Regional

Recent Updates to Chinese Cybersecurity and Data Protection Measures

Introduction

The Cyberspace Administration of China ("**CAC**")[1] recently released a series of draft measures and regulations pertaining to cybersecurity and data protection in China for public comments in quick succession. These draft measures and regulations are:

1. Cybersecurity Review Measures[2];
2. Data Security Administrative Measures[3];
3. Regulations on the Protection of Children's Personal Information Online[4]; and
4. Measures on Security Assessment of the Cross-border Transfer of Personal Information[5].

The measures and regulations will impose higher standards and strengthen China's cybersecurity and data protection regime across various sectors and fields of application. This update will examine the measures and regulations, as well as their potential implications.

Cybersecurity Review Measures

On 21 May 2019, the CAC issued the draft Cybersecurity Review Measures ("**CR Measures**") for public comments. The Measures will replace the current Measures for the Security Review of Network Products and Services (Trial Implementation).

Purpose of the Measures

Article 1 of the CR Measures provides that the aim of the CR Measures is to "improve the degree of security and controllability of Critical Information Infrastructures ("**CII**")" and "maintain national security".

In this regard, Article 18 provides that "security and controllability" shall mean "product suppliers and service providers shall not, when supplying products and providing services, unlawfully collect user data,

[1] 国家互联网信息办公室
[2] 网络安全审查办法（征求意见稿）. See http://www.moj.gov.cn/news/content/2019-05/24/zlk_235516.html
[3] 数据安全管理办法（征求意见稿）See http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm
[4] 儿童个人信息网络保护规定（征求意见稿）See http://www.gov.cn/xinwen/2019-06/03/content_5397071.htm
[5] 个人信息出境安全评估办法（征求意见稿）See http://www.gov.cn/xinwen/2019-06/13/content_5399812.htm

unlawfully control and manipulate user devices, unlawfully profit from user reliance and dependence on the products and services, or force users to upgrade their systems."

Establishment of the Cybersecurity Review Unit

Article 5 of the CR Measures provides that the CAC shall establish a national cybersecurity review unit ("**CRU**") in conjunction with other regulatory bodies and entities[6].

In addition, a cybersecurity review office ("**CRO**") will also be established within the CAC to develop cybersecurity review related regulations and procedures, organise cybersecurity reviews, and supervise and review the implementation of decisions.

Requirement to conduct Cybersecurity Review

Article 2 of the CR Measures provides that CII Operators must conduct cybersecurity reviews where procurement of network products or services may affect national security. In this regard, CII Operators are defined under Article 18 as "Operators recognized by CII protection authorities".

Article 6 of the CR Measures provides that when procuring network products or services, CII Operators must conduct a pre-assessment of the potential security risks before such products or services go online and produce a security risk report.

In addition, CII Operators are also required to apply to the CRO for cybersecurity review where there is a possibility that the following circumstances might occur:

(i) shutdown or function failure of the CII;
(ii) leakage, loss, corruption or cross-border transfer of massive personal data and important data;
(iii) supply chain security threats compromising the operation and maintenance, technical support and upgrading of the CIII; and
(iv) other potential risks that could severely jeopardize the CII.

Article 7 of the CR Measures further requires that CII Operators must contract with product suppliers and service providers on the basis that any contracts would only come into effect after the contemplated transaction has completed the cybersecurity review.

[6] Such as the National Development and Reform Commission, the Ministry of Information and Industry, the Ministry of Public Security, the Ministry of Commerce, the Ministry of Finance, the People's Bank of China, the State Administration of Small Markets, the State Administration of Radio and Television, the State Secrecy Bureau, and the State Cryptography Administration Office.

Article 19 also provides that if members of the CRU are of the opinion that any products or services or infocomm activities affect or may affect national security, the CRO may carry out a cybersecurity review against such products, services or activities.

Factors considered in review

Article 10 of the CR Measures provides that in assessing the potential national security risks brought about by procurement activities, the CRO will take into consideration the following factors:

(i) Impact on the CII's ability to continue operations in a safe and stable manner, including the possibility that the CII may be manipulated, interruption to its services or disruption to its business continuity;
(ii) Possibility that large quantities of personal data or important data would be leaked, destroyed, corrupted, damaged or transferred abroad;
(iii) The controllability, transparency of the products and services, and the security of the supply chain, including possibility of disruption to the supply of products and services due to political, diplomatic, trade relations and other non-technical reasons;
(iv) Impact on national defence, military industries and CII industries and technologies;
(v) The compliance with national laws and administrative regulations by the product suppliers and service providers, and the obligations and duties which such suppliers and providers have undertaken;
(vi) Whether product suppliers and service providers are funded or controlled by foreign governments and similar situations; and
(vii) Any other risks and threats that may severely compromise the security of the CII or the country.

