DEACONS
的近律師行

Corporate Commercial Client Alert

China Trade & Investment

28 August 2023

Highlights of the Administrative Measures for the Personal Information Protection Compliance Audit (Comment Draft)

Edwarde Webre and Hayley Li

The Personal Information Protection Law (**PIPL**) of China explicitly requires that a personal information processor regularly conduct compliance audits on its processing of personal information to ensure compliance with the PRC's laws and administrative regulations and authorizes the responsible authorities to require a personal information processor to engage a professional agency to conduct a compliance audit on its personal information processing activities. The Cyberspace Administration of China has issued for comment the Administrative Measures for the Personal Information Protection Compliance Audit (Comment Draft) (the **Measures**) which set out potential requirements for compliance audits under the PIPL.

The Measures specifies the frequency of the compliance audits: a personal information processor that processes the personal information of more than 1 million individuals is required to carry out personal information protection compliance audits at least once a year; and any other personal information processor is required to conduct a compliance audit at least once every two years.

The Measures categorize compliance audits into self-audits or compulsory audits.
Self-audits: the personal information processor carries out a personal information protection compliance audit by itself, either using internal departments within the organization or engaging a professional agency to carry out such audit.

Compulsory audits: responsible personal information protection authorities require personal information processors to engage a professional agency to conduct compliance audits for their personal information processing activities where they find that there are relatively high risks in personal information processing activities, or personal information security incidents have occurred.

The Measures do not elaborate on Self-audits, but mainly set out a series of requirements regarding the compulsory audits. A personal information processor must select a professional agency to conduct the personal information protection compliance audit as soon as possible after receiving a compulsory audit notice. Regarding the selection of a professional agency, Article 13 of the Measures states that the national cyberspace authority, in concert with the public security departments and other relevant departments under the State Council, shall establish a recommended catalogue of professional agencies for personal information protection compliance audits. Professional agencies shall maintain independence and objectivity, and may carry out the personal information protection compliance audits for the same entity for no more than three times consecutively. The compulsory audits shall be completed within 90 working days, and the compliance audit report shall be signed by the person in charge of the compliance and the person in charge of the professional agency, with the official seal of the professional agency affixed. The audit results shall be submitted to the related responsible authorities. Where the professional agency gives rectification suggestions, the personal information processor shall make the rectifications in accordance with the suggestions and submit a rectification report to the responsible authorities following review by the professional agency.

An annex of Reference Points for Compliance Audit of Personal Information Protection (**Points**), consisting of 31 articles in total, is attached to the Measures. The Points list out the main auditing items, so as to provide references to personal information processors to conduct compliance audit activities, in accordance with the compulsory requirements in PIPL and other laws, administrative regulations and national standards, etc. It covers a wide range of personal information processing activities, including the basic legality, personal information processing rules, third-party processor involvement, automated decision-making, disclosure of personal information, cross-border transfer of personal information, the rights of the subject of personal information, the obligations of personal information processor, special requirements for the operators of large Internet platforms.

The Measures are still in comment draft form. A future official edition may refine and improve on the rules for personal information protection compliance audits. The Measure are open for comment through 2 September 2023. Deacons will pay close attention to the status of legislation on personal information protection, and provide updates on changes that may impact your business. Please contact us for tailored measures and practical advice to manage risk in personal information processing.

Want to know more?

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

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

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

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

Mark Stevens
Partner
mark.stevens@deacons.com
+852 2825 5192

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