Client Alert

February 2025

China CAC Issued Detailed Rules on Personal Information Protection Compliance Audit

Contents

On February 12, 2025, the Cyberspace Administration of China ("**CAC**") issued the Measures for the Administration of Personal Information Compliance Audit (the "**Audit Measures**"), which will take effect from May 1, 2025. The draft of the Audit Measures was first released for solicitation of public comments on August 3, 2023, and it took a year and a half for CAC to finalize the Audit Measures. In the final version of the Audit Measures, there are a few notable changes compared with the draft version, which reflect the evolving and more relaxed data protection regulatory stance of the CAC.

The Audit Measures are detailed rules for the implementation of the general requirements for personal information protection compliance audits stipulated under the *Personal Information Protection Law of the PRC* (the "**PIPL**") and the *Regulations on the Administration of Network Data Security* (the "**Network Data Security Regulations**", which took effect from January 1, 2025). Under the PIPL, each personal information processor ("**PIP**", which is akin to a "data controller" under the data privacy laws in the EU and some other jurisdictions) has a statutory obligation to conduct a personal information compliance audit ("**Audit**") periodically (Article 54 of the PIPL), and where any considerable risk is found in the personal information activity of a PIP or any personal information security incident is found with a PIP, the relevant data protection authority in China such as CAC (the "**Data Protection Authority**") may require such PIP to engage a professional institution to conduct an Audit (Article 64 of the PIPL). Article 27 of the Network Data Security Regulations requires each network data processor (a concept that can be considered almost equivalent to PIP, where only personal information but not other data is concerned) to conduct an Audit periodically either by itself or by engaging a professional institution to do the same.

The PIPL, the Network Data Security Regulations and other laws and regulations have imposed quite a large number of data protection obligations on PIPs. Obviously CAC does not and will never have sufficient resources and bandwidth to supervise all PIPs' personal information processing activities. By establishing and rolling out the Audit requirements, CAC will be able to leverage social resources (whether PIPs themselves or the professional institutions engaged by them) to exert more effective mandate on PIPs for ongoing compliance of personal information processing activities with applicable laws and regulations.

We set out below a few highlights of the Audit Measures.

Who must conduct the Audit?

As the Audit Measures are intended to implement the PIPL and the Network Data Security Regulations, while the Audit Measures do not explicitly provide so, it can be reasonably inferred from the Audit Measures that each PIP in China has a statutory obligation to conduct the Audit periodically (a "**Periodical Audit**"). As mentioned below, depending on the volume and nature of personal information processed by a PIP, the frequency requirement would be different. For example, if a PIP processes over 10,000,000 individuals' personal information, it must conduct an Audit every two years

Furthermore, the Data Protection Authority has the power to require a PIP to engage a professional institution to conduct an Audit (a "**Required Audit**") under any of the following circumstances:

(i) where personal information processing activities pose a relatively high risk (including serious impact on individuals' rights and interests, serious lack of security measures, etc.);
(ii) where personal information processing activities may infringe upon the rights and interests of a large number of individuals; or
(iii) where a personal information security incident has occurred, resulting in the leakage, tampering, loss or destruction of 1,000,000 or more individuals' personal information or 100,000 or more individuals' sensitive personal information.

According to Article 3 of the PIPL, the PIPL is applicable extraterritorially to certain PIPs incorporated outside of China when they process personal information of individuals located in China. However, Articles 2 of the Audit Measures provides that the Audit Measures apply to Audits conducted in China. The Audit Measures do not expressly stipulate that those overseas PIPs should also conduct Audits for processing of personal information of individuals located in China.

Who can/should carry out the Audit work?

For a Periodical Audit, a PIP can either conduct the Audit by itself via an internal organ (which could be its data privacy team, legal or compliance department, as applicable), or engage a professional institution (e.g., a law firm) to carry out the Audit work.

For a Required Audit, a PIP must engage a professional institution (subject to conditions that may be imposed by the Data Protection Authority) to carry out the Audit work, and the PIP should provide necessary support to the professional institution and bear the Audit fees.

