



Overview of China's Cybersecurity Law

IT Advisory
KPMG China
—
February 2017

Contents

Cybersecurity Law timeline	4
Challenges arising from the Cybersecurity Law	5
Amendments to the draft Cybersecurity Law	6
Highlights and interpretation of the Cybersecurity Law	7
KPMG China's cybersecurity services	15

Cybersecurity Law timeline

Prior to the enactment of the Cybersecurity Law, China already had some laws, rules and regulations relating to information security, such as *Administrative Measures for Prevention and Treatment of Computer Viruses* and *Administrative Measures for Hierarchical Protection of Information Security*. The Cybersecurity Law, which indicates that China is increasingly focussing on cybersecurity, was adopted by the National People's Congress (NPC) in November 2016 after a year of legislative proceedings, and will come into effect on 1 June 2017.



Challenges arising from the Cybersecurity Law



Key considerations under the Cybersecurity Law

1

Personal information protection

- The Law pays more attention to the protection of personal information and individual privacy
- The Law standardises the collection and usage of personal information
- Enterprises should focus not only on “data security”, but also on “individual privacy protection”, which is of greater significance

2

Security requirements for network operators

- The Law presents clear definitions of network operators and security requirements
- Most of the larger financial institutions may become “network operators”

3

Critical information infrastructure

- The Law places greater demands on the protection of key information infrastructure
- The Law specifies the scope of key information infrastructure

4

Restrictions on the transfer of personal information and business data overseas

- Foreign enterprises and organisations normally need to transfer information outside China
- The Cybersecurity Law stipulates that sensitive data must be stored domestically

5

Penalties

- Penalties for violating the Law are clearly stated, and include the suspension of business activities
- Serious illegal action may lead to the closing of businesses or the revocation of licences
- The maximum fine may reach RMB1,000,000

Amendments to the draft Cybersecurity Law



Comparison between the draft and final versions of the Cybersecurity Law

The table below highlights the significant amendments to the draft Cybersecurity Law that are present in the final version:

Article	Final version	Significant amendment
Article 31	Regarding cybersecurity protection, the state emphasises the protection of critical information infrastructure in <u>public communications and information services, energy, finance, transportation, water conservation, public services and e-governance</u> , as well as other critical information infrastructure that could cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked.	This article clarifies the industries and sectors in which the protection of critical information infrastructure will be given priority.
Article 43	Individuals have the right to require network operators to correct errors in personal information collected or stored by them. <u>Network operators should take measures to remove or correct the errors.</u>	This article gives citizens greater rights to protect their personal information, and increases the network operators' obligation to correct errors in a timely manner.
Article 46	Individuals or organisations <u>are responsible for the use of their networks</u> , and shall not set up websites or communications groups for fraudulent purposes or other illegal activities.	This article emphasises that individuals and organisations bear the responsibility for the use of their networks.
Article 76 (5)	"Personal information" refers to all kinds of information, recorded electronically or through other means, that can determine the identity of natural persons independently or in combination with other information, including, but not limited to, a <u>natural person's</u> name, date of birth, identification number, personal biometric information, address and telephone number.	This article expands the scope of personal information protection from "citizens" to "natural persons".
Article 63	People who violate Article 27 of the Law and engage in activities that endanger cybersecurity may be detained for 5 to 15 days and may be fined <u>RMB100,000 - RMB1,000,000</u> , depending on the severity of the case.	The maximum penalty for violating the Cybersecurity Law has been increased to RMB1,000,000.

Highlights and interpretation of the Cybersecurity Law



Highlights of the Cybersecurity Law

Comprising 79 articles in seven chapters, the Cybersecurity Law contains a number of cybersecurity requirements, including safeguards for national cyberspace sovereignty, protection of critical information infrastructure and data and protection of individual privacy. The Law also specifies the cybersecurity obligations for all parties. Enterprises and related organisations should prioritise the following highlights of the Cybersecurity Law:



Personal information protection

The Cybersecurity Law clearly states requirements for the collection, use and protection of personal information.



Critical information infrastructure

The Cybersecurity Law frequently mentions the protection of “critical information infrastructure”.



Network operators

“Network operators” are the owners and administrators of networks and network service providers. The Cybersecurity Law clarifies operators’ security responsibilities.



