DEACONS
的近律師行

Corporate Commercial Client Alert

China Trade & Investment

11 November 2021

China's New Draft Guidance of Security Assessment for Outbound Data Transfers

Edwarde Webre and Joyce Mu

From 29 October to 28 November 2021, the Cyberspace Administration of China (CAC) is seeking public comments on the Measures for the Security Assessment of Outbound Data (Draft). This third draft has been formulated on the basis of China's Cybersecurity Law (CSL), Data Security Law (DSL, effective as of 1 September 2021) and Personal Information Protection Law (PIPL, effective as of 1 November 2021), whereas the previous two drafts circulated in 2017 and 2019 were primarily based on the CSL. It is expected that this Draft will be enacted soon and probably take effect in early 2022.

Scope of application

The Draft intends to regulate the outbound transfer of (including cross-border assess to) important data and/or personal information (PI) collected/generated in domestic operations within China. Thus it shall not be applicable to offshore/overseas entities directly collecting personal information from individuals in China. For clarity, "offshore/overseas" herein shall include Hong Kong, Macau and Taiwan, in addition to the foreign countries (regions).

There is no unified definition of important data under the current legislation in China. The DSL has delegated authority to the local governments and various government departments to make specific catalogues of important data for their respective regions and for relevant industries and fields. For instance, the CAC, the NDRC (National Development and Reform Commission), the MIIT (Ministry of Industry and Information Technology), the MPS (Ministry of Public Security) and the MOT (Ministry of Transport) jointly issued the Several Provisions on Automotive Data Security Management (for Trial Implementation), which became effective on 1 October 2021, to define the important data (involved in the design, manufacturing, sales, use, operation and maintenance of automobiles) as the data that may endanger national security, public interests or the legitimate rights and interests of individuals or organisations once they are tampered with, damaged, disclosed, illegally obtained or illegally used, and elaborates on the specific types of the same.

The security assessment requirement was initially introduced in the CSL against the critical information infrastructure (CII) operators only. Now the Draft has extended the security assessment obligation to all data processors, and provides two types of security assessment to be undertaken before providing data from China to overseas.

I. Risk self-assessment; and

II. Security assessment by CAC.

Risk self-assessment

All data processors shall conduct a risk self-assessment before providing any data abroad (which may include offshore mirror / remote access, intra-group sharing staff information, outbound transfer of personal information after de-identification etc.). The term "data processor" is not defined in the Draft or current legislation in China. By reference of the DSL, the term "Data" refers to any recording of information by electronic or other means; and "Data Processing" includes the collection, storage, use, processing, transmission, availability and disclosure of data, etc. Accordingly, the outbound data concerned could be any type of data including but not limited to the personal information, non-personal information, and a company's business data.

The risk self-assessment shall focus on:

1) The legality, justifiability, necessity of the outbound data transfer and the purpose, scope and method of the overseas recipient's data processing;

2) The quantity, scope, type and sensitivity of the outbound data; risks to national security, public interests and the legitimate rights and interests of individuals or organisations that may arise from the outbound data transfer;

3) Whether the management, technical measures and capabilities of the data processor in the data transfer link can prevent data leakage, damage and other risks;

4) The responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management, technical measures and ability to perform the responsibilities and obligations can ensure the security of the outbound data;

5) Risks of leakage, damage, tampering and abuse of data after the data is transmitted abroad and further transferred, and whether the channels for individuals to maintain their rights and interests in personal information are unblocked; and

6) Whether the relevant contract(s) for the outbound data concluded with the overseas recipient(s) fully specifies the responsibilities and obligations for data security protection.

