China Releases Measures for Personal Information Protection Compliance Audits

The obligation of personal information processors to conduct personal information compliance audits is stipulated in the *PRC Personal Information Protection Law* ("PIPL") and the *Regulations on Network Data Security Management*. To provide systematic and operational guidelines for conducting personal information compliance audits, the Cyberspace Administration of China has formulated and released the *Measures for Personal Information Protection Compliance Audits* ("Measures"), which will come into effect on 1 May 2025.

We have listed below three key aspects that companies should focus on.

1. Which companies need to conduct compliance audits and when?

There are two scenarios to conduct personal information protection compliance audits, which are self-conducted audits and ordered audits.

As to self-conducted compliance audits, it is explicitly required that personal information processors handling the personal information of more than 10 million individuals should conduct audits at least once every two years. For other personal information processors, they only need to reasonably determine the frequency of regularly conducting audits based on their own circumstances.

Compliance audits ordered to be conducted, refer to situations where the cyberspace authority and other authorities responsible for personal information protection, may require the personal information processor to engage a professional organization to carry out compliance audits: (1) If significant risks, such as serious impacts on individuals' rights and interests or a severe lack of security measures, are identified in personal information processing activities; (2) If the personal information processing activities may infringe upon the rights and interests of a large number of individuals; or (3) If a personal information security incident occurs, resulting in the leakage, alteration, loss, or damage of the personal information of one million individuals or more, or of the sensitive personal information of 100,000 individuals or more.

In summary, for general companies, not subject to conduct ordered compliance audits, there are no compulsory requirements for an immediate compliance audit. However, to avoid triggering a compliance audit ordered by the authorities, we recommend that general companies also refer to the standard of conducting compliance audits once every two years and initiate the first audit as soon as possible. According to the relevant provisions of the PIPL, failure to conduct personal information

protection compliance audits may result in facing administrative such as warnings, confiscation of illegal gains, fines, or even criminal liabilities.

2. Who shall conduct compliance audits?

When personal information processors conduct compliance audits on their own, they can choose to have them carried out by an internal body or entrust a third-party professional institution to do so. However, when the authorities explicitly require companies to conduct compliance audits due to significant data security risks or incidents, the company must entrust a third-party professional institution to perform the audits.

Regarding entrusting third-party professional institutions to conduct audits, the Measures clearly outline three obligations for companies: Firstly, ensuring the smooth conduct of compliance audits by providing necessary support and audit fees. Secondly, selecting a professional institution as required by the authorities and completing the audits within a specified time frame. Lastly, after completing the compliance audits, the personal information processor must submit the personal information protection compliance audit report issued by the professional institution to the authorities and make rectifications as required.

3. What are the key points for compliance audits?

Given the extensive content involved in compliance audits, the Measures have included all reference points for conducting the audits in the attachment of the Measures, i.e. the *Guidelines for Personal Information Protection Compliance Audits* ("Guidelines"). The Guidelines outline key compliance matters that shall be focused on under 26 different scenarios. Taking the key matters for assessing whether companies have established an internal management system and operating procedures as an example, compared to a single sentence in the PIPL, the Guidelines clearly list the following items for companies to review:

- Whether the policies, objectives, and principles for personal information protection comply with laws and regulations;
- Whether the organizational structure, staffing, code of conduct, and management responsibilities for personal information protection are appropriate to the personal information protection responsibilities;
- Whether personal information is classified based on its type, source, sensitivity, and intended use;
- Whether an emergency response mechanism for personal information security incidents has been established;
- Whether a personal information protection impact assessment system and compliance audit system have been established;
- Whether a clear process for accepting personal information protection complaints and reports has been established;
- Whether the authorization to operate personal information processing are reasonably defined;
- Whether a plan for conducting personal information protection security education and training has been developed;
- Whether a performance evaluation system for relevant personnel has been established;
- Whether an accountability system for unlawful personal information processing has been established; and

- Any other matters specified by laws and regulations.

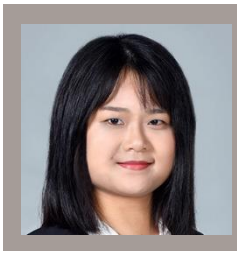
Therefore, the Guidelines not only serve as a reference for compliance audits but also can be referred to in companies' daily data compliance management activities to identify gaps and inadequacies.

In addition, there is the draft version for public comments for the national standard *Data Security Technology - Requirements for Personal Information Protection Compliance Audits* ("Standard"). This draft Standard covers detailed audits processes, audits evidence, audits methods, audit reports template etc., and will become a critical reference standard for companies upon its official release.

We recommend that when companies conduct compliance audits, they should review each point listed in the Guidelines and may need to address each point individually in the audit report, referring to the audit report template in the Standard.

The Measures will come into effect in three months. Considering that data compliance may require communication across multiple departments, companies should refer to the Measures and the Guidelines, or entrust professional institutions, to promptly establish personal information compliance audits mechanisms or address deficiencies in existing audits mechanisms to fulfill the obligation of conducting personal information compliance audits.

In case you have questions or for further information, please contact the authors of this newsletter:



Panpan Tang
Senior Associate
CMS, China

T +86 21 6289 6363
E Panpan.Tang@cmslegal.cn

Daisy Lv
Junior Associate
CMS, China

T + 86 21 6289 6363
E Daisy.Lv@cmslegal.cn

CMS Hasche Sigle Shanghai
Representative Office (Germany)
3108 Plaza 66, Tower 2
1266 Nanjing Road West
Shanghai 200040, China

CMS Cameron McKenna LLP Beijing
Representative Office (UK)
Room 1405, West Tower, World Financial Centre
No.1 Middle East Third Ring Road
Beijing 100020, China