There is no mandatory qualification requirement for the professional institution under the Audit Measures. As long as a professional institution has Audit capabilities and has appropriate personnel, office, facilities and funds, it will be allowed to provide Audit services. However, a single professional institution and its affiliates and a single responsible person thereof cannot conduct the Audit against the same target for three times consecutively. The final version of the Audit Measures remove the mechanism proposed in the draft version, where CAC will issue and maintain a recommended list of the professional institutions and encourage the PIPs to give priority to ones included in such recommended list when choosing the professional institutions for the Audit. Instead, Article 7 of the final version of the Audit Measures provides that professional institutions are encouraged to obtain professional certification in accordance with applicable certification regulations in China.

We believe that such an arrangement is mainly due to the reason that the Audit is not only a procedural process but a comprehensive review and rectification exercise. The Audit result may have significant impact on a PIP's business operation and, therefore, the professional judgement and advice would be critical especially under the current fluid and fast-evolving data protection law regime. Textbook advice without market experience and practical consideration may invite unnecessary complications and in turn, significantly increase a PIP's compliance burdens and costs.

Additionally, if a PIP processes personal information of 1,000,000 or more individuals, it must designate a person responsible for personal information protection (who is effectively the data protection officer ("**DPO**") of the PIP), and such responsible person will be in charge of the Audit. This is the first time when the threshold regarding the appointment of a DPO (as mentioned in Article 52 of the PIPL) is made clear and explicit. However, the Audit Measures are silent on the qualification of the DPO (including whether an external advisor can take on such role for a PIP).

A PIP that (i) provides important Internet platform services, (ii) has a huge number of users or (iii) operates a complicated set of businesses of different categories should set up an independent organ mainly consisting of external members to supervise the Audit.

How frequently should the Audit be conducted?

The Audit Measures only stipulate that a PIP processing over 10,000,000 individuals' personal information must conduct a Periodical Audit every two years. In the draft version, this requirement was proposed to apply to the PIPs processing over 1,000,000 individuals' personal information and the frequency of the Periodical Audit was set on an annual basis. This significant increase of the statutory threshold for the Periodical Audit shows CAC's intention to balance the compliance burden and regulatory goal to minimize risks arising out of processing of personal information.

For other PIPs, the Audit Measures are silent on the frequency of Periodical Audits that they need to conduct. CAC stated in its official press release that such other PIPs should reasonably determine the frequency based on their own situations. We believe that the period between two Periodical Audits can at least be reasonably longer than two years.

It is worth noting that according to Article 37 of the *Regulations on the Cyber Protection for Minors* (the "**Minors Regulations**", which took effect from January 1, 2024), if a PIP processes personal information of minors (under the age of 18),[1] it should conduct the Audit by itself or with the assistance of a professional institution every year, and should report the Audit details to CAC and/or other Data Protection Authority in a timely manner. Such annual audit could be viewed as a dedicated Audit for minors' personal information protection. As the Minors Regulations were issued by the State Council, we believe that this Article 37 should not be affected or prevailed over by the Audit Measures (which were issued by CAC, an authority subordinate to the State Council). There is no legal consequence of a failure to comply with this Article 37 under the Minors Regulations.

Should the Audit results be submitted to the Data Protection Authority?

A Required Audit must be completed within the timeframe as prescribed by the Data Protection Authority, and an Audit report duly executed by the issuing professional institution must be submitted to the Data Protection Authority. CAC stated in its press release that such Audit report would be a rather important reference for the law enforcement actions to be taken by the Data Protection Authority. In the case of a Required Audit, the Data Protection Authority may require the audited PIP to rectify its non-compliances as identified in the Audit report filed with the Data Protection Authority, and the audited PIP should submit a rectification report to the Data Protection Authority within 15 working days after the rectification is completed.

As mentioned above, Article 37 of the Minors Regulation requires a PIP that processes minors' personal information to report its annual Audit details to CAC and/or other Data Protection Authority in a timely manner.

