DS NEWSLETTER savoir faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

Take a closer look at the China Personal Data Audit – Key FAQs

CHINA

The Administrative Measures for Personal Information Protection Compliance Audit of the PRC ("*Measures*"), effective from May 1, 2025, outline what businesses must check to comply with China's data privacy laws. Indeed, according to the Personal Information Protection Law of the PRC ("*PIPL*"), all personal information ("*PI*") controllers shall conduct audit of its PI processing activities regularly. Thus, audits are mandatory for all enterprises processing PI in China, focusing on ensuring that PI is processed legally and securely.

Unlike PIPL, Measures give comparatively clear list of key points to be audited in its Guidelines attached to Measures.

Below is a list of frequently asked questions we have obtained in practice and answers in brief for your reference.

Q1: Who must comply?

A: Measures will apply to all PI controllers who are subject to PIPL. Foreign-invested enterprises ("FIEs") and multinationals with operations in China would be directly subject to these rules. State authorities and public affairs organizations are NOT subject to Measures.

Q2: When are compliance audits required?

A: Measures distinguish between self-initiated audits and those requested by regulators, with specific frequencies based on the volume of PI subjects.

- Mandatory self-audits: Controllers processing PI of or over 10 million individuals must conduct audits at least once every (2) two years. In this case, the audit report is NOT mandatorily required to be submitted to any authority.

  How about controllers who do not reach 10 million in terms of the number of PI subjects? They still have the mandatory obligation of the self-audit per PIPL but the frequency of the audit could be reasonably decided by themselves.

  Besides, controllers shall also examine if there is any other mandatory regulation requesting stricter frequency of the self-audit. For example, controllers processing minors' PI should conduct the self-audit annually, despite the number of the PI subjects.

- Triggered audits: Authorities may require an audit by a professional organization if any of the following scenario occurs: , Serious risks to individuals' rights are identified (e.g., inadequate security measures).
  - The PI processing activity may have adverse impact on a large number of individuals/PI Subjects.
  - Data breach of non-sensitive PI impacts 1 million+ individuals; or, data breach of sensitive PI impacts 100k+ individuals.

  In this case, the audit should be completed within the time frame required by the authority, and the audit report is mandatorily required to be submitted to the competent authority. After rectification, the controller should also submit the rectification report to the authority within 15 working days following the completion of the rectification.

Q3: What are the key points in practice in Measures and its Guidelines?

A: Measures reflect principles set by PIPL and also the recent regulation, namely, the *Regulation on Network Data Security Management* (promulgated on September 24, 2024 and took effect on January 1, 2025). Besides, there are some detailed rules provided by Measures, taking the effectiveness of compliance efforts to the next level. It is no longer a question of "*do you have it or not; or, have you done that*", but more to inspect "*how did you do it and how can you prove what and how you've done*".

In particular, controllers have to bear in mind some key points provided in these Measures that they need to comply with the following obligations when required:

- Controllers process PI of 1 million individuals or more shall appoint a PI protection officer to be responsible for PI protection compliance audits. Where the controller provides important internet platform services, have a large user base, and operate a complex type of business, it shall also establish an independent body that is primarily composed of external members, to supervise PI protection compliance audits.

- The PI protection officer's professional capability and its functioning of work will also be audited. Merely having a PI Protection Officer in name will no longer suffice. The PI Protection Officer must possess both professional experience and expertise, as well as be granted the necessary resources and authority to effectively manage PI processing activities and order internal rectification.

- Measures specifically address the installation of image capture and personal identification equipment in public places, requiring legality and necessity. (E.g., where the PI is used for purposes other than public security, to check if separate consent is obtained after proper notice to the PI subject.)

- Processing publicized PI and have any of the following scenarios would be considered illegal:
  - Sending commercial information unrelated to the purpose of disclosure to email addresses, mobile phone numbers, and other publicly available PI;
  - Using publicly disclosed PI for activities such as online harassment, spreading rumors, or disseminating false information;
  - Processing PI that the individual has explicitly refused to allow processing, even though it was publicly disclosed;
  - Failing to obtain consent from the individual for processing PI that has a material impact on the individual's rights and interests; or
  - Collecting, retaining, or processing publicly disclosed PI beyond a reasonable scope, period, or purpose.

- Where a professional organization is chosen to conduct the PI audit, it shall not subcontract the audits to other organizations. The same professional organization and its affiliated entities, as well as the same compliance audit officer, shall not conduct more than three (3) consecutive audits for the same "auditee". It remains to be clarified in practice if the auditee refers to the controller/independent legal person, or also could be different projects/systems of the same controller.

Q4: What are the key audit focus areas?

A: For FIEs, they will need to pay extra attention to cross-border data transfers and consent, given their operations. At the operational level, audits must align with the Compliance Audit Guidelines (attached to Measures). Critical areas include:

- Legal basis for processing (e.g., valid consent, exceptions for non-consensual processing).
- Transparency and notification (clear disclosure of processing rules).
- Cross-border PI transfers (compliance with security assessments/certifications).
- Automated decision-making (fairness, transparency, opt-out mechanisms).
- Sensitive PI processing (e.g., biometrics, health PI; requires separate consent).
- Minor protection (guardian consent for under-14s).
- Incident response plans (tested protocols for breaches).

Q5: How do Measures impact cross-border PI flows?

A: In addition to the existing cross-border PI transfer rules, one new provision worths attention. PI shall not be provided to organizations and/or individuals which/who are located outside China and blacklisted or listed in the restriction group. It remains to be further introduced by future governmental notices that how the lists work in managing the cross-border PI transfers.

Except the above, Measures do not substantially change the existing rules apply for transferring PI to overseas, however, it is emphasized by Measures that compliance documents for lawful processing of PI should be properly prepared and kept, in case of future audits and/or governmental inspections.

Q6: What are the specific requirements for internal management systems?

A: Measures mandate that controllers establish comprehensive internal governance frameworks, including:

- Policies and procