Updates
July 17, 2019

# Introduction and Comments on Measures for Data Security Management in China

The Cyberspace Administration of China (i.e., the Office of the Central Cyberspace Affairs of China) promulgated the draft *Measures for Data Security Management* (the Measures) for public comment on May 28. The Measures focus on the data collection, data processing and use, data security supervision, and management of personal information and important data by "network operators." The definition of what constitutes a "network operator" is very broad. Simply speaking, the term covers all companies who own and manage websites and provide services through the internet (according to the definition given in the Cybersecurity Law of China).

The Measures, together with other draft measures that the Office recently issued for public comments, such as the *Measures for Network Security Review*, the *Regulations for the Network Protection of Children's Personal Information* and the *Measures for Safety Assessment on Cross-Border Transfer of Personal Information*, will likely be the supporting documents of the *Network Security Law*. This update provides an introduction and summary of the main content of the Measures.

## Main Contents of the Measures

### Application

These measures will apply to the collection, storage, transmission, process and use of data, as well as the protection, supervision and administration of cybersecurity in China. (Article 2)

### Responsible Authority

The responsible authority structure includes the Central Cyberspace Affairs Commission as leader, the state cyberspace administrative organizations as overall coordinator and supervisor, and the municipal cyberspace administrative organs as the local responsible authority. (Article 5)

### Network Operator's Obligations in Data Security

1. Perform data security protection obligations in accordance with relevant laws and administrative regulations and by reference to national cybersecurity standards;
2. Establish the accountability of data security management and evaluation systems;
3. Formulate data security plans;
4. Implement data protection technical measures;
5. Carry out data security risk assessments;
6. Develop emergency response plans;
7. Timely deal with security incidents; and
8. Organize data security education and training. (Article 6)

### Rules for Data Collection and Use

The rules for data collection and use can be included in the privacy policy (Article 7) and should be specific and easy to understand/access. The following items should be included (Article 8):

1. General information about the network operator;
2. The name and contact information of the network operator's main responsible person, as well as the person responsible for the data security;
3. The purposes, types, volume, frequency, methods and scope of the personal information to be collected and used;
4. The place of storage, retention period and what the network operator will do with personal data after the retention period expires;
5. The rules to be followed when providing personal information to others (if the information will be provided to others);
6. How the network operator protects the security of personal information and other relevant information;
7. The ways and methods for the data subject to withdraw consent and to access, correct and delete personal information; and
8. Channels and methods for making complaints and reports.

**Requirements for Special Cases in Data Collection and Use**

1. **Targeted Push Information:** (A) Network operators shall not, through authorization by default, bundling functions or other means, force or mislead data subjects to consent to the collection of personal information. (Article 11) (B) Network operators shall, when using user data and algorithms to push news and commercial advertisements, prominently use the label "targeted push," and provide an option for users to stop receiving the targeted push contents. (C) If the user chooses not to receive targeted push information, network operators shall stop the push and erase the device identification code and other collected user data as well as any personal information. (D) Network operators shall, when conducting targeted push activities, comply with laws and regulations, respect social morality and business ethics, abide by public order and good morals, and be honest and diligent. All discriminatory and fraudulent acts shall be prohibited. (Article 23)
2. **Collection of Important Data or Sensitive Personal Information for Business Operation Purposes:** (A) Network operators shall make a filing with the local cybersecurity administration. The filing shall include the rules for collection and use of such data, the purpose, volume, method, scope, type and retention period of the data, excluding the content of data itself. (Article 15) (B) Network operators shall appoint the person responsible for data security. The person responsible for data security shall be selected from among personnel who have relevant management work experience and professional knowledge of data protection, participate in important decisions of relevant data activities and report work directly to the main responsible person of the network operators. (Article 17)
3. **Crawler**[1]: (A) Network operators shall not interfere with the normal operation of their websites. (B) If such acts seriously affect the operation of websites (e.g., if the traffic of automatic visits or data collection exceeds one-third of the average traffic of the website) and the website requests the network operator to cease such automatic access and collection, the network operator shall cease such practice. (Article 16)
4. **Automatic Synthesized Information:** (A) Network operators shall, when using big data, artificial intelligence or other technologies to automatically synthesize information such as news, blogs and comments, prominently use the label "synthesis." (B) Network operators shall not automatically synthesize information for the purposes of making profits or damaging the interests of any other person. (Article 24)