Review process

Article 9 provides that the initial phase of the cybersecurity review should be completed within 30 working days, which may be subject to an extension of 15 days.

Article 11 provides that the initial review results will be submitted to the members of the CRU. Where the opinions of the members are unanimous, it will be made final; where there are discrepancies, the results will be subject to a special review procedure.

Article 13 provides that the special review procedure shall be completed within 45 days in principle, which may be extended further for complex cases.

Our analysis

The CR Measures reveal heightened concern by China over the stability and security of its CIIs vis-à-vis external threats and resolve to strengthen the state of its cybersecurity and national security.

On 15 May 2019, the US Department of Commerce added Chinese telecommunications giant Huawei and over 70 subsidiaries to its entities list under the Export Administration Regulations. This had effectively cut off Huawei's access to parts and software from US-based companies. A little more than a year ago, another Chinese telecommunications giant, ZTE, was slapped with a 7-year ban prohibiting US companies from providing exports to ZTE. Although the bans on export to ZTE were eventually lifted, these incidents had no doubt raised China's alarm towards the risks of over dependence on foreign technological imports. The inclusion of potential disruption to supply chain, in particular those "due to political, diplomatic, trade relations and other non-technical reasons" as part of the factors for cybersecurity review was likely to have been drafted with these incidents in mind, with a view for the CAC to regulate and control the extent of CII Operators' dependence on foreign technologies.

Parties contracting with CII Operators will need to factor both the requirement for cybersecurity review and the potential duration of such reviews into their considerations, and bear in mind that passing the cybersecurity review is now virtually a mandatory condition precedent for such contracts to proceed.

Data Security Management Measures

On 28 May 2019, the CAC issued the draft Data Security Management Measures ("**DSM Measures**") for public comments.

Under the 13th National People's Congress Legislative Plan, Data Security Law is listed as one of the draft laws "for which the conditions are relatively mature, and which are planned to be submitted for deliberation during the term". The DSM Measures can therefore be seen as a herald for the Data Security Law pending its legislation.

The DSM Measures are divided into 4 Parts:

(i) General Provisions;
(ii) Data Collection;
(iii) Data Processing and Usage; and
(iv) Supervision and Regulation of Data Security.

General Provisions

The General Provisions set out the principles underlying data protection in China and the scope of the DSM Measures.

Purpose

Article 1 of the DSM Measures provides that the DSM Measures were developed for the purposes of "safeguarding national security, public interest, protecting the lawful rights and interests of citizens, legal entities and other organizations in cyberspace".

Article 3 makes clear that the State balances the interests of data security and protection against the interests of promoting the development and use of data resources.

Scope

Article 2 of the DSM Measures sets out its scope by providing that it applies to the collection, storage, transfer, processing, use and other activities relating to data conducted over the internet within China.

Actions to comply

Article 6 sets out the actions which Network Operators must take in order to fulfil their data protection obligations. Such actions include:

(i) Establishing data security standards;
(ii) Formulating data security plans;
(iii) Implementing technical measures for data protection;
(iv) Carrying out data security risk assessments;
(v) Developing emergency response plans for cybersecurity incidents;
(vi) Dealing with security incidents in a timely manner, and
(vii) Organizing data security training sessions.

In this regard, "Network Operators" is defined under Article 38(1) to include "network owners, network managers, and internet service providers".

Regional

Data Collection

General requirements

Part 2 of the DSM Measures sets out rather detailed and comprehensive obligations for Network Operators in respect of collection and use of personal data from individuals. Some of the requirements are not dissimilar to those in other jurisdictions, such as Europe's General Data Protection Regulation ("**GDPR**") or Singapore's Personal Data Protection Act ("**PDPA**").

Article 7 requires Network Operators to develop and disclose rules for collection and use of personal data ("**Rules**").

