Technology, Media & Telecommunications

Draft Measures on Transfer of Personal and Important Data out of China Released

Introduction

On 11 April 2017, the Cyberspace Administration of China ("**CAC**") released a highly anticipated draft of the Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data (the "**Draft Measures**") for public comments, for a period of one month until 11 May 2017. The Draft Measures were released pursuant to the Cybersecurity Law ("**CSL**"), which takes effect from 1 June 2017.

Scope of the Draft Measures

Under Article 37 of the CSL, operators of critical information infrastructure ("**CII**") are required to store personal information and important data collected and generated during their operations in the People's Republic of China ("**PRC**") within the country itself, and if such data needs to be transferred overseas, to obtain a security assessment from the authorities prior to such transfer ("**the Data Localisation Requirement**").

However, Article 2 of the Draft Measures extends the scope of the Data Localisation Requirement to cover network operators. This means that network operators whose operation span across the PRC and other countries, but who are not CII operators, are nevertheless subject to the Data Localisation Requirement.

What data has to be localised?

The Data Localisation Requirement applies to two types of data:

(a) personal information – data, whether stored electronically or otherwise, from which an individual may be identified either on its own or together with other data; and

(b) important data – data which is closely conncted with national security, economic development and public interest.

In particular, the definition of "important data" under the Draft Measures remains ambiguous and open to interpretation, and does not clearly define the scope of obligations of network operators under the Data Localisation Requirement.

Separately, prior to any cross-border transfer of any personal data regulated under the CSL, the network operator concerned must notify the individual to whom such data relates, the purpose, scope, content, recipient and country of such transfer, and obtain the consent of the individual for the transfer.

What are the factors to be considered in a security assessment?

Article 7 of the Draft Measures imposes an obligation on network operators to carry out self-assessments for all cross-border transfers of data and to take responsibility for the results of its self-assessments. In carrying out a

security assessment of the relevant data to be transferred overseas, the network operator should place heavier weight on the following factors (Article 8 of the Draft Measures):

(a) the necessity of the cross-border transfer;

(b) in relation to personal data, the amount, scope, type, sensitivity of such data as well as whether the individual to whom the data relates has given his or her consent for the transfer;

(c) in relation to important data, the amount, scope, type and sensitivity of such data;

(d) the security measures taken by and the ability of the recipient to protect the transferred data, as well as the cybersecurity landscape of the country in which the recipient is located;

(e) the possibility of unauthorised disclosure, destruction, alteration and misuse of data transferred overseas, and other similar risks;

(f) the potential risks to national security, public interest and personal interest that the cross-border transfer of data may bring; and

(g) other important factors.

In any event, Article 11 of the Draft Measures prohibits the cross-border transfer of personal data and important data in the following circumstances:

(a) the individual to whom the data relates has not consented to the transfer or his or her personal interests may be jeopardised by the transfer;

(b) the transfer of data may result in risks to the politics, economy, technology and national defence of the PRC, or can potentially undermine national security or public interest; and

(c) other circumstances as prescribed by the relevant authorities, including the CAC.

Article 12 of the Draft Measures requires network operators to conduct self-assessments at least once a year, and to report the results of such self-assessments to the sectoral regulator or the CAC. In particular, where there are changes to content of the data to be transferred, or significant changes to the purpose, scope, amount and type of data, or when the recipient is involved in any major data security breach incident, the network operator should conduct a timely reassessment of the security of the cross-border transfer of data.

When should you request for the relevant authorities to conduct the security assessment?

Where the data to be transferred out of the PRC meets one or more of the following criteria, the network operator concerned will have to request for the relevant sectoral regulator or the CAC to conduct a security assessment of the data transfer:

(a) the data to be transferred contains the personal data of 500,000 or more individuals;

(b) the amount of data exceeds 1000 gigabytes;

(c) the data includes information relating to nuclear facilities, biochemical, national defence, population and health, major projects or events, marine environment and sensitive geographical information;

(d) the data contains information on loopholes in the basic data infrastructure, data security and other cybersecurity related information;

(e) personal information or important data is being transferred overseas by a CII operator; and

(f) other relevant circumstances relating to national security and public interest, as prescribed by the sectoral regulator or the CAC.

Conclusion

The Draft Measures, which extend the scope of application of the Data Localisation Requirements, impose an onerous burden on network operators to ensure that any transfer of personal data and important data out of the PRC is justified and secure. In this regard, it is hoped that after the public consultation, the CAC will be able to provide a clearer definition of what constitutes important data under the CSL, so that network and CII operators can precisely define the scope of their obligations, assess the potential risks and formulate suitable business strategies to comply with the new legislative requirements.

