

BUSINESS SWEDEN



# MARKET INSIGHT CHINA

CYBERSECURITY LEGISLATION

# CYBERSECURITY LEGISLATION

**KNOWN FACTS.** The rapid growth in electronic commerce and electronic payment methods, and technological advances in cloud computing and big data analytics, has given rise to new cybersecurity concerns. The online trade of personal information has also become big business in China, leading to concerns and more stringent rules around the collection, use and storage of personal information.

The **Great Firewall of China** controls external information inflow into China, while the **Cybersecurity Law of the People's Republic of China** (“**Cybersecurity Law**”), which came into force on 1 June 2017, is designed to protect data outflow as well as data residing in China.

The *Cybersecurity Law* is a law covering various aspects of network security. This law was the foundation for the comprehensive cybersecurity regulatory regime in China. *Cybersecurity Law* focuses on the nature and flow of digital information that has been generated in China. It places a strong emphasis on securing personal information and other important data that has been collected in China, and standardizes its collection and usage.

So far, there are a series of specific measures aimed to facilitate the implementation of the *Cybersecurity Law* that have been released, such as:

- *The Measures on the Security Review of Network Products and Services* (for Trial Implementation);
- *National Emergency Response Plan for Cybersecurity Incidents*;
- *Regulation on Graded Protection of Network Security* (seeking opinions).

There are also draft regulations and guidelines on the protection of critical information infrastructure (“CII”) and security assessment of outbound data transfers where relevant authorities are now seeking opinions, including:

- *The draft Regulations on the Security Protection of Critical Information Infrastructure*;
- *The draft Measures for the Security Assessment of Personal Information to be Transmitted Abroad*;
- *The draft Guidelines for the Security Assessment of Cross-border Data Transfer*.

**IMPLICATIONS FOR SWEDISH FIRMS.** To Swedish firms and other international stakeholders, the implementation of the laws in the cybersecurity area will have significant impact on the daily operations.

The comprehensive legislation regime addresses the cybersecurity matters, including monitoring, detection, prevention, mitigation and management of incidents. This may include, for example, data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

## I. INFORMATION & DATA

Critical Information Infrastructure Operators (CIIO, so far no fixed definition of the term) shall store personal information and important data collected and generated in China within mainland China. If transmission of such data out of China is necessary due to business needs, clearance procedures shall be followed according to separate rules formulated by the Cyberspace Administration of China.

Institutions collecting customer information must obtain consent, tell customers about the information’s intended use, notify the Government of breaches and delete or amend personal data on the user’s request. There is restriction on the transfer of personal information and business data overseas – sensitive data must be stored domestically.

## II. VPN

## KEY MESSAGES

China aims to build up a comprehensive legislation regime, by releasing the Cybersecurity Law as a foundation, and followed up a series of measures and rules to facilitate the implementation of the law.

The Cybersecurity Law, designed to protect data outflow, has put a stringent environment in relation to the entities where cyber data is handled, with potential impact on business operations.

Actions shall be taken to adapt the laws, particularly within applications areas such as VPN, cloud services and cross-border data transfer.

New directives have also been released aimed at “clearing up” and regulating the Internet access service market. Telecom businesses will need prior approval before providing VPN services. Businesses using unapproved VPNs could be impacted if the particular VPN they are using is affected by the regulations.

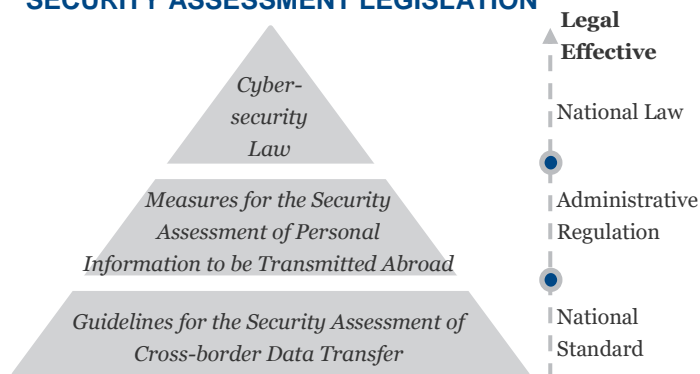
Foreign businesses who need to access cross-border networks can rent VPNs from authorized carriers.

### III. CLOUD SERVICE

Multinational companies may choose either international or domestic Cloud service providers in China. Nevertheless, even if choosing the same Cloud service provider, there will be an isolated account created, which is separated from the global account of the same Cloud service provider, and via its Chinese partner’s service (which is still subject to certain foreign investment restrictions).

Cloud service providers may also need to follow the same draft requirements for security self-assessment and potential audits by regulators as are applicable to network operators when transferring personal information and “important data” across borders.

## PYRAMID OF CROSS-BORDER DATA TRANSFER SECURITY ASSESSMENT LEGISLATION



## LEGISLATION AFFECTING SOME SPECIFIC SECTORS

- In terms of import/export controls of encryption software and hardware, pursuant to the *Regulation on the Administration of Commercial Cipher Codes* of China, import of encryption products and equipment with encryption technology or export of commercial encryption products shall be approved by the national encryption administrations. Any sale of foreign encryption products by an entity or individual is prohibited.
- The *Provisional Rules on Management of the Individual Credit Information Database* is promulgated by the People’s Bank of China to ensure the secure and legitimate use of personal credit information.
- Pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or Internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

## CONTACTS

**MAIL:** ask.china@business-sweden.se

**WEB:** business-sweden.se/china

**LINKED IN:** business sweden asia-pacific

Published: December 13, 2019

## KEY RECOMMENDATIONS

Swedish companies are recommended to assess and address the areas impacted by cybersecurity legislation, particularly within cross-border data transfer.

### Concrete actions recommended are:

- Companies with centralized CRM, HR, Procurement or other critical business systems will need a strategy for dealing with the data that flows to these central hubs. An option is to build local data centers or moving to cloud-based services hosted in China-based data centers.
- Companies need to start monitoring the information in their networks for restricted content. All text, audio and video content have to be screened, illegal content must then be removed, and the actions should be recorded and reported.
- For companies using VPN service, make sure the provider of your VPN is licensed in China.
- It is required to regulate the use of certified network products and services. Specialized equipment, products and services designed to ensure network security (such as routers, switches and servers) must adhere to compulsory government standards in order to be used in China.

**For help with assessing your readiness level and defining required measures, do not hesitate to contact us!**



We help Swedish companies grow global sales and international companies invest and expand in Sweden.

**BUSINESS SWEDEN in Beijing**

609, 6F, CYTS Plaza, No. 5 Dongzhimen Nandajie, 100007 Beijing, China  
T +86 10 5815 6006 F +86 10 5815 6223

**BUSINESS SWEDEN in Shanghai**

12F, Sail Tower, 266, Hankou Road, 200001 Shanghai, China  
T +86 21 6218 9955 F +86 21 6217 5152

**BUSINESS SWEDEN Box 240, SE-101 24 Stockholm, Sweden**

World Trade Center, Klarabergsviadukten 70

T +46 8 588 660 00 F +46 8 588 661 90

info@business-sweden.se [www.business-sweden.se](http://www.business-sweden.se)