Article 8 requires such Rules to be specific, comprehensible and easily accessible, as well as to include key information such as:

(i) The purpose, type, quantity, frequency, method, scope and other information of the collection and use of personal data;
(ii) The place of storage, period for which personal data will be retained ("**retention period**"), and the method of disposal of personal data upon expiration of retention period;
(iii) Rules for disclosing personal data to third party (if personal data is to be provided to third parties);
(iv) Strategies for personal data protection and other relevant information;
(v) Ways and methods for the individuals to withdraw consent, or access, correct and delete his/her personal data; and
(vi) Channels and methods of making complaints and reports.

Article 9 further provides that Network Operators may only collect personal data after the individual has provided express consent to the collection and use of personal data.

Article 12 requires Network Operators to seek consent from guardians before collecting personal data from minors under the age of 14.

Article 14 further provides that Network Operators who have obtained personal data from third party sources share the same responsibilities in protecting such personal data as if they had directly collected such data themself.

Dealing fairly

In addition to commonly found data protection requirements, the DSM Measures also require Network Operators to deal fairly with individuals. For example:

Article 11 prohibits Network Operators from bundling functions or forcing or misleading individuals to consent to collection of personal data, on the grounds of "improving service quality, user experience, content recommendation or research and development of new products". It also prohibits the denial of core service functions because consumers have refused to provide personal data for ancillary purposes.

Article 13 also prohibits Network Operators from discriminating against customers, for example in terms of service quality and price, on the basis of whether consent was given or the scope of such consent.

Data Protection Officer ("DPO")

The DSM Measures also introduced the concept of a "person responsible for data protection", which is similar to the role of a DPO under the PDPA and GDPR.

Article 17 requires Network Operators to appoint a person with relevant managerial experience and professional expertise on data protection to be DPO when collecting important or sensitive personal data for business purposes.

Article 18 sets out the responsibilities and obligations of such DPO which includes:

(i) Organising the formulation of the data protection plan and managing its implementation;
(ii) Organising data security risk assessments and rectify and eliminate risks;
(iii) Reporting to relevant government authorities and cybersecurity administration authorities on the protection of data and handling of incidents; and
(iv) Accepting and handling complaints and reports.

Collection of important or sensitive data

Article 15 provides that when Network Operators collect "important data or sensitive personal data" for business purposes, they must make a filing with the local cybersecurity administration authorities. The information to be filed shall include the rules for collection and use, the purpose, quantity, method, scope, type and retention period for collection, but shall exclude the personal data itself.

In this regard, "important data" is defined under Article 38 to include "data, which if leaked may directly affect national security, economic security, social stability, public health and security, such as undisclosed government information, large-scale population, genetic health, geographic, mineral resources." It is clarified that "important data" will usually not include "information related to the production and operation of enterprises, internal management information or personal information".

"Sensitive personal data" is not defined in the DSM Measures itself. However, "sensitive personal information" is defined under the draft Measures on Security Assessment of Cross Border Transfer of

Personal Information (discussed below) to mean "personal data which once disclosed, stolen, falsified or illegally used, may endanger the person or property of the individual or cause damage to the reputation, physical or mental health of the individual." It is likely that the phrase will have a similar definition under the DSM Measures when it comes into effect eventually.

Automated collection of data

The Measures also addressed the use of web crawlers and other means of automated data collection.

Article 16 provides that the use of automated means of accessing or collecting data from websites shall not interfere with the normal operations of such websites. If the act of collection severely interferes with the operations of such websites (e.g. when it exceeds 1/3 of the average daily traffic volume to such websites), the Network Operator shall cease such collection and access when requested by the website.

Data Processing and Usage

The third part of the DSM Measures deals with the processing and use of data by Network Operators.

General requirements

Again, the DSM Measures contain requirements similar to those found in other jurisdictions. Some examples are highlighted below.

Article 19 requires Network Operators to categorise, back-up and encrypt personal data to strengthen protection of personal data and important data.

Article 20 requires Network Operators to collect and use data only during the retention period as stated in their data collection Rules, beyond which such data must be securely destroyed or anonymized such that they cannot be used to identify the individual.

Article 21 provides that Network Operators must at an individual's request allow access to, correction or deletion of that individual's personal data.

Article 22 further provides that Network Operators must not use personal data beyond what is provided in the Rules. If personal data is to be used for a different scope, additional consent is required.

