

Legal Commentary

February 17, 2025

New Rule for PI Protection Compliance Audit and Implications

Authors: Ting ZHENG | Eryin YING | Shirley LIANG | Hattie ZHANG

On 14 February 2025, the Cyberspace Administration of China (“CAC”) released the *Administrative Measures for the Personal Information Protection Compliance Audit* (《个人信息保护合规审计管理办法》, the “**PI Audit Measures**”) and its FAQ on its official website¹. Prior to that, CAC presented the consultation draft of PI Audit Measures in August 2023, and the National Cyber Security Standardisation Technical Committee of China proposed a set of national standards on compliance audit requirements in July 2024.

Compliance audit for personal information (“PI”) protection is an existing requirement derived from Art. 54 of *Personal Information Protection Law* (《个人信息保护法》, the “**PIPL**”) and Art.27 of the *Regulation on Network Data Security Management* (《网络数据安全条例》, the “**Network Data Regulation**”). The PI Audit Measures serve as implementing rules for these compliance audit requirements and will take effect from 1 May 2025.

We set out below the key requirements under the PI Audit Measures and its implications for foreign funded financial institutions and multinational corporations as PI processors.

Triggers, frequency and methods of two compliance audits

I. Self-initiated audits

- Where a PI processor processes PI of less than ten million individuals, the PI processor shall conduct a self-initiated audit at a frequency that it determines depending on own specific circumstances. We anticipate a compliance audit every three to five years should be reasonable.
- Where a PI processor processes PI of more than ten million individuals, the PI processor will be required to conduct compliance audit at least once every two years.
- In a self-initiated audit, PI processors will have flexibility to determine whether to conduct the audit internally or by engaging an external professional agency.

¹ Official links: https://www.cac.gov.cn/2025-02/14/c_1741233507681519.htm; https://www.cac.gov.cn/2025-02/14/c_1741232792029282.htm.

II. Compulsory audits

- CAC and/or industry regulators may mandate a PI processor to appoint an external professional agency to conduct a compliance audit as soon as possible upon occurrence of any of the following events:
 - (1) there is a significant risk in its PI processing activities that severely affects individuals' rights or lacks adequate security measures; or
 - (2) its PI processing activities may infringe on the rights of a large number of individuals; or
 - (3) a PI security incident occurs, resulting in the leakage, tampering, loss, or destruction of PI of over one million individuals or sensitive PI of over 100,000 individuals.
- It remains unclear what precisely constitutes the first two trigger events. The regulators may have discretionary interpretations during the implementation of the compulsory audits.
- There is no specific timeframe for conducting a compulsory audit. The timeframe will be subject to the regulators' discretion case by case, and it may only be extended upon special approval from the regulators.
- In a compulsory audit, PI processors will be required to provide necessary assistance to the professional agency, bear audit costs, conduct the rectification as required by the regulators, and submit the relevant report to the regulators within 15 business days after completion of the audit.
- It remains to be seen which professional agencies will be qualified to conduct compliance audits for PI processors. A PI processor cannot engage the same professional agency to conduct over three consecutive compliance audits for PI protection.

Scope and standards of compliance audits

I. Legal basis and scope

Self-initiated and compulsory audits shall be conducted based on the PIPL, the Network Data Regulation and other laws, administrative regulations applicable to PI processing activities. The *Personal Information Protection Compliance Audit Guidelines* (《个人信息保护合规审计指引》) attached to the PI Audit Measures set out the key aspects that shall be covered in any compliance audit, including but not limited to:

- legitimacy of the basis and rules for PI processing;
- disclosure and explanation of the PI processing rules;
- joint processing and entrusted processing of PI;
- transfer and sharing of PI;
- automated decision-making;
- public disclosure of PI;

-
- legitimacy of the basis and purpose of image collection and ID devices;
 - processing of disclosed PI;
 - processing of sensitive PI and minors under the age of 14;
 - cross-border transfer of PI;
 - protection of data subjects' rights in PI processing activities;
 - adequacy of internal organizational setup and measures for data security;
 - efficacy of IT measures for data security; and
 - training, IT security emergency handling and PIPIA etc.

II. Recommended standards

The 2024 draft of national standards on compliance audit requirements (《数据安全技术 个人信息保护合规审计要求》) provided comprehensive guidelines for conducting compliance audits for PI protection, including detailed standards on implementation procedures and evidence management, as well as capability and independence of auditors. These are recommended standards and may represent best practice in the market. It remains to be seen whether National Cyber Security Standardisation Technical Committee of China would propose new set of national standards based on the PI Audit Measures.

Legal liability for violations

Any breaches of the PI Audit Measures will render a PI processor subject to penalties in accordance with the PIPL and the Network Data Regulation, including but not limited to confiscation of illegal gains, an order to make corrections, suspension or termination of business, fine and revocation of business license. Senior officers may also face personal liabilities.

Recommendations

It's important for all PI processors to comply with the PI Audit Measures. Proper audits will help a PI processor to reduce risks of being challenged or penalized by CAC or industry regulators in data breaches and complaints. It's highly recommended that PI processors should set up PI protection compliance audit systems, procedures and responsible team and take immediate actions to ensure all audit requirements will be fulfilled.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Ting ZHENG

Tel: +86 21 6080 0203

Email: ting.zheng@hankunlaw.com