In relation to the obligation to conduct regular self-assessments on the cross-border transfer of data, network operators are reminded give sufficient consideration to the relevant factors prescribed under the Draft Measures, and when in doubt, to seek assistance from professional advisors in conducting these assessments.

Contacts

Rajesh Sreenivasan
Partner
Head, Technology, Media & Telecommunications

D (65) 6232 0751
F (65) 6428 2204
rajesh@rajahtann.com

Benjamin Cheong
Partner
Technology, Media & Telecommunications

D (65) 6232 0738
F (65) 6428 2233
benjamin.cheong@rajahtann.com

Linda Qiao
Senior International Counsel
Rajah & Tann Shanghai Representative Office

D (86) 21 6120 8818
F (86) 21 6120 8820
linda.qiao@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

ASEAN Economic Community Portal

The launch of the ASEAN Economic Community ("AEC") in December 2015, businesses looking to tap the opportunities presented by the integrated markets of the AEC can now get help a click away. Rajah & Tann Asia, United Overseas Bank and RSM Chio Lim Stone Forest, have teamed up to launch "Business in ASEAN", a portal that provides companies with a single platform that helps businesses navigate the complexities of setting up operations in ASEAN.

By tapping into the professional knowledge and resources of the three organisations through this portal, small- and medium-sized enterprises across the 10-member economic grouping can equip themselves with the tools and know-how to navigate ASEAN's business landscape. Of particular interest to businesses is the "Ask a Question" feature of the portal which enables companies to pose questions to the three organisations which have an extensive network in the region. The portal can be accessed at http://www.businessinasean.com.

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 894 0377 to 79 / +632 894 4931 to 32 / +632 552 1977
F +632 552 1978
www.cagatlaw.com

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

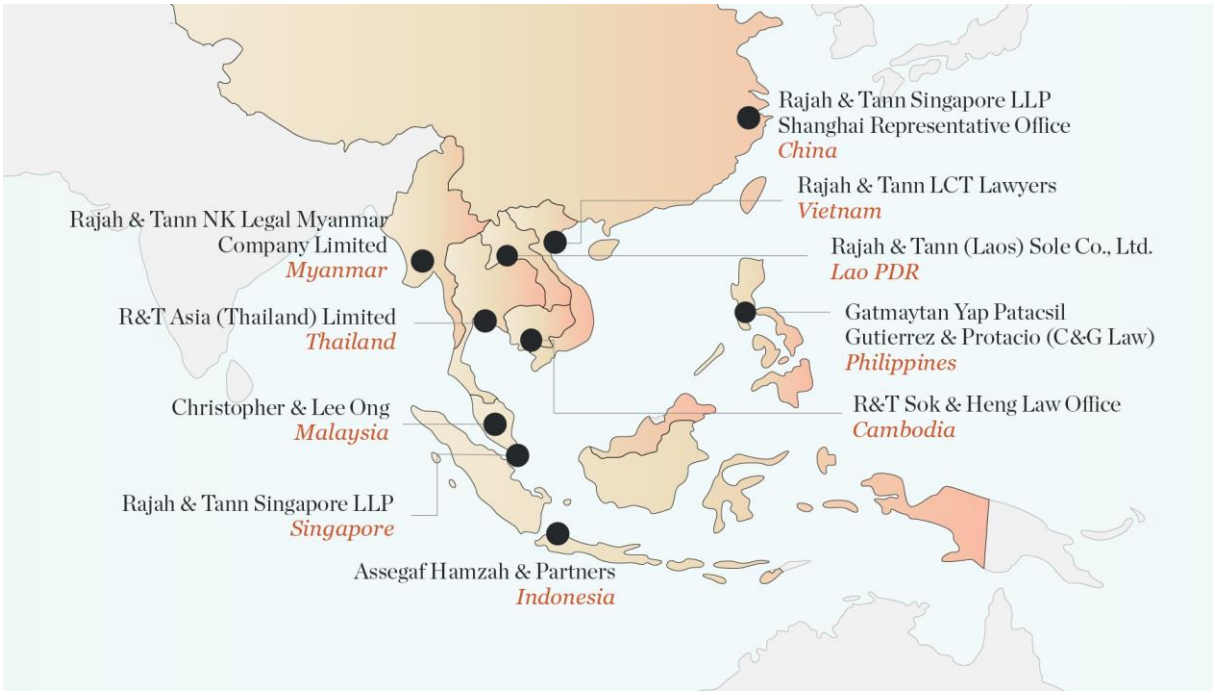
RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 8 3821 2382 / +84 8 3821 2673
F +84 8 3520 8206

Hanoi Office
T +84 4 3267 6127
F +84 4 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.