data transmission across the border will easily create the impression that most of these uncertainties and burdens will fall upon international business operators whose daily operation very much relies upon the free movement of data. The administrative data export control mechanism may not be business friendly when compared with, for example, the EU. According to the latter's regulatory framework, a B2B- level data protection agreement suffices for data export to a country/region not recognised by the EU as providing an adequate level of data protection.

Considering the broad coverage of the Draft with regard to both whom and what shall be regulated, it is strongly recommended that digital business operators should keep a close eye on the finalised version of the Draft and be prepared for the coming data export control assessment/clearance obligations. Since the Draft also creates many pending uncertainties and questions (for example what exactly is meant by "export" and what those open ended "other" situations are), proactive communication with the regulators and implementation of a proper assessment system, with both supported by experienced legal professionals, will be a must to tackle these new regulatory challenges in China.

*This article was originally published in Digital Business Lawyer and the link is **here**.*

Michael Tan

Partner | Shanghai

Find more articles here:

New Cyber Security Enforcement Agency (July 6)

From July 28, 2017: Opening the Market? China's 2017 Negative List for Foreign Investment (June 30, 2017)

MOFCOM Solicits Public Comments on Measures on Filing Administration of Establishment and Change of Foreign-Invested Enterprises ("FIEs") (June 16, 2017)

Silent upheaval in the automotive sales in China: the promulgation of new automotive sales measure (June 2, 2017)

CAC to Regulate Data Export (April 19, 2017)

TaylorWessing

Email to the editor: shanghai@taylorwessing.com
In case you do not wish to receive emails in the future, please send an email to h.song@taylorwessing.com

TAYLOR WESSING PARTNERSCHAFTSGESELLSCHAFT
von Rechtsanwälten, Steuerberatern, Solicitors und Avocats à la Cour mbB
Sitz Düsseldorf, AG Essen, PR 1530

TAYLOR WESSING Shanghai Representative Office
Unit 1509, United Plaza, 1468 Nanjing West Road
Jing'an District, Shanghai 200040, China

TAYLOR WESSING Beijing Representative Office
Unit 2307, West Tower, Twin Towers, B-12 Jianguomenwai Avenue
Chaoyang District, Beijing 100022, China

TAYLOR WESSING Hong Kong
21st Floor, 8 Queen's Road Central
Hong Kong, China

Website www.taylorwessing.com