Article 27 also provides that prior to disclosing personal data to third parties, Network Operators must analyse the risks involved, and seek consent from the individuals concerned, unless the disclosure fell within a list of exemptions. Such exemptions include:

(i) Personal data collected from public channels which disclosure is consistent with the individual's understanding;
(ii) Personal data voluntarily disclosed by the individual;
(iii) Personal data had been anonymized;
(iv) Disclosure is necessary for law enforcement agencies to perform their duties; and
(v) Disclosure is necessary for safeguarding national security, social and public interest, or protecting the life or security of the individual concerned.

Information dissemination via big data analytics

In addition, the Measures also set out requirements pertaining to information dissemination via big data analytics.

Article 23 requires Network Operators using data and algorithm to make "targeted recommendations" of news articles and advertisements to users to clearly stipulate to the users that they are the subject of such "targeted recommendations", and to provide them with the option to opt out. In addition, such targeted recommendations must comply with laws and regulations, respect society standards of morality and ethics, and be honest and diligent.

Article 24 requires Network Operators to stipulate when news article, blog posts, posts and comments have been synthesized or generated by big data, AI or other technologies. Network Operators are also prohibited from synthesizing or generating content for the purpose of profits or damaging interests of any persons.

Data trading and transferring

The Measures also set out Network Operators' obligations when trading or transferring personal data. Article 28 requires Network Operators to conduct risk assessment and notify to the relevant regulatory department for approval prior to disclosing, sharing or trading personal data, or transferring personal data across borders to third parties. If there is no clear regulatory department, Network Operators are required to report to the Provincial Cybersecurity Administration Authority for approval. In addition, the rules for transferring data across borders must be complied with.

Article 30 further provides that Network Operators must set out data security requirements and responsibilities for third parties to whom personal data has been transferred, and are responsible for supervising the data security management of such third parties. In the event a data security incident occurs, the Network Operator may be deemed partly or even wholly liable, unless it can prove it has not committed any fault.

Supervision and Regulation of Data Security

The fourth part of the measures deal with supervision and regulation of data security.

Data security incident

Article 35 sets out the requirements for Network Operators in the event a data security incident occurs, such as when personal data has been leaked, destroyed, corrupted, damaged or lost, or if the risk of data security incident occuring has increased significantly. Network Operators are required to immediately notify the individuals concerned, as well as to report such incidents or occurrences to competent supervising department and cyberspace administration authorities.

Provision of data to State Council Departments

Article 36 provides that if relevant competent departments of the State Council require network operators to provide relevant data in its possession for the purpose of national security, social management, economic control and other functions and duties, Network Operators must provide such data.

In turn, the State Council departments are required to assume the responsibility of protecting the data, and are not permitted to use the data for purposes unrelated to the performance of its functions.

Enforcement

Article 34 provides that when Network Operators has been found to be in breach of its data security management obligations, a cyberspace administration authority may urge it to rectify such breaches.

Article 37 provides that if Network Operator violates the Measures, the competent authority may impose disciplinary actions in accordance with relevant laws. Such disciplinary action may include public censure, confiscating income obtained through non-compliance, suspension of business, ceasing business operation for rectification, shutting down of websites, revocation of relevant licences or permits. Network Operators may also be liable for criminal liability if their violation constitutes a criminal offence.

Our analysis

The DSM Measures had raised personal data protection in China to an unprecedented level, reflecting a heightened state of concern and awareness of the importance of personal data protection. Many of the requirements under the DSM Measures are comparable to, if not more stringent than, data protection laws in other jurisdictions.

The DSM Measures will have significant impact on China's new media and data analytics companies. Article 11 seeks to regulate and limit the circumstances under which personal data may be collected. Article 16 serves to control automated collection of data. Articles 23 and 24 also control the way in which new media and data analytics companies may generate and recommend media content.

The DSM Measures, through Article 36, also accord the "relevant departments of the State Council" with broad powers to demand the surrender of personal data. This may prove to be a source of concern for foreign governments and companies.

Regulations on Protection of Children's Personal Information Online

On 31 May 2019, the CAC issued the draft Regulations on the Protection of Children's Personal Information Online ("**Regulations**") for public comments.

Article 1 of the Regulations provides that it is developed for the purposes of "protecting children's personal information security and promoting the healthy development of children." In this regard, Article 27 explained that "children" for the purpose of the Regulations refer to minors under the age of 14.

Higher standards

It is noted at the outset that many requirements under the Regulations are similar to those under the draft DSM Measures.