Preservation of sensitive information

The Cybersecurity Law requires personal information/important data collected or generated in China to be stored domestically.



Certification of security products

Critical cyber equipment and special cybersecurity products can only be sold or provided after receiving security certifications.



Legal liabilities

Enterprises and organisations that violate the Cybersecurity Law may be fined up to RMB1,000,000.

Interpretation of highlights: Personal information protection

Collection of personal information	Article 22	Network product and service providers that collect users' information are required to inform and obtain consent from the users.
	Article 41	Network operators are required to collect and use personal information in a legal and proper manner.
	Article 44	Individuals and organisations must not steal or use other illegal means to obtain personal information.



KPMG interpretation:

- The articles above emphasise that personal information can only be collected when individuals are informed and agree to the aims and scope of the collection.
- Citizens provide personal information for many purposes, including for education, healthcare, public transportation and online-to-offline transactions. These articles standardise approaches and methods for enterprises and related institutions to obtain personal information.

Collection of personal information	Article 41	Network operators must gather and store personal information in accordance with the Law, administrative regulations and their agreements with users.
	Article 42	Network operators must not disclose, tamper with or destroy collected personal information.
	Article 43	In an instance where a network operator has violated the Law's provisions, individuals have the right to request the operator to delete their personal information.
	Article 45	Departments with legal responsibilities for cybersecurity supervision must ensure that all personal information obtained is kept confidential.



KPMG interpretation:

- The articles above stipulate requirements for the protection of personal information, especially for avoiding disclosure, damage and loss of personal information.
- Amidst a growing focus on telecom fraud and personal information leaks, the Cybersecurity Law introduces stricter requirements on the protection of personal information owned by organisations.
- Accurately identifying personal information owned by organisations, protecting the information using technology and identifying potential information leak risks are becoming key priorities for enterprises.

Interpretation of highlights: Network operators

Definition of “network operators”

Article 76 of the Cybersecurity Law: “Network operators” refers to owners and administrators of networks and network service providers.

Since the applicable scope of “network operators” has expanded significantly, enterprises and institutions that provide services and conduct business activities through networks may also be defined as “network operators”.

In addition to traditional telecom operators and internet firms, network operators may also include:

- Financial institutions that collect citizens’ personal information and provide online services, such as banking institutions, insurance companies, securities companies and foundations.
- Providers of cybersecurity products and services.
- Enterprises that have websites and provide network services.

Overall security requirements	Article 10	When creating and operating networks or providing services through networks, technical and other necessary measures should be taken to safeguard network operations, effectively respond to cybersecurity incidents and to prevent cybercrime. These measures should also maintain the integrity, confidentiality and accessibility of network data, in accordance with the Law’s provisions and national standards.
	Article 21	The state will adopt a tiered system for cybersecurity protection. Network operators are required to follow certain security procedures to safeguard networks from interference, destruction or unauthorised access, and to prevent network data from being leaked, tampered with or stolen.



KPMG interpretation:

The articles above stipulate the overall cybersecurity requirements for network operators. Article 21 introduces the following security requirements:

- **Security administration:** Network operators are required to clarify responsibilities within their organisations, and ensure network security by implementing sound rules and regulations and operational processes.
- **Technology:** Network operators shall adopt various technologies to prevent, combat and investigate cyber-attacks to mitigate network risks.
- **Data security:** Network operators shall ensure data availability and confidentiality by backing up and encrypting data.

Building an effective security administration system, finding rational technical solutions and improving data protection capabilities are expected to be key priorities for network operators.

Interpretation of highlights: Network operators

Detailed cybersecurity requirements

Article 22

Network product or service providers must not set up malicious programmes. Upon discovering a security flaw, vulnerability or other risk in their product or service, network providers must take remedial action immediately, inform users and report the issue to the relevant departments.