A PIP that does not fall under the circumstances mentioned above is not required to submit its Audit reports, results or other related information to the Data Protection Authority under the Audit Measures. In other words, it is not a compulsory requirement to file any Periodical Audit report with the Data Protection Authority.

What should the Audit cover and how should the Audit be conducted?

According to the Audit Measures, the Audit refers to a supervisory activity of reviewing and evaluating the compliance of a PIP's personal information processing activities with laws and administrative regulations. Those laws and administrative regulations may include (without limitation) the PIPL, the Network Data Security Regulations, etc. Hence, unless otherwise required by the Data Protection Authority, the Audit should be a comprehensive review of the personal information protection compliance status and issues (if any) against the relevant laws and administrative regulations, which may arise out of all personal information processing activities of a PIP covering the entire life cycle of personal information. Accordingly, if a PIP has never conducted any Audit,[2] it would be advisable for it to conduct its first Audit after the Audit Measures become effective. While we believe CAC's regulatory intention is to have the Audit cover comprehensive personal information activities of a PIP, it is unclear under the Audit Measures whether a single Audit (being a Periodical Audit or a Required Audit) (i) must cover a PIP's entire business scenarios involving personal information processing, or (ii) can be limited to specific business scenarios (while the remaining business scenarios are covered in one or more separate Audits for the reasons of priority consideration, available resources, etc.). We tend to believe that PIPs have certain flexibility at least in terms of how their Periodical Audits should be organized under the Audit Measures. For example, they could consider starting with or giving priority to an Audit concerning personal information processing activities of either the least complicated business scenario (so that it would be manageable in terms of time and efforts and such PIPs may gain experience for future Audits) or complex or inherently high-risk business scenario(s).

[1] Unlike the PIPL which provides special protection for minors under the age of 14 (whose personal information should be deemed as sensitive personal information under the PIPL), the Minors Regulations do not mention the age of 14, and "minors" in a broader sense means individuals who are under the age of 18.

[2] A number of PIPs enlisted by CAC conducted a pilot audit in late 2024, and we understand that the pilot audit was mostly conducted on specific business scenarios.

The Audit Measures contain an annex, which serves as CAC's guidance on the Audit and checklist of the items that an Audit should focus on for different compliance obligations and different categories of personal information processing activities. Each PIP should refer to this annex when conducting the Audit. This annex basically covers all major aspects of the PIPL and the Network Data Security Regulations, including but not limited to (i) the legal basis of personal information processing activities, (ii) personal information processing rules, (iii) notifications given to individuals, (iv) joint processing of personal information with other PIP(s), (v) engagement of an entrusted processor, (vi) provision of personal information to other PIP(s), (vii) personal information processing by automated decision-making, (viii) processing of sensitive personal information, (ix) processing of personal information of minors under the age of 14, (x) export of personal information, (xi) individuals' exercise of their rights, (xii) responses to individuals' requests, (xiii) sufficiency of a PIP's internal management and operational procedures for personal information protection, (xiv) effectiveness of security protection technical measures, (xv) DPO's performance of duties, (xvi) personal information protection impact assessment, (xvii) establishment, assessment and implementation of security incident emergency response plan, etc. Under each topic, there is a checklist providing PIPs with guidance as to what they should specifically consider and review when auditing their relevant personal information processing activities or protection practices.

Additionally, a draft recommended national standard for the Audit ("**Audit Standard**") was released for solicitation of public comments on July 12, 2024 and an updated draft of the Audit Standard has been completed on November 25, 2024 and submitted for final review and approval. It is wide expected that this Audit Standard will soon be finalized and formally issued (likely no later than May 1, 2025, i.e. the effective date of the Audit Measures). Although the Audit Standard is a "recommended" national standard and thus will not be legally binding by its nature, it will provide further guidance on how the Audit should be conducted and what requirements the personnel conducting the Audit should meet.

What are the differences between the Audit and other assessments concerning personal information?