However, it may also be useful to note certain salient features of data protection for children. There must be a higher level of protection for the personal data of children given that they are more vulnerable. Further, as children may lack the capacity to give consent to the collection and use of data directly, consent must be obtained from their guardians.

In this regard, Article 5 requires Network Operators to "formulate dedicated policies and user agreement for the protection of children's personal information". Network Operators are also required to appoint dedicated DPOs for children's personal information.

Article 7 also requires Network Operators to inform the guardian in a prominent and clear way when collecting and using personal data of children, and obtain their express consent on a specific, informed and voluntary basis.

Article 8 also requires Network Operators when seeking consent to provide the option to refuse consent, and provide the guardian with certain information including:

(i) the purpose, scope, method and retention period of the collection, storage, use, transmission, and disclosure of children's personal data;
(ii) the place of storage, retention period, and method of disposal of children's personal data upon expiration of retention period;
(iii) security measures taken to protect children's personal data;
(iv) contact information of the DPO for children's personal data; and
(v) consequences of refusing to provide consent.

Further, when there are any changes to the aforementioned information, the Network Operator is required to update the Guardian and obtain their consent again.

Under Article 12, Network Operators are also required to restrict and control access to children's personal data by its staff and personnel strictly in accordance with the principle of minimisation. Access to children's personal data by its staff and personnel must be approved and documented by the children's personal data DPO. In addition, Network Operators are also required to implement technical measures to prevent illegal copying and downloading of children's personal data.

Articles 14 and 15 also require Network Operators to inform and obtain consent from the guardian prior to sharing personal data of children with, or transferring children's personal data to a third party.

The situations in which Children's personal data may be collected, used, transferred or disclosed without consent are also more limited as compared to general categories of personal data, and are only permissible for the purposes of:

(i) safeguarding national security or public interest;
(ii) eliminating urgent risks to the children's lives or property; or
(iii) other circumstances as prescribed by laws or regulations.

It should be noted that data anonymisation, or the fact that children's personal data had been voluntarily disclosed by the guardian or are collected from public channels are NOT viable defences under the Regulations.

Finally, the sanctions that may be imposed are also more explicit as compared to the Measures. Under Article 25, any Network Operator who violates the Regulations may face public censure, be subject to a fine between 2 to 10 times of its illegal income or up to 1 million RMB if there is no such income. The persons in charge may also be fined between 10,000 and 100,000 RMB. If the offences are egregious, Network Operator may face suspension of business, ceasing business operation for rectification, shutting down of websites, revocation of relevant licences or permits. Network Operators may also be liable for criminal liability if their violation constitutes a criminal offence.

Our analysis

"Children" is defined under the Regulations to refer to minors below age of 14. This may present novel challenges for Network Operators in compliance, as they must now implement new measures or tweak existing ones to ascertain the age of network users.

Network Operators who may be collecting and using Children's personal data should also note the requirement to now have a dedicated officer overlooking such data activities.

Measures on Security Assessment of the Cross-border Transfer of Personal Information

On 31 May 2019, the CAC issued the draft Measures on Security Assessment of Cross Border Transfer of Personal Information ("PI **Measures**") for public comments.

Article 1 of the PI Measures provides that they are developed "for the purpose of protecting the cross-border transfer of personal data".

Article 19 also provides that where China had concluded agreements or treaties with other countries, regions and internal organisations containing specific provisions on cross-border transfer of personal data, such agreements or treaties shall take precedence unless China has declared reservations over such provisions.

Requirement for security assessment

Article 2 provides that Network Operators must first conduct a security assessment prior to transferring personal data collected within the territory of China to another country ("**cross-border transfer of personal data**"). Network Operators shall not carry out such transfer if the security assessment reveals that such transfer may endanger national security, compromise public interest, or fail to provide adequate protection for the personal data.

Article 3 requires Network Operators to apply for security assessment with the provincial cybersecurity administration authorities prior to the cross-border transfer of personal data.

Documents to be submitted

Article 4 sets out the documents which the Network Operators must submit, which includes:

(i) the contract between the Network Operator and the recipient ("**Contract**"); and

(ii) a report on the risks and security measures of the cross-border transfer of personal data ("**Report**").

In this regard, Article 17 provides that the Report must include:

(i) the background information of the Network Operator and Recipient; and
(ii) the relevant information pertaining to the cross-border transfer, including the duration, volume and scale of such transfer, and whether the personal data will be transmitted to a third party after the transfer.

