GIDE

GIDE LOYRETTE NOUEL

client alert

TMT | CHINA | 17 MARCH 2017

CHINA ISSUES NEW CYBER SECURITY LAW

On 7 November 2016, the Standing Committee of the National People's Congress of the People's Republic of China ("**PRC**" or "**China**") issued the *Cyber Security Law* ("**CSL**"). This new law, which will come into force on 1 June 2017, imposes stringent obligations on network operators, with an aim to improve online security, prevent networks from attacks and intrusion, and ensure the integrity, correct use and confidentiality of network data.

"Network operators" are defined as network owners, network managers and network services providers. "Network" is defined as a system comprising computers and/or other information terminals and equipment that collects, stores, transmits, exchanges, and processes information under specific rules and procedures.

Given the broad scope of the CSL, the law will likely impact a wide range of business operators in China. This Client Alert highlights its main provisions.

GENERAL OBLIGATIONS OF NETWORK OPERATORS

Under the CSL, all network operators have a series of obligations to prevent their networks from attacks and intrusion, including:

- Formulating internal security management systems and designating a person in charge of cyber security;
- Implementing technical measures to prevent computer viruses, network attacks, and network intrusions;
- Implementing technical measures to monitor and record network operations and cyber security incidents;
- Monitoring and recording network operations and cyber security incidents, and maintaining operation logs for at least six months; and
- Backing up and adopting encryption of important data.

Network operators will also be required to put in place contingency plans to promptly respond to security incidents, such as attacks, intrusions, bugs, and viruses.

Non-compliance with these obligations may result in fines ranging from RMB 10,000 to RMB 100,000. Additional fines may be imposed on the person directly in charge.

Network operators may be required to provide technical assistance and support to authorities during national security or criminal investigations.

KEY INFORMATION INFRASTRUCTURE

Operators of key information infrastructure ("**KII**") will be subject to additional requirements. KII is broadly defined as information infrastructure in certain key industries such as public communications and information services, energy, transport, water resource utilisation, finance, public services, e-government, and other key information infrastructure that may have a significant impact on national security and public interests. The exact scope of KII will be identified by the State Council.

Under the CSL, KII operators are required to:

- Set up a dedicated cyber security management body and designate people in charge, who must have passed a security background check;
- Provide regular cyber security training, as well as technical training and examination;
- Implement disaster recovery backup for important systems and databases; and
- Formulate emergency plans for cyber security incidents and regularly conduct drills.

In addition, KII operators must conduct an assessment of its cyber security at least once a year and submit the results to authorities. They will also be subject to random cyber security risk reviews by authorities.

Non-compliance with these obligations may result in fines ranging from RMB 100,000 to RMB 1,000,000. Additional fines may be imposed on the person directly in charge.

Another key consequence for KII operators is the obligation to store in the PRC all personal data and other important information collected and generated in the PRC. Any transfer of such data and information outside China must be necessary for business purposes and will be subject to a security assessment conducted by authorities. An unauthorised transfer may result in fines for the operator ranging from RMB 50,000 to RMB 500,000, as well as other penalties such as revocation of the network operator's business licence or shutdown of its website. Additional fines may be imposed on the person directly in charge.

STRENGHTENED REQUIREMENTS FOR EQUIPMENT USED BY NETWORK OPERATORS

Under the CSL, critical network equipment and specialised cyber security products must comply with compulsory national standards and be certified by a qualified organisation. However, authorities have yet to release the catalogue of critical network equipment and specialised cyber security products.

In addition, any purchase of network products or services by a KII operator that may threaten national security will be subject to national security review by PRC authorities. Non-compliance with this obligation may result in fines ranging from one to 10 times the purchase price, and additional fines may be imposed on the person directly in charge.

Suppliers of the above equipment must therefore also comply with these requirements in order to penetrate the Chinese market.

DATA PROTECTION

The CSL codifies (and goes further) certain existing provisions in various regulations related to personal data protection. In particular, network operators must:

- Keep all personal data that they have collected in strict confidence and adopt measures to protect such data;
- Obtain the consent of the person whose personal data is to be collected before they collect and use such data;
- Not collect any personal information that is unrelated to the services they provide;
- Not divulge, tamper, or destroy personal information that they have collected, and not disclose personal information to a third party without the prior consent of the person whose personal information was collected (unless such information has been processed to prevent the identification of such person);
- Upon the request of any person whose personal information was collected, delete his or her personal information (if it has not been used in compliance with the law or any agreement between such individual and the network operator) or correct such information (if it appears inaccurate).

Non-compliance with these obligations may result in fines ranging from one to 10 times the illegal earnings of the operator, or up to RMB 1,000,000 in the absence of any illegal earnings. Violators may also face other penalties such as revocation of their business licence or shutdown of their website. Additional fines may be imposed on the person directly in charge.

COMMENTS

This important piece of legislation raises several concerns given its broad scope, unclear provisions, and tough requirements on network operators. Detailed implementing rules are needed to clarify certain issues, including the exact scope of KII and the catalogue of critical network equipment and specialised cyber security products.

Gide will continue to follow the implementation of the CSL and any development or interpretations regarding cyber security and data protection regulations in the PRC. Please feel free to contact us should you have any questions.

CONTACTS

Beijing

GUO MIN
guo@gide.com

Shanghai

FAN JIANNIAN
fan@gide.com

ANTOINE DE LA GATINAIS
gatinais@gide.com

China / Hong Kong

DAVID BOITOUT
boitout@gide.com

Paris

CHARLES-HENRI LEGER
leger@gide.com

GUILLAUME ROUGIER-BRIERRE
rougier@gide.com

THOMAS URLACHER
urlacher@gide.com

STEPHANE VERNAY
vernay@gide.com

BEIJING | Unit 01, Fl. 15, Tower B Parkview Green Tower - No. 9, Dong Da Qiao Road - Chaoyang District - Beijing 100020 - P.R.C. | tel. +86 10 6597 4511 | beijing@gide.com
HONG KONG | Suite 3701, Edinburgh Tower, The Landmark, 15 Queen's Road Central - Central, Hong Kong SAR - P.R.C. | tel. +852 2536 9110 | hongkong@gide.com
SHANGHAI | Suite 2008, Shui On Plaza, 333 Huai Hai Zhong Road - Shanghai 200021 - P.R.C. | tel. +86 21 5306 8899 | shanghai@gide.com
PARIS | 22, cours Albert 1er - 75008 Paris - France | tel. +33 (0)1 40 75 60 00 | info@gide.com - gide.com