PILLAR LEGAL

China to Require Government Approval to Transfer User Data Overseas

CHINA REGULATION WATCH[1]
April 14, 2017

By: Greg Pilarowski | Lu Yue

On April 11, 2017, the Cyberspace Administration of China, also known as the State Internet Information Office (国家互联网信息办公室) (the "CAC")[2], released for public comment a draft of the Measures for Security Assessment of Transferring Personal Information and Critical Data Overseas (个人信息和重要数据出境安全评估办法) (the "Overseas Data Transfer Draft").

The main purpose of the Overseas Data Transfer Draft is to require companies, organizations and individuals in China to apply for permission, under certain circumstances, to transmit personal information and critical data ("Digital Data") out of the country. The draft rules would require two different types of security assessments in connection with overseas transfers of Digital Data: (i) self-assessments conducted by the companies, individuals and organizations planning to transfer the Digital Data overseas, and (ii) assessments conducted by the respective primary industry regulators charged with supervising the operation of those companies, individuals and organizations (the "Primary Regulators").

The public comment period with respect to the Overseas Data Transfer Draft will end on May 11, 2017. Although the Overseas Data Transfer Draft is not a final rule, the content of the draft is a clear indication of the direction in which CAC intends to move with respect to China's data security rules.

1. Who Will Be Regulated?

If the Overseas Data Transfer Draft is adopted in its current form, the CAC would require all "internet operators" to apply for permission to transfer Digital Data out of China. In the draft document, internet operator is defined in very broad terms, capturing "all network owners, network managers, and internet service providers".[3] We understand this broad language to include all companies, individuals and organizations that collect Digital Data through the internet.

This is not the first time that regulators in China have proposed or adopted restrictions on cross-border data transfers. China's Cyber Security Law, which was approved by the National People's

---

[1] This China Regulation Watch is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This China Regulation Watch may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-474-3258 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: greg@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Since being established in May 2011, CAC has exercised widespread censorship control over the internet.

[3] See Section 2, Section 17 of the Overseas Data Transfer Draft.

Congress Standing Committee (全国人民代表大会常务委员会) on November 7, 2016 (the "Cyber Security Law"), requires internet operators who operate critical information infrastructure to store the personal information and critical data within China. If this select group of internet operators want to transfer Digital Data overseas, they must submit an application to their Primary Regulator to determine whether or not the relevant Digital Data will be permitted to be transferred out of China.[4] The Overseas Data Transfer Draft broadens this security assessment requirement to all "internet operators", as opposed to just "internet operators of critical information infrastructure", which was the scope under the Cyber Security Law.

2. Definition of Personal Information and Critical Data

Personal Information and Critical Data, as used in the Overseas Data Transfer Draft, are defined as set forth below.

- Personal Information. "Personal Information" means all information that can be used on its own or together with other information to determine the identity of a natural person, including an individual's name, date of birth, identification card number, biometric data, address, and telephone number.[5]

- Critical Data. "Critical Data" means data which is very closely related to China's national security, economic development or societal public interests. Because this definition is very broad and general, CAC indicated that other government departments will further elaborate the scope of Critical Data through future detailed standards and instructions.[6]

3. Prior Consent of Users Required

Pursuant to the Overseas Data Transfer Draft, if user Personal Information is transferred overseas, the internet operators transferring the data must clearly explain to users the purpose of collecting such information, the scope of the Personal Information collected and the countries or regions where the intended recipients of such information are located (the "Data Recipients"). In addition, without the prior consent of a user, an internet operator must not transfer such user's Personal Information overseas. If the Personal Information of a child is to be transferred overseas, the prior consent of the child's guardian must be obtained.[7] The Overseas Data Transfer Draft does not include any specific requirements about how the relevant consent should be obtained, with no discussion of whether an "opt out" approach is sufficient or whether an "opt in" approach is required.

[4] See Section 37 of the Cyber Security Law.
[5] See Section 17 of the Overseas Data Transfer Draft.
[6] See Section 17 of the Overseas Data Transfer Draft.
[7] See Section 4 of the Overseas Data Transfer Draft.

4. Security Self-Assessment Requirement

Pursuant to the Overseas Data Transfer Draft, prior to transfer of any Digital Data out of the country, internet operators must conduct a security self-evaluation assessing the following elements:

- Necessity. The necessity of transferring the Digital Data out of China.

- Personal Information. Quantity, scope, type and level of sensitivity of the Personal Information, and whether or not users' prior consent for the overseas transfer of the Digital Data has been obtained.

- Critical Data. Quantity, scope, type and level of sensitivity of the Critical Data.

- Digital Recipients. The capability of the Digital Recipients with respect to adopting security measures to protect the Digital Data they will receive, and the internet security of the countries or regions where the Digital Recipients are located.

- Digital Information Risk. The risk of leakage, damage, falsification and misuse of the Digital Data after it is transferred abroad and re-transferred to other destinations around the world.

- Adverse Impacts. The likelihood of any adverse impact on China's national security, public interests and individual legitimate interests as a result of the Digital Data being transferred overseas.[8]

Internet operators must conduct a self-evaluation at least once per year, and promptly report the results to their Primary Regulator. In the event that (i) the Digital Recipients change, (ii) the purpose, scope, quantity and type of Digital Data to be transfer overseas changes substantially, or (iii) there are any major data security incidents, the internet operator's self-evaluation shall be updated accordingly.[9]

5. Primary Regulator Security Assessment

Pursuant to the Overseas Data Transfer Draft, under any of the situations described below, an internet operator must submit an application to their Primary Regulator for a security assessment with respect to the proposed overseas transfer of Digital Data:

- The Digital Data includes the Personal Information of more than 500,000 persons, irrespective of whether this threshold is met with respect to a single transfer or on an accumulated basis through multiple transfers.

[8] See Section 8 of the Overseas Data Transfer Draft.
[9] See Section 12 of the Overseas Data Transfer Draft.

- The storage size of the Digital Data exceeds 1,000 gigabytes.

- The Digital Data includes information related to nuclear facilities, chemical biology, national defense, military, human health, large-scale construction projects, marine environment or geographic information about sensitive locations.

- The Digital Data includes information relating to system loopholes or security protection measures for critical information infrastructure.

- The Digital Data originates from Internet Operators who operate critical information infrastructure.

- The Digital Data has the potential to affect national security or societal public interests, and the Primary Regulators believe it is necessary to conduct a security assessment with respect to such Digital Data.[10]

Pursuant to the Overseas Data Transfer Draft, the Primary Regulators shall complete the assessment and report the results to the applicants and the CAC within sixty (60) days after receipt from an internet operator of an application to transfer Digital Data overseas.[11]

[10] See Section 9 of the Overseas Data Transfer Draft.
[11] See Section 10 of the Overseas Data Transfer Draft.