

Explore the draft guidance on preparing for the Certification of Cross-border Data Transfer

May 5, 2022

On April 29, the 'Practical Guidance of Cybersecurity Standards—Technical Specifications for Certification of Cross-border Handling of Personal Information (Draft for Comment)' (hereinafter referred to as 'Certification Technical Specifications') was released by the National Information Security Standardization Technical Committee. It is the first document to explore personal information protection certification under Article 38 of Personal Information Protection Law (PIPL).

Article 38 provides four mechanisms of transferring personal information abroad, one of which is getting certified by professional agencies. The other three are (i) conducting security review by government agencies, (ii) SCC-alike mechanism, i.e., entering into standard contracts with data recipients abroad, and (iii) a catch-all provision, i.e., conditions as stipulated by applicable laws or regulations. While the security review mechanism specifies that it applies to critical information infrastructure operators and data handlers that process certain threshold of personal information, the applicable scopes of other mechanisms are unclear, including certification.

The Certification Technical Specifications endeavors to define the scope of cross-border transfer of personal information by certification. It also enumerates factors to be assessed in certification. Although it will be a guidance instead of a mandatory regulation if passed, it would have reference value before competent authorities promulgate rules in this regard.

Scope of application

The 'Certification Technical Specifications' applies to the following situations:

- a. Cross-border processing of personal information within a multinational company or within the same economic or business entity;
- b. The overseas personal information handlers stipulated in the second paragraph of Article 3 of the PIPL process personal information of domestic natural persons outside China.

For a. and b., in essence, it is a judgment on what is 'data export behavior'. The key question is whether the data is contacted by foreign subjects. Based on this standard, the transfer of data across jurisdictions, or, though the data has not crossed the border, the access by foreign subjects, are all data export behaviors.

This provision extends the application to the second paragraph of Article 3 of the PIPL, which is usually understood as extraterritorial application of the PIPL. Since the birth of the PIPL, it is controversial as to the issue of whether the requirements of cross-border data transfer apply to extraterritorial application of processing activities. Now judging from the 'Certification Technical Specifications', the answer is affirmative.

It is also provided in this provision that cross-border processing activities of personal information that need to pass the security assessment shall be reported to the national cybersecurity and informatization department in accordance with

applicable laws and regulations. It emphasizes that this certification is not an alternative path to security assessment, but a parallel path. A security assessment must be performed when the situation requires.

Who can apply for certification

For cross-border processing of personal information within a multinational company or within the same economic or business entity, the domestic party may apply for certification and bear legal responsibility.

Overseas personal information processor specified in paragraph 2 of Article 3 of the PIPL may apply for certification through its specialized agencies or designated representatives set up by overseas organizations in China.

Basic principles

In addition to the principles of legality, legitimacy, necessity, the principle of openness and transparency, the principle of information quality, and the principle of responsibility stipulated in the PIPL that all personal information processing activities must follow, the 'Certification Technical Specifications' also clarifies the principle of equal protection and voluntary certification, both originate from Article 38 of the PIPL.

The principle of equal protection requires that cross-border processing of personal information should meet the personal information protection standards stipulated in the relevant laws and regulations of China.

Certification agency

The list of certification agencies needs to be officially designated. The China Cybersecurity Review Technology and Certification Center (CCRC) is likely to become one of the designated certification bodies. The 'Certification Technical Specifications' clearly mentions that its drafting process is supported by CCRC.

The content of certification

According to the Certification Technical Specifications, the content of certification at least include the following 6 dimensions.

1. Legal constraints: legally binding and enforceable documents, i.e., data export contract, should be signed between relevant parties;
2. Management organs: this refers to the person in charge of personal information protection and the personal information protection department;
3. Rules for cross-border processing of personal information;
4. Personal information protection impact assessment: see Articles 55, 56 of PIPL and another public standard 'Information Security Technology ---- Guidance for Personal Information Security Impact Assessment' for more details;
5. Rights of personal information subject;
6. Responsibilities of the related parties.

Key Takeaways

Article 38 of the PIPL provides four paths for cross-border transfer of personal information: security assessment,

certification, standard contract and other conditions. Previously, the Cyberspace Administration of China issued the 'Information Security Technology ---- Guidelines for Personal Information Security Impact Assessment'. It has covered the possible contents of security assessment and standard contracts. The 'Certification Technical Specifications' is the first document to explore the certification of personal information protection.

The certification of cross-border personal information handling activities is a voluntary certification recommended by the state. Eligible parties involved in cross-border personal information activities are encouraged to apply for certification. The applicable scope suggests that certification would be a preferable option for multinationals that have frequent cross-border transfer of personal information.

The 'Certification Technical Specifications' puts forward requirements in terms of basic principles, the scope and method of certification, and the content of certification. It provides basis for future certification agencies to implement certification for cross-border personal information processing activities. It also provides a reference for personal information handlers to the framework of certification.

The 'Certification Technical Specifications' also leaves many issues unsolved. such as whether the effectiveness of certification can defend against compliance inspections, how long the certification is valid, how many scenarios, purposes can a single certification cover, which agencies would be in charge of the certification, etc.. It is necessary for the Cyberspace Administration of China to issue additional measures in the future.

Your Key Contacts



Ken (Jianmin) Dai

Partner, Shanghai

D +86 21 5878 1965

M +86 139 1611 3437

jianmin.dai@dentons.cn



Jet (Zhisong) Deng

Senior Partner, Beijing

D +86 10 5813 7038

M +86 135 2133 7332

zhisong.deng@dentons.cn