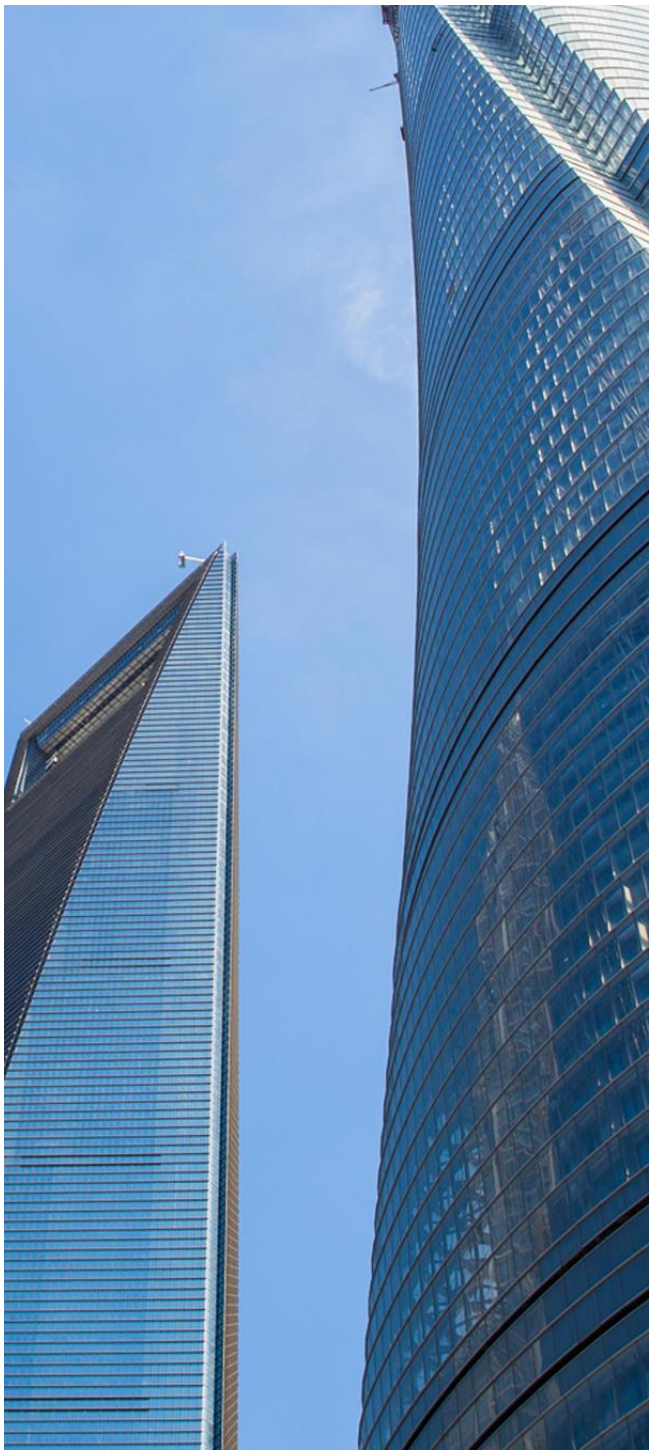
CUATRECASAS

China offices

Legal flash

June 2019

This issue covers legislation published in May 2019



Index

Draft Measures on Administration of Data Security released for public comment (《数据安全管理办法（征求意见稿）》发布)

On May 28, 2019, the Cyberspace Administration of China ("CAC") released the Draft Measures on Administration of Data Security (the "Data Security Draft") for public comment. The Data Security Draft sets out obligations for network operators carrying out data activities, particularly those involving the collection of personal information and important data.

The Data Security Draft is based on the Cyber Security Law and includes requirements already provided under the Information Security Technology – Personal Information Security Specification (GB/T 35273-2017). Although it is not legally binding, the latter is a national standard for personal information protection and has been extensively applied by administrative agencies and industries concerned.

Under the Data Security Draft, data compliance requirements mainly affect network operators that carry out data activities, namely owners, network administrators, and network service providers.

Requirements imposed on network operators:

- Data collection

  Network operators must develop and publish their rules for collection and use, and obtain the data subjects' consent before collecting and using personal information. The rules for personal information collection can be included in the privacy policies of websites, apps and other products, provided they are summarized and clearly visible.

  The rules for data collection and use must be clear, specific simple, plain and easy to access, and they must include information such as (i) the name and contact details of the person responsible for the network and the person in charge of data protection; (ii) the purposes, frequency, methods and scope of the data collected; (iii) how data subjects can withdraw their consent and delete personal information; and, if applicable, (iv) the practices adopted if personal information is transferred to third parties.

Network operators are prohibited from forcing or misleading data subjects to consent to the collection of their personal information by means of using pre-checked authorization or bundled functions.