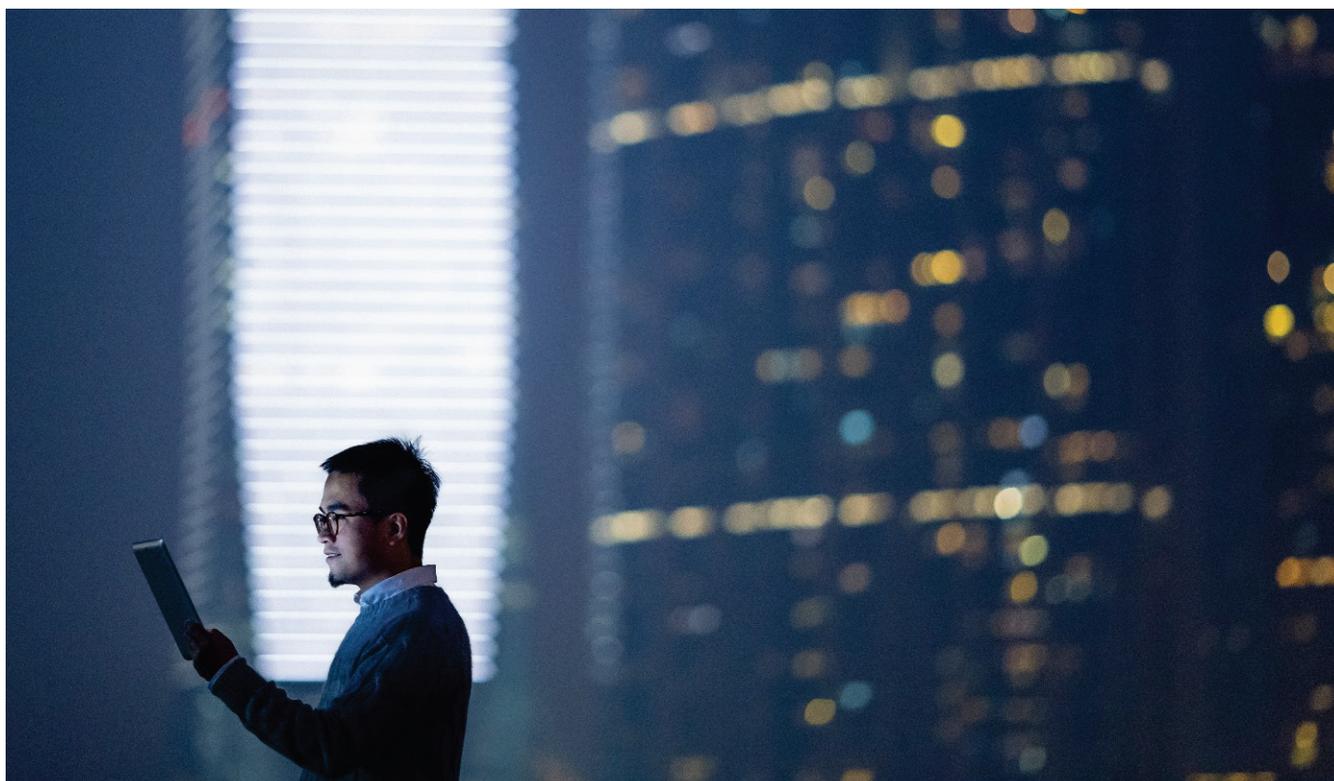
Network product and service providers are required to conduct security maintenance for their products and services. This security maintenance must not be terminated during the period stated in the agreements between parties.



KPMG interpretation:

This article is applicable to cybersecurity product manufacturers, security service suppliers and other organisations that provide services through networks. These network operators are required to respond to security flaws in their products and services and provide security maintenance.

Currently, some network security product and service providers do not respond quickly and effectively to flaws in their products and services, which also impacts security maintenance. This may create cybersecurity risks for users of their products and services.



Interpretation of highlights: Critical information infrastructure

Security of critical information infrastructure	Article 31	Regarding cybersecurity protection, the state emphasises the protection of critical information infrastructure in public communications and information services, energy, finance, transportation, water conservation, public services and e-governance, as well as other critical information infrastructure that may cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked. The State Council will convey the scope and security protection measures for critical information infrastructure.
	Article 38	Critical information infrastructure operators are required to evaluate cybersecurity and other potential risks at least once a year, either on their own or with the help of network security service providers. Operators must report the evaluation results and measures for improvement to the relevant departments responsible for critical information infrastructure protection.



KPMG interpretation:

The Cybersecurity Law mentions that the scope of critical information infrastructure and protection procedures will be defined by the State Council, but the scope has not yet been clarified officially. Enterprises can estimate the scope by considering factors like the number of users, information leak risks, potential implications and the size of data centres.

Enterprises that are qualified to operate critical information infrastructure must regularly assess their cyber risks in accordance with Article 38 of the Cybersecurity Law.



