China's Cybersecurity Law Draft

Overview of Planned Changes

Cybersecurity Law – Draft

On July 6, 2015, the Standing Committee of the National People's Congress (NPCSC) of the People's Republic of China published a draft on Cybersecurity Law. A public comment period on the Cybersecurity Law was open until August 5, 2015.

As shown, the Cybersecurity Law draft has not yet been finalized. Some significant provisions which are part of the draft show the priorities that govern the promotion of cybersecurity in China. A handful of these provisions point out that the final version could be no less than a fundamental turn-around. The data-localization especially, is an example of China pushing a policy towards saving their citizens data. On the basis of this provision, important data has to be stored within the territory of the People's Republic of China.

Data protection in particular is one of the main topics of the draft, namely tasking internet companies with securing user data more securely.

General Requirements

The intension of the draft is the safeguarding of network security and national security protecting the rights and interests of citizens, legal persons, and other organizations. For this purpose the National Cyberspace Administration is named to be responsible for comprehensive planning, coordinating network security efforts, related supervision, and management efforts.

1. General Security

Under the Cybersecurity Law, network operators are obligated to consider the following security protocols:

a) Internal security management systems and operating rules

b) Determination of persons responsible for network security and implementation of network security protection responsibility

c) Technological measures to prevent computer viruses, network attacks, network intrusions, and other actions endangering network security

d) Technological measures for recording and tracking the status of network operations, for monitoring and recording network security incidents, and for preserving network logs according to regulations;

e) Measures such as data classification, back-up of important data, and encryption

f) Other obligations as provided by law or administrative regulations. After detection of security flaws or leaks providers of network services are encouraged to inform affected users and take remedial measures. At this point, it is not yet clear what is meant by critical network equipment and specialized network security products, which have to be certified by a qualified establishment or meet the requirements of a security inspection. Therefore the State Council is empowered to release a catalog of critical network equipment and specialized network security products.

   Moreover emergency response plans for security incidents have to be prepared so that system leaks, computer viruses, network intrusions, network attacks, and other such network security risks can promptly be uncovered. When network security incidents occur, remedial measure must be taken and incidents must be reported to the relevant departments.

2. Security for Critical Information Infrastructure

The draft defines "Critical Information Infrastructure" to include the following types of systems:

a) Basic networks for public communications and radio and television transmission services
b) Critical information systems for:
   - key industries such as energy, transportation, water conservancy, and finance
   - Public service sectors such as power, utilities, health care, social security, etc.
   - Military networks and government networks; and
   - networks and systems with a "massive number" of users. Personal information of citizens shall be stored within the mainland territory of the People's Republic of China. If storage outside the mainland or transfer abroad is necessary due to business requirements, it is necessary that the person in charge follows the measures formulated by the National Cyberspace Administration to conduct a security assessment. A yearly inspection and assessment of network security report must be sent to the relevant department responsible for critical information infrastructure security.

Bearing in mind the special requirements for protection of critical information infrastructure, the draft enumerates the following measures which may be adopted:

a) Testing and evaluation of security risks to critical information infrastructure
b) Organization of emergency network security drills increasing the responses to network security incidents.
c) Promote network security information sharing among relevant departments, critical information infrastructure operators, network security services institutions, and relevant research institutions.
d) Provide technical support and assistance for network security emergency management and recovery.

Cybersecurity Law (CHN)	Federal Protection Act (GER)
Set up of user information protection systems, strengthening protection of users' personal information, privacy, and commercial secrets	§ 9
Collecting and using citizens' personal information driven by principles of legality, propriety and necessity, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consent of the person whose data is gathered. No gathering of citizens' personal information unrelated to the services they provide; no violation of the provisions of laws, administrative regulations or bilateral agreements to gather or use citizens' personal information. Disclosure of rules for collecting or using citizens' personal information.	§ 4a
Keeping citizens' personal information strictly confidential and do not disclose, distort, damage it, sell, or illegally provide it to others. Adopting technological measures and other necessary to ensure the security of citizen's personal information, and prevent the citizens' personal information from leaking, damage, or loss. In case of information leaks, damage, or loss remedial measures must be immediately taken. Users who might have been affected must be informed, and reports must be made to the competent departments in accordance with regulations.	§ 4a, 9, 42a

The citizens' right to request that the network operators delete their personal information; When discovering that personal information gathered or stored by network operators has errors, they have the right to request that the network operators make corrections.	§ 35
Set up of network information security complaint and reporting system. Publicly disclosing information such as the methods for making complaints or reports, and promptly accepting and handling complaints and reports relevant to network information security.	§ 34

Scope

For the Cybersecurity Law, the following terms have these meanings:

a) "Networks" refers to networks and systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange, and processing.

b) "Network safety" refers to taking necessary measures to prevent attacks, invasion, disturbance, undermining, and unlawful use of networks. Network safety is also responsible for unexpected accidents. This causes the networks to be in a state of stability and reliable operation. It also as well as safeguards the integrity, secrecy and usability of network information storage, transmission, and processing.

c) "Network operators" refers to the owners and administrators of networks. As well as network service providers using networks owned or administrated by others, to provide related services, that include basic telecommunications operators, network information service providers, major information system operators, and other services.

d) "Network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

e) "Citizen's personal data" refers to personal data such as a citizen's name, date of birth, identification card number, personal bio-metric data, profession, residence, or telephone number. It is recorded electronically or by other means. All other kinds of data from which a citizen's identity may be determined, either by itself, or combined with other data are also recorded.

Penalties for Data Protection Violation

Current violation of the Cybersecurity Law can be penalized with a fine of € 7,000 up to € 140,000. The person in charge and other directly responsible personnel are fined between € 700 and € 14,000 However, it is not yet clear if the fine is imposed for a single incident, or as a maximum fine.

Risks of Non-Compliance

Because this law is still in draft form there is no experience on how this draft which uses a broad language will be interpreted. Regulating government agencies will help implement rules by filling in the gaps.

Actions to Consider

These new rules stated in the draft, highlight a recent trend of stronger rules regarding cross-border data transfers. For multinational companies, operating critical information infrastructure in China, it will be more difficult to transfer personal data internationally.
Currently it is not stated whether the personal data of foreign citizens collected in China would be covered by this. It is also unclear if this provision would apply to future collection of personal information, or if data already collected. would also be affected. The procedures for the "security assessment" are unclear. Companies with an interest in doing business in China should monitor the development of these rules before they store data of citizens of these People's Republic of China.

For further infomations

Get in contact with us and together we will evaluate how data privacy will become a main stakeholder in your organisation and your developments to be one step ahead.

GERMANY - EUROPE

legitimis GmbH (Headquarter)
Dellbrücker Str. 116
51469 Bergisch Gladbach
phone: +49 (2202) 289 410
fax: +49 (2202) 289 4147
infomail@legitimis.com
www.legitimis.com

Legitimis®