Factors considered

Article 6 provides that in considering the application, the authorities will have regard to the following:

(i) whether the transfer complies with relevant laws and regulations;
(ii) whether the terms of the Contract can protect the legal rights and interests of the individuals;
(iii) whether the Contract is enforceable;
(iv) whether the Network Operator has past histories of transgression, and whether any significant network security incident had happened in the past; and
(v) whether the personal data had been obtained legally and legitimately.

Record retention

Article 8 requires Network Operators to retain records of cross border transfer of personal data for at least 5 years. Such records shall contain:

(i) the date and time of such cross-border transfer;
(ii) the identity of the recipient; and
(iii) the type, volume and level of sensitive of the personal data transferred.

Suspension/ Termination of cross-border transfers

Article 13 also sets out that in the event of certain circumstances, the cybersecurity administration authorities may request a Network Operator to suspend or terminate cross-border transfer of personal data. Such circumstances include:

(i) where data abuse or data leakage has occurred to the Network Operator or the recipient;
(ii) where the individuals concerned are unable or find it unduly difficult to protect their legal rights and interests in relation to their personal data; and
(iii) where the Network Operator or recipient is incapable of protecting personal data.

Requirements for contracts

The PI Measures also set out detailed provisions relating to the use of Contracts between the Network Operator and the recipient.

Article 13 provides that Contracts or other legally binding documents between Network Operators and recipients must contain certain provisions to the following effects:

(i) the purpose of the transfer, the types of personal data transferred and retention period;
(ii) the individual concerned is the beneficiary of the clauses in the Contract involving the rights and benefits of the personal data subject;
(iii) where the legal interests of the individual have been harmed, the individual may claim damages against the Network Operator or the recipient jointly or severally, and the Network Operator or recipient shall compensate the individual unless it is proven that the Network Operator or recipient is not liable;
(iv) if the legal environment in the recipient's country has changed such that it is difficult to perform the Contract, the Contract shall be terminated, or the security assessment shall be conducted again; and
(v) the termination of the Contract cannot exonerate the Network Operator and the recipient from their respective obligations relating to the legal rights and interests of the individual as specified in the Contract, unless the recipient has destroyed or anonymised the personal information received.

In addition, the PI Measures also impose certain mandatory obligation on Network Operators and recipients.

Article 14 provides that Network Operators must:

(i) inform the individual of the purpose of transfer, the types of personal data transferred and retention period;
(ii) provide a copy of the Contract at the request of the individual; and
(iii) relay any requests from the individual to the recipient, including requests for compensation. Where the individual is unable to obtain compensation from the recipient, the Network Operator shall be responsible for compensating the individual.

On the other hand, Article 15 sets out obligations of the recipient, which includes:

(i) to provide access to, amend or delete personal data of an individual at his or her request;
(ii) to use personal data strictly in accordance with the terms of the Contract and not exceeding the retention period;

(iii) to verify that its entry into and performance of the Contract will not violate local laws and regulations, and to inform the Network Operator and provincial cybersecurity administration authorities in the event of any changes to the laws of the recipient which may affect the performance of the Contract.

In addition, Article 16 also provides that recipients shall not transmit personal data which it received to a third party unless the following conditions are met:

(i) the recipient had informed the individual concerned of such further transmission;
(ii) the recipient covenants that it will, when requested by the individual, stop such transmission and request the third party to destroy personal data which had been transmitted and received;
(iii) where sensitive personal data is concerned, the individual has given his or her consent; and
(iv) the Network Operator has agreed to compensate the individual if any harm is caused to the individual's lawful rights and interests arising from such transmission.

Our analysis

Unlike Singapore's PDPA which requires organisations seeking to engage in cross border transfer of personal to conduct self-assessments, the PI Measures require Network Operators seeking to do so to apply for and be subject to security assessments conducted by provincial cybersecurity administration authorities. Furthermore, the PI Measures also seek to regulate the further transmission of personal data by recipient to third parties.

Parties seek to conduct cross-border transfer of personal data out of China should therefore note such requirements.

In addition, parties should also note the requirements for mandatory obligations to be imposed in contracts on Network Operator and data recipients.