Interpretation of highlights: Preservation of sensitive information

Detailed cybersecurity requirements

Article 37

Personal information and important data collected and generated by critical information infrastructure operators in the PRC must be stored domestically. For information and data that is transferred overseas due to business requirements, a security assessment will be conducted in accordance with measures jointly defined by China's cyberspace administration bodies and the relevant departments under the State Council. Related provisions of other laws and administrative regulations shall apply.



KPMG interpretation:

The article above sets out new requirements on the protection of sensitive information.

- **Potential implications:** Some enterprises need to transmit data to their headquarters, partners and/or suppliers overseas. If these enterprises are qualified to operate critical information infrastructure, they will need to reassess their approach regarding data transfers.
- **Response:** For personal information/important data that is stored overseas, the most direct and effective way is to transfer and store the data locally in China. For personal information/important data that is stored in China but needs to be transferred overseas, the content and approach of the transfer should be adjusted to meet the new requirements.
- **Implementation of the article:** China's cyberspace administrative bodies and other regulatory bodies will introduce policies to clarify the requirements for domestically stored data. At present, there are no official rules and regulations to support the implementation of the article.



Interpretation of highlights: Certification of security products

Detailed cybersecurity requirements	Article 23	Critical network equipment and special cybersecurity products can only be sold or provided after being certified by a qualified establishment, and are in compliance with national standards. China’s cyberspace administrative bodies and the relevant departments under the State Council will draft a catalogue of critical network equipment and special products.
	Article 35	Critical information infrastructure operators that purchase network products and services that might affect national security must pass a national security review.



KPMG interpretation:

The articles above stipulate that providers can only sell their critical network equipment, products or services after receiving security certifications. They may also need to pass a national security review.

The security review/assessment is designed to ensure the security of personal information and support the secure operations of critical information infrastructure described in the Cybersecurity Law.

Providers of network equipment, products or services should actively respond to national security reviews to avoid negative business implications as a result of failing to obtain security certifications.



Interpretation of highlights: Legal liabilities

Detailed cybersecurity requirements	Article 64	Network operators or providers of network products or services that violate Paragraph 3 of Article 22, or Articles 41, 42 and 43 of the Law will be required to correct their actions. They may be issued warnings, have their illegal income confiscated and/or receive a fine of up to 10 times the illegal income amount. If there is no illegal income, the fine could be up to RMB1,000,000. In serious cases, the relevant departments can order the suspension of business operations, shut down websites and revoke business certificates or licences.
	Article 66	Network operators or providers of network products that violate Article 37 of the Law will be ordered by the relevant departments to correct their actions. The departments can issue warnings, confiscate illegal income and impose penalties ranging from RMB50,000 to RMB500,000. They can also suspend business operations, shut down websites and revoke business certificates or licences.



KPMG interpretation:

The article above specifies the penalties that network operators, network product or service providers and operators of critical information infrastructure may face if they violate certain articles of the Cybersecurity Law.

Network operators, network product or service providers and operators of critical information infrastructure should carefully follow the related provisions of the Cybersecurity Law to avoid being penalised.



KPMG China's Cybersecurity services

With many years of experience in cybersecurity advisory services, KPMG has a deep understanding of the cybersecurity landscape in China, as well as the requirements of laws and regulations.

KPMG provides a variety of advisory services based on customer demands. The following four types of services in cybersecurity management are provided by KPMG:





Contacts

Henry Shek

Partner

Tel: +852 2143 8799

henry.shek@kpmg.com

Richard Zhang

Director

Tel: +86 (21) 2212 3637

richard.zhang@kpmg.com

Jason R.K. He

Director

Tel: +86 (755) 2547 1129

jason.rk.he@kpmg.com

Alvin Li

Associate Director

Tel: +852 2978 8233

alvin.li@kpmg.com

Shane Wang

Associate Director

Tel: +86 (21) 2212 3651

shane.wang@kpmg.com

Frank Xiao

Associate Director

Tel: +86 (10) 8508 5456

frank.xiao@kpmg.com

Matrix Chau

Associate Director

Tel: +852 2685 7521

matrix.chau@kpmg.com

kpmg.com/cn

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG Advisory (China) Limited, a wholly foreign owned enterprise in China, is a member firm of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.