**Access, Correct and Delete Personal Information**

1. The retention of personal information by the network operator shall not exceed the retention period provided in the rules for collection and use.
2. Personal data shall be deleted in a timely manner after the users close their accounts, unless the personal information has been processed to make it impossible to identify a specific person from the information and such information cannot be processed to re-identify such a person (hereinafter referred to as "anonymization"). (Article 20)
3. Network operators shall, upon receipt of requests to access, correct and delete personal information and close accounts, fulfill such requests within a reasonable time and at reasonable cost. (Article 21)

**Cross-Border Transfer of Important Data**

Network operators shall assess potential security risks before publishing, sharing or selling important data or transferring such data across borders, and report to the competent regulatory department for approval. (Article 28)

**Obligations Between Network Operator and Third-Party App Operator**

1. Network operators shall specify data security requirements and responsibilities for third-party apps connected to platforms and supervise third-party app operators to strengthen data security management.
2. If data security incidents occur due to third-party apps and cause damage to users, network operators shall assume all or part of the liability unless they are able to prove that they are not at fault. (Article 30)

**Supervision and Regulation Methods**

The following actions will be taken if there are violations of the law:

1. Summon the main responsible person of the network operator and urge them to rectify the violation. (Article 33)
2. Notify the public.
3. Take disciplinary actions, such as confiscating the violator's illegal income, suspending relevant business operation, ceasing business operation for rectification, shutting down the website, revoking the relevant business permit or business license or other punishments as the case may be.
4. If the violation constitutes a crime, the violator will be subject to criminal liability in accordance with the law. (Article 37)

**Unclear Issues**

There are ongoing discussions among companies about several unclear issues presented in the draft Measures. Below we outline a few of those concerns.

**Network Security Responsible Person and Data Security Responsible Person**

In the Cybersecurity Law, it is required that a network security responsible person should be appointed. In the Measures, it is required that a data security responsible person should be appointed. We understand these two responsible persons should be the same person, but this needs to be clarified. (Article 17)

**Official Security Assessment**

In the Cybersecurity Law, official security assessment/approval is merely applied to the Key Information Infrastructure Operator (KIIO), but in the Measures, it seems to be applied to all network operators whenever important data is published, shared, transacted and transferred. There is no other type of assessments (e.g., self-assessment) mentioned in the Measures, and it should be clarified. (Article 28)

**Several Definitions Need Clarification**

The following are three definitions we identified that need further clarification:

1. "Network Data" is defined in Article 38, but "Data" is used in the Measures.
2. "Important Data" is defined as excluding information related to the production and operation of enterprises, internal management information and personal information, which might need more clarification.
3. "Sensitive Personal Information" mentioned in Article 15 has no definition in Article 38.

We advise companies to pay close attention to the public comments on the draft Measures and the final version once it is released.

**Endnote**

[1] In this case, crawler means a computer program that gathers and categorizes information on the internet.

This update has also been published in the February-March 2020, Vol. 6 No. 2 issue of *Pratt's Privacy & Cybersecurity Law Report*.



## Authors

**Xinlan Liu**

Business Professional
XLiu@perkinscoie.com 86.10.5971.9369

## Explore more in

Corporate Law Privacy & Security

**Related insights**

Update

## A Greener Holiday Future: California Establishes Nation’s First Apparel and Textile Article EPR Program

Update

## FERC Meeting Agenda Summaries for October 2024