Disclaimer: *Rajah & Tann Singapore LLP Shanghai Representative Office is a foreign law firm licenced by the Ministry of Justice of the People's Republic of China (the "**PRC**"). As a foreign law firm, we may not issue opinions on matters of PRC law. Any views we express in relation to PRC laws and regulations for this matter are based on our knowledge and understanding gained from our handling of PRC-related matters and through our own research, and also from our consultations with PRC lawyers. Therefore, such views do not constitute (and should not be taken as) opinion or advice on PRC laws and regulations.*

Contacts

Benjamin Cheong
Partner
Rajah & Tann Singapore LLP

D +65 6232 0738
F +65 6428 2233

benjamin.cheong@rajahtann.com

Chen Xi
Partner (Foreign Lawyer)
Rajah & Tann Singapore LLP

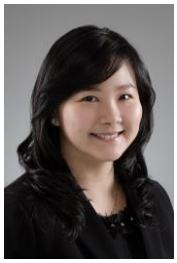
D +65 6232 0158
F +65 6428 2256

chen.xi@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



Chia Lee Fong
Partner (Foreign Lawyer)
Rajah & Tann Singapore LLP

D +65 6232 0734
F +65 6428 2254

lee.fong.chia@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.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) 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 7304 0763 / +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
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

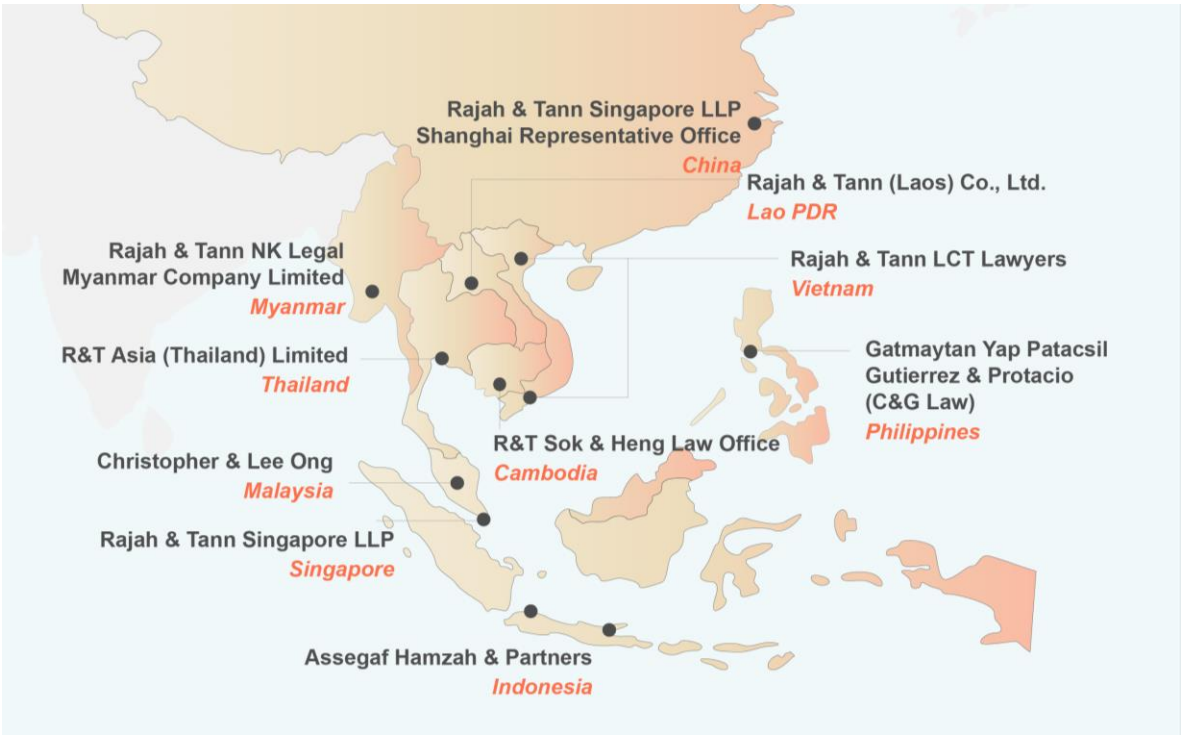
RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP Shanghai Representative Office works closely with Rajah & Tann Singapore LLP's China service group in Singapore to handle a wide range of matters for both domestic and foreign clients in China. The key areas of expertise of our lawyers are in joint ventures, mergers & acquisitions, foreign investments, financing, construction, infrastructure, intellectual property and dispute resolution.

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