Note that the contract(s) between a data processor and overseas recipient(s) in item (6) above does not need to be the standard form formulated by the CAC as mentioned in the PIPL, however shall include but not be limited to the following:

a) The purpose and method of transmitting the data abroad and the scope of the outbound data; and the purpose and method of data processing by the overseas recipient;

b) The place and duration of overseas storage of the data, as well as the measures to deal with the data after the storage period expires, the purpose agreed upon is completed or the contract is terminated;

c) restrictive clauses restricting the overseas recipient from re-transferring the data transmitted abroad to other organisations or individuals;

d) Security measures that shall be taken in case of any substantial change in the actual control right or business scope of the overseas recipient, or any change in the legal environment of the country or region where the overseas recipient is located, which makes it difficult to guarantee data security;

e) Liability for breach of the data security protection obligation, and binding and enforceable dispute resolution clauses; and

f) Properly carrying out emergency response in case of data leakage and other risks and ensuring the smooth channels for individuals to safeguard their personal information rights and interests.

Security assessment

The security assessment by CAC will be triggered in any of the following circumstances:

i. the outbound data contains important data, regardless of whether the data processor is a CII operator;

ii. the outbound data contains personal information collected and generated by CII operators;

iii. the outbound personal information is provided by a PI Processor (as defined in the PIPL) having processed PI of more than 1 million people; or

iv. the outbound personal information is provided by a data processor having provided to overseas the PI of more than 100,000 people or Sensitive PI of more than 10,000 people accumulatively.

To apply for the security assessment, the risk self-assessment report and contact(s) between the applicant/data processor and overseas recipient(s), among others, shall be submitted to the CAC. Within 7 working days from the receipt of an application for security assessment, the CAC shall confirm in writing if the application is acceptable. In the subsequent 45-60 working days, the CAC shall complete the security assessment, and inform the applicant in writing of the assessment result which shall be valid for 2 years. For continuous outbound transfer of data, application for assessment shall be made again no later than 60 working dates prior to the expiration of the prior assessment. During the 2-year valid period, reassessment shall be required if:

(i) there is any change to the purpose, method, scope or type of outbound data, or to the usage or method of data processing by the overseas recipient;

(ii) the period for overseas storage of PI and important data is extended;

(iii) there is any change that may affect the security of the outbound data such as in the legal environment of the country or region where the overseas recipient is located, or in the actual control of the data processor or the overseas recipient, or in the contract between the data processor and the overseas recipient.

Data outbound activities shall cease if the reassessment has not been done as legally required. Where the CAC finds that any outbound data which has passed the assessment no longer meets the security management requirements in the actual process, it shall revoke the assessment result and notify the data processor in writing of the same. The data processor concerned shall then terminate the outbound data activities before making rectification and passing the reassessment.

Any entity or individual who is aware of that any data processor provides data abroad without an assessment may report or complain to the CAC office at provincial level or above.

Sanctions

The Draft does not provide specific sanctions against the violation, and simply refers to relevant penalties under the CSL, DSL and PIPL, which means that penalty up to RMB50 million (or 5% of turnover in the preceding year whichever is higher) may be imposed for illegal outbound transfer of personal information, and/or penalty up to RMB 10 million may be imposed for illegal outbound transfer of important data, as the case may be.

Suggestions

It is advisable for the subsidiaries of multinationals to review the type and quantity of its outbound data, and take actions necessary for legally transfer data abroad from China, for instance:

- Communicating with offshore office(s) and commercial partners on the scope, type and volume of outbound data allowed under the China law;
- Improving the system and mechanism on local backup, classification management, data masking, remote access control etc. if needed;
- Making template of contract on outbound transfer of data;
- Build up internal protocol of risk self-assessment on outbound data;
- Do research on legal environment in the place where the data receipt is located;
- Prepare initial draft of risk self-assessment report; and
- Closely follow up on the legal update and development of business practices.

For tailored measures and practical advices on legal compliance, please contact us.

Want to know more?

Cynthia Chung
Partner
cynthia.chung@deacons.com
+852 2825 9297

Machiuanna Chu
Partner
machiuanna.chu@deacons.com
+852 2825 9630

Edwarde Webre
Partner
edwarde.webre@deacons.com
+852 2825 9730

Elsie Chan
Partner
elsie.chan@deacons.com
+852 2825 9604

Helen Liao
Partner
helen.liao@deacons.com
+852 2825 9779

Stefano Mariani
Partner
stefano.mariani@deacons.com
+852 2825 9314