Network operators may not discriminate against data subjects that do not fully authorize the collection of personal information in terms such as service quality and price difference.

To collect the personal information of anyone under the age of 14, network operators must obtain consent from the minor's guardian.

Data processing and usage

Network operators must respect the data retention period specified in the rules for collection. Also, unless it is anonymized, network operators must promptly delete any personal information related to a data subject's account once it has been closed.

Network operators must respond within a reasonable time to any requests from data subjects regarding data access, correction and deletion and the closure of an account.

If network operators combine user data and algorithms to generate personalized recommendations, they must clearly mark the information with the words "targeted push" and provide users with an opt-out mechanism. If users choose to opt out of targeted advertising, network operators must stop the "targeted push" and delete any user data and personal information collected, including device ID.

Before sharing collected personal information with third parties, network operators must assess the potential security risks and obtain the data subjects' consent, unless:

- the data is collected from legal public sources without overriding the data subject's wishes;
- data subject has voluntarily disclosed this data;
- the data has been anonymized;
- sharing the data is required by a law enforcement authority to perform its functions and duties in accordance with the law;

- sharing the data is required to safeguard national security, public interest or data subjects' lives.

Before publishing, sharing, selling or making a crossborder transfer of important data, network operators are required to conduct a security risk assessment and request approval from the competent authorities.

The Data Security Draft establishes the supervision obligation of a network operator that enables third-party applications to collect data through its platforms. Also, the network operator may be liable for any data incidents caused by the third-party applications.

Data security administration

› Filing requirements

The Data Security Draft requires network operators to report their data protection practices to the local CAC if they collect important data or sensitive personal information for "operational purposes."
However, there is no express definition of "sensitive personal information" or "operational purposes" under the Data Security Draft. The filing information must include the rules for collection and use, purposes, volume, methods, scope, types and duration of the collection and use of data.

› Personnel responsible for data security

If network operators collect important data or sensitive personal information for operational purposes, they are also required to designate a person in charge of data security, who must have management experience and data security expertise, and must participate in the important decision-making processes for data activities. The functions and duties of the person in charge of data security include:

- coordinating the development and implementation of an internal data protection plan;

- coordinating the data security risk assessment and ensuring the removal of data security threats;

- reporting data protection issues and incident responses to the competent authorities; and

- accepting and handling data subject complaints.

› Notification and report

If a data security incident involves leakage, damage or loss of personal information, or the risk of a security threat increases, network operators must adopt immediate remedial measures and promptly notify the affected data subjects by telephone, SMS, email or mail. They must also report the situation to the competent authorities.

› Penalties

Disciplinary actions against network operators that fail to comply with the obligations provided under the Data Security Draft include public exposure, confiscating illegal income, suspending business operations, suspending business for rectification, shutting down a website and revoking relevant business permits or the business license.

We will provide an update when the final version is released.

Date of issue: May 28, 2019. Deadline for comments: June 28, 2019

Draft Measures on Cybersecurity Review released for public comment (《网络安全审查办法（征求意见稿）》发布)

On May 24, 2019, the CAC released the Draft Measures on Cybersecurity Review (the "Cybersecurity Review Draft") for public comment. Once finalized, they will replace the Measures for Security Review of Network Products and Services (for Trial Implementation) to implement the cybersecurity review regime provided under article 35 of the Cybersecurity Law.

Highlights

› In line with article 35 of the Cybersecurity Law, under the Cybersecurity Review Draft, "the procurement of network products and services by critical information

infrastructures ("CII") operators that may affect national security" will be subject to cybersecurity review.

- The Cybersecurity Review Draft requires all CII operators to conduct a pre-assessment of potential security risks and prepare a security risk report before purchasing any network product and service. CII operators are obliged to report to the corresponding cybersecurity review office if, based on their pre-assessment, using a product or service may result in:
  - complete shutdown of CII or failure of their main functions;
  - a large volume of personal information or important data being leaked, lost, destroyed or transferred outside Chinese territory;
  - a supply chain security threat that could jeopardize the operation, maintenance, technical support or upgrading of CII; or
  - other potential risks seriously threating the safety of CII.
- For CII operators to procure a product or service subject to cybersecurity review, they must ensure that (i) the product or service provider is bound by contract or other means to cooperate with the review, and (ii) this contract is contingent on the product or service clearing the cybersecurity review.
- The reviewing authority will assess the national security risks associated with the procurement, focusing on the following factors:
  - Impact on the continuity, security and stability of CII operation.
  - The possibility that a large volume of personal information or important data may be leaked, lost, destroyed or transferred outside Chinese territory.
  - Controllability, transparency and supply chain security of network products and services.
  - Impact on technology and industries related to national defense, the military industry and CII.
  - The product or service provider's compliance with PRC laws and regulations, and their commitment to responsibilities and obligations.

- Financing or control over the provider by a foreign government.
- Other factors that could jeopardize national and CII security.

› Moreover, the Cybersecurity Review Draft also stipulates the authorities, working mechanism, document requirements and procedure of the cybersecurity review.

Network product and service providers that sell to Chinese CII operators must pay close attention to the potential regulatory change.

Date of issue: May 24, 2019. Deadline for comments: June 24, 2019

Three new national standards released for Cybersecurity Classified Protection V2.0 (网络安全等级保护2.0时代三个新国家标准颁布)

On May 13, the State Administration for Market Regulation and the National Standardization Administration Commission jointly issued three national standards for implementation of the cybersecurity classified protection system, which will take effect from December 1, 2019.

The cybersecurity classified protection system is based on article 21 of the Cybersecurity Law, under which network operators are required to fulfill certain security obligations based on the risk level associated with their network. The future Regulations on Classified Protection of Cybersecurity are expected to give detailed guidelines on its implementation.

Although most existing and new national standards on classified protection of cybersecurity are intended as recommendations rather than rules, they are critical to the interpretation and implementation of the cybersecurity classified protection system and are expected to be widely adopted by the relevant industries and government agencies.

The major changes of these standards are the specifications under the Baseline for Classified Protection of Cybersecurity, which specify the general security requirements and extended security requirements for level 1-4 objects and particularly cover the emerging technologies such as cloud computing, big data, IoT, mobile internet and industrial control system.

The three new national standards are:

- GB/T 222239-2019 Information Security Technology – Baseline for Classified Protection of Cybersecurity
- GB/T 25070-2019 Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity
- GB/T 28448-2019 Information Security Technology – Evaluation Requirements for Classified Protection of Cybersecurity

The new standards, along with other regulations and national standards to be issued at a later date, will make up the "Cybersecurity Classified Protection System V2.0."

Announcement released expanding scope of accelerated depreciation of fixed assets to all manufacturing sectors

On May 23, 2019, the Ministry of Finance and the State Administration of Taxation jointly released the announcement on Expanding the Applicable Scope of the Preferential Policy for Accelerated Depreciation of Fixed Assets, Announcement [2019] No. 66).

According to the Announcement, since January 2019, the accelerated depreciation introduced for certain encouraged manufacturing sectors in 2014 (by Cai Shui [2014] No. 75), and expanded in 2015 (by Cai Shui [2015] No. 106), has been extended to all manufacturing sectors.

Eligible taxpayers may now choose between:

- reducing the depreciation period for newly purchased fixed assets by up to 40% ("the minimum depreciation years must not be less than 60% of the depreciation years"); or
- applying the double declining balance method or sum-of-the year's digits method (accelerated methods).

For these reasons, the State Bureau of Statistics has defined the manufacturing sector as a whole.

Date of issue: April 23, 2019. Effective date: January 1, 2019

Announcement released clarifying enterprise income tax treatment of perpetual bonds

On April 16, 2019, the Ministry of Finance and the State Taxation Administration jointly released the announcement on issues concerning Enterprise Income Tax Policies for Perpetual Bonds, Announcement [2019] No. 64 ("Announcement 64").

Before Announcement 64, the tax treatment applicable to perpetual bonds was unclear, because the Enterprise Income Tax Law does not define them as equity or debt.

Announcement 64 provides two methods (the issuer and the investor must apply the same method):

- Method 1: Consider perpetual bonds an equity tool

  Issuer: interest paid is not deductible for tax purposes.
  Investor: income obtained is exempt for tax purposes because the income is considered a dividend.

- Consider perpetual bonds a debt tool

  Issuer: interest paid is deductible for tax purposes.
  Investor: income obtained is subject to and not exempt from tax.

Announcement 64:

(i) does not clarify the tax treatment applicable to non-resident investors;

(ii) provides conditions for determining the nature of a perpetual bond that are different from those established in the Value Added Tax Law; and

(iii) only applies to perpetual bonds approved by the National Development and Reform Commission, the People's Bank of China, the Bank of China Insurance Regulatory Commission, the China Securities Regulatory Commission, or those registered by the China Association of Banking Market Dealers, China.

Date of issue: April 4, 2019. Effective date: January 1, 2019

Contact

Omar Puertas

Partner
omar.puertas@cuatrecasas.com

Cuatrecasas
Shanghai office

20 F Shui On Plaza,
333 Huai Hai Middle Road
Shanghai 200021, PRC
+86 21 2327 7000
+86 21 2327 7007
shanghai@cuatrecasas.com

Pablo Cubel

Partner
pablo.cubel@cuatrecasas.com

Cuatrecasas
Beijing office

15/F Parkview Green, Tower B,
9 Dong Da Qiao Road
Beijing 10002, PRC
+86 10 5651 0200
+86 10 5651 0268
beijing@cuatrecasas.com