China Cyber News Alert

April 2017

Ever since China adopted the Cybersecurity Law in November 2016, questions have been raised as to the security requirements on overseas data transfer. A few aspects of the security assessment, for example, were unclear such as which government body or department is responsible for the security assessment? Which organisations are required to be assessed? What is the scope of the assessment?

With the Law due to come into effect on 1 June 2017, some of those questions have been answered when the State Internet Information Office released the Measures for Carrying out Security Assessment on Personal Information and Important Data for Overseas Transfer (Draft for Public Comment) on 11 April 2017.

1. Functional departments:

China's cyberspace administration bodies are responsible for arrangement and coordination whereas the industry authorities / regulatory bodies are responsible for execution.

2. Key assessment areas:

- Necessity of the transfer of the data
- Involvement of personal information: the amount, scope, type, level of sensitivity, and whether the transfer has been authorised by the personal information subject
- Involvement of critical data: the amount, scope, type and level of sensitivity
- The intended recipient's security measures, capabilities and, competence, and the cybersecurity environment of the country and region where the recipient is located
- Unauthorised data disclosure, modification or even damage risk during overseas transfer or re-transfer
- Whether the transfer and aggregation of data can lead to national security risks, or harm public and personal legal interests

3. Overseas data transfer shall be reported for a security assessment if:

- It contains personal information of more than 500,000 individuals
- It exceeds 1000 GB in size
- It contains information regarding nuclear facilities, chemical and biological sciences, national defence and military projects, population health, major engineering projects, marine environment, and sensitive geographical data
- It contains cybersecurity information such as loopholes in critical information infrastructures
- Critical information infrastructure operators need to provide personal information or critical data to overseas recipients

4. Overseas data transfer is prohibited if:

- It is not authorised by the personal information subject or if it can infringe personal interests
- It can lead to political, economic and technological risks, impact national security, or harm public interests
- Other cyberspace, public security and safety administration bodies deem it non-overseas transferable

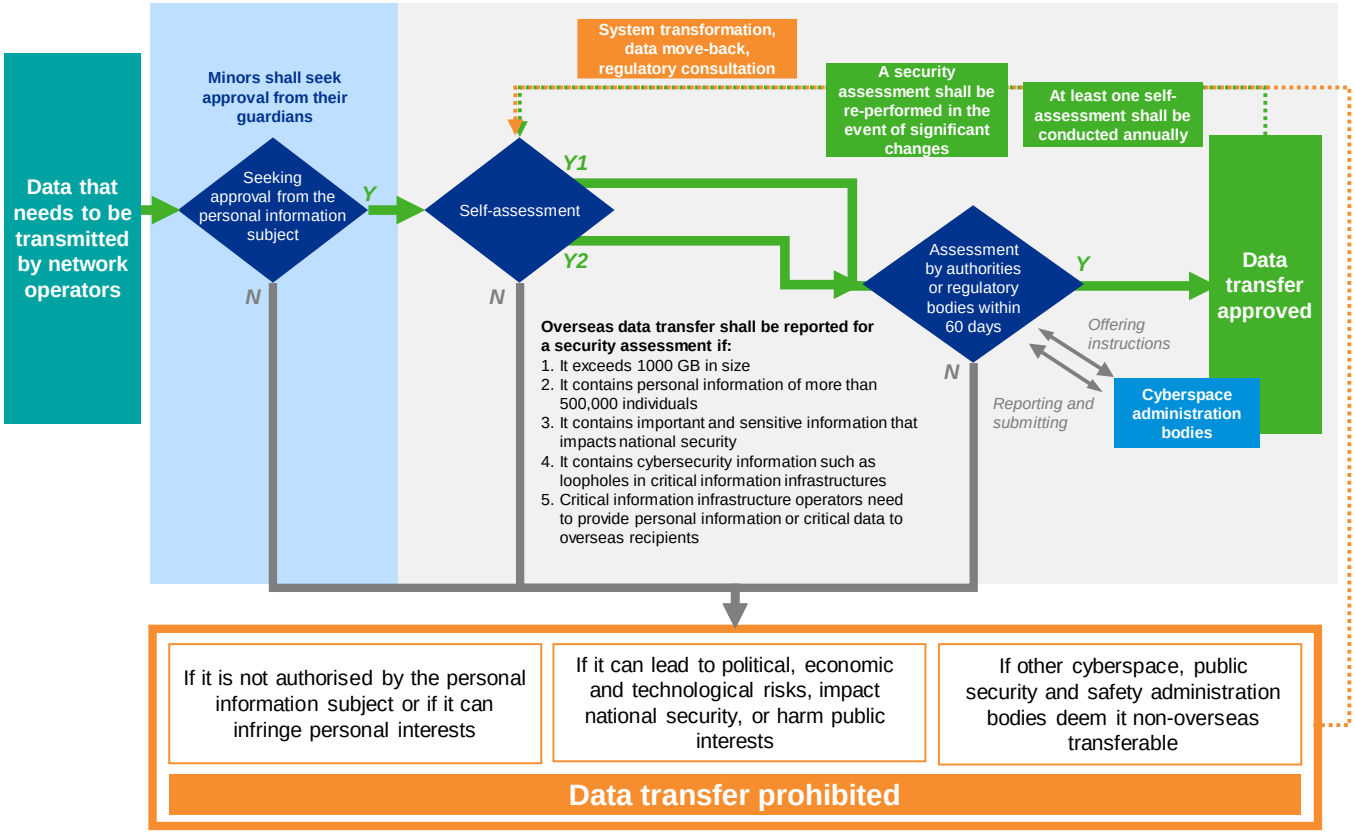
5. Requirements for network operators:

- At least one security assessment shall be conducted annually on transferring data outside of China and the results shall be reported to the industry authorities/regulatory bodies in a timely manner
- A security assessment shall be re-performed if the intended recipients have changed; if there is a significant change in the purpose of transfer; if there is a change in the scope, amount or type of data; if there is a major security incident involving either the recipients or the data

Based on our interpretation of the Measures for Carrying out Security Assessment on Personal Information and Important Data for Overseas Transfer (Draft for Public Comment), the following is a simplified flowchart for companies to follow when conducting an assessment of their overseas data transmission.

Key assessment areas

1. Necessity of the transfer
2. Involvement of personal information, and whether the transfer is authorised by the personal information subject
3. Involvement of critical data
4. The intended recipient's security measures, capabilities and, competence, and the cybersecurity environment of the country and region where the recipient is located
5. Unauthorised data disclosure, modification or even damage risk during overseas transfer or re-transfer
6. Whether the transfer and aggregation of data can lead to national security risks, or harm public and personal legal interests
7 Other important areas that need to be assessed



Contact us

Henry Shek
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Jason R.K. He
Director
Tel: +86 (755) 2547 1129
jason.rk.he@kpmg.com

Matrix Chau
Associate Director
Tel: +852 2685 7521
matrix.chau@kpmg.com

Richard Zhang
Director
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Alvin Li
Associate Director
Tel: +852 2978 8233
alvin.li@kpmg.com

Frank Xiao
Associate Director
Tel: +86 (10) 8508 5456
frank.xiao@kpmg.com

kpmg.com/cn