Under the PIPL, a personal information protection impact assessment ("**PIPIA**") should be completed by PIPs in respect of certain types of personal information processing activities There is also a similar concept of data protection impact assessment ("**DPIA**") stipulated under the GDPR. To help multinational companies that may be subject to data compliance requirements in various jurisdictions gain a better understanding of the Audit and the PIPIA and better plan and allocate their efforts and resources to fulfil these requirements, a table is prepared below to provide a general comparison with respect to the Audit, the PIA and the DPIA.

	PIPIA	The Audit	DPIA
Legal basis	Article 55 of the PIPL	Articles 54 and 64 of the PIPL	Article 35 of the GDPR
Applicable scenarios	• Processing of sensitive personal information • Using personal information for automated decision-making • Entrusting a third party with the processing of personal information • Providing personal information to another PIP • Making personal information public • Providing personal information to a recipient outside of China	• Periodical Audit • Required Audit An Audit can either cover a company's entire business scenarios involving personal information processing, or only cover specific selected business scenario(s).	A processing of personal data is likely to result in a "high risk" to the rights and freedoms of individuals.
Commencement time	Before the processing of personal information	Can be initiated at any time (according to the internal plan) or at the time specified by the Data Protection Authority	Before the processing of personal data
Purposes / Focuses	To prevent potential compliance risks in relation to specific processing activities	To review the compliance status of existing personal information processing activities and to rectify non-compliance (if any) as identified in the Audit	To prevent potential compliance risks in relation to "high risk" processing activities

What actions are recommended for a PIP in China?

The Audit Measures do not stipulate how frequently a PIP that processes no more than 10,000,000 individuals' personal information should conduct the Audit, and when the first Audit should be initiated and completed. Therefore, even after May 1, 2025 (i.e., the effective date of the Audit Measures), it would not be compulsory for a PIP to initiate or complete an Audit immediately. As mentioned above, further guidance on the implementation of the Audit Measures (including the relevant recommended national standard that is still in the pipeline) is expected to be issued in the near future. PIPs in China may consider temporarily holding off the formal commencement of the Audit, while keeping abreast of the regulatory development and getting prepared for a comprehensive Audit. However, this does not mean that nothing can be prepared for the Audit. With the 10,000,000-individual threshold and flexibility on the business scenarios when conducting the Audit, a PIP processing personal information of considerably large number of individuals in China may consider making use the time period before the effective date of the Audit Measures to conduct data mapping / inventory so that the PIP can have a full picture and better visibility of (a) the total number of individuals in China whose personal information is processed by it; (b) the exact business scenarios involving the processing of personal information.

If a PIP that (i) will be required to conduct a Required Audit due to the number of individuals being processed based on the data mapping / inventory or (ii) have already foreseen or been aware of any relatively higher security risk in connection with certain personal information processing activities, they may also consider starting the planning of the Required Audit, conducting some dedicated review and take corresponding remedial actions in advance, in order to reduce the possibility of being required by the Data Protection Authority to conduct a Required Audit and avoid the identification and subsequent rectification of major or too many non-compliance issues during a Required Audit (if applicable). PIPs that process over 10,000,000 individuals' personal information may consider planning for their Periodical Audit, which we believe should be completed no later than two years after the Audit Measures take effect.

Aside from compliance with the statutory requirements, completing the Audit could also have profound business implications. For instance, PIPs that process personal information of considerably large number of individuals in China (who may or may not be subject to the Required Audit requirement) could be requested by Chinese regulators to provide evidence of its Audit to demonstrate its compliance with the data protection and data security laws and regulations in terms of processing of personal information. Also, PIPs that may receive personal information for processing (no matter in the capacity as a PIP or an entrusted processor) from other PIPs could also be requested by the latter to provide evident of its Audit to demonstrate its compliance status and personal information processing capability. Hence, although there is certain level of flexibility for PIPs to conduct Periodic Audit, PIPs should not take the Audit requirements lightly.

Contact Us

Zhenyu Ruan
Partner
zhenyu.ruan
@bakermckenziefenxun.com

Chris Jiang
Counsel
chris.jiang
@bakermckenziefenxun.com