CLIFFORD
CHANCE

Briefing note June 2017

New PRC Cyber-Security Law comes into Force

The *Cyber-security Law of the People's Republic of China* (the Law) took effect on 1 June 2017. The Law applies to everyone who operates networks in the PRC and will have particular impact on multinational corporations. The Cyberspace Administration of China (CAC) has issued a series of regulations implementing the law, and has also asked the public for comments on other proposed implementing rules, including measures affecting the transfer of personal data outside the PRC.

Application

The Law states that China will take steps to monitor, defend and address cyber-security risks and threats originating from within and outside China. It applies to the construction, operation, maintenance and utilisation of networks as well as the regulation of cyber-security within the PRC. The law applies to both the internet and individual intranets as long as there is any network-related activity taking place in the PRC.

Among other things, the Law focuses on network operation security and network information security.

Network operators

A network operator refers to an entity or person that owns or administers a network and/or (importantly) provides services through a network. By definition, therefore, any person or entity in China who has access to a network may become a network operator.

Networks in China are given grades based on their perceived importance and have to abide by specific standards related to the network functions, the number of users and the potential impact of a network failure.

Information infrastructures

The Law also focuses on so-called *"critical information infrastructures"* (CIIs). If a network operator operates a CII, it will be subject to additional rules.

CIIs include information infrastructures for public communication and information services, utilities (such as energy, transportation and water), public services and online government services. Crucially, the financial sector is also included.

Pending the specific scope of CIIs designated by the regulators, financial institutions operating in the PRC (especially those with a large retail client base) are advised to participate in the consultation process to be organised by the regulators in order to ensure that their concerns can be properly addressed. CIIs also include networks that may endanger state security, the economy, public welfare and the public interest if they were destroyed, disabled or subject to data breaches.

CII operators must carry out an assessment of their facilities' cyber security at least once a year and report potential risks and proposed remediation measures to the authorities.

Key issues

- The new law states that the PRC will monitor and defend itself against cyber-security risks and threats.
- It applies to anyone operating networks within the PRC, even if this is only a closed intranet.
- Multinationals should beware of potential issues regarding the export of data outside the PRC.

Items that are deemed to constitute critical network equipment as well as specialised cyber security products must have security certification before being supplied or sold.

Where CIIs purchase network products and services that may influence national security, these must go through a security review carried out by the CAC and other government authorities.

Network information security

The Law prohibits a network operator from disclosing personal information of living individuals to others, including overseas, without the consent of the person whose data may have been collected.

The CAC has recently clarified that a person can give implied consent to their data being transferred through a number of everyday operations, such as making an international phone call, sending an email, instant messaging and performing transactions online.

There is also an exception that allows for the processing of personal information on an anonymised basis for statistical purposes. Organisations may therefore transfer redacted personal information offshore for the purpose of data analysis without the need to obtain the consent of the data subject.

Data export

The *Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data* govern restrictions on exporting personal information and important data out of China by network operators in China. Self-assessment would be required for any data export, and regulatory assessment would be further triggered in certain prescribed scenarios.

These measures are presently under consultation. CAC originally intended to adopt these measures on 1 June 2017 (the effective date of the Law). However, this has now been postponed.

Scope

A CII is expressly prohibited from transferring information collected within China outside the country unless a separate security assessment has been completed, or if allowed under the applicable laws and administrative regulations.

In order to comply, a CII needs to assess whether (i) all China-sourced personal information and other important data is stored in data centres within China; and (ii) confirm that offshore users do not have system entitlements that allow them to access or review the data stored within China.

The use of cloud computing and global outsourcing of internal functions makes this assessment challenging for multinationals and foreign financial institutions.

The scope of network operators intended to be caught by these measures is broad and catches even those companies that only operate an intranet.

Advice for multinationals

Although the Law only covers activities in connection with an establishment in China (which may be only a small part of its operation), multinationals need to consider whether their overall IT system set-up and any global outsourcing in place complies with the Law.

The Law also imposes an obligation to cooperate with public and State security authorities to investigate suspicious crimes, which may expose multinationals' and foreign financial institutions' network systems to PRC authorities.

It is advisable therefore for a multinational to consider measures to ensure data is properly segregated to avoid inadvertent disclosure to the PRC authorities.

Pending detailed rules for CIIs and data export, it is still difficult to assess the impact of the Law on multinational corporations and financial institutions. Multinationals and financial institutions should be advised to follow developments closely and prepare for the inevitable additional compliance burden.

They should also be ready to take an active part in consultations organised by the PRC regulators on key implementing rules and thus ensure that their voices are heard and opinions properly taken into account.

Contacts

Tiecheng Yang
Partner

T: +86 106535 2265
E: TieCheng.Yang
@CliffordChance.com

Ling Ho
Partner

T: +852 2826 3479
E: Ling.Ho
@CliffordChance.com

Mark Shipman
Partner

T: +852 2825 8992
E: Mark.Shipman
@CliffordChance.com

Yin Ge
Counsel

T: +86 212320 7202
E: Yin.Ge
@CliffordChance.com

Richard Sharpe
Consultant

T: +852 2826 2427
E: Richard.Sharpe
@cliffordchance.com

Lei Shi
Consultant

T: +852 2826 3547
E: Lei.Shi
@CliffordChance.com

Kimi Liu
Associate

T: +86 10 6535 2263
E: Kimi.Liu
@CliffordChance.com

Feifei Yu
Associate

T: +852 2825 8091
E: Feifei.Yu
@CliffordChance.com

Clifford Chance, 27th Floor, Jardine House, One Connaught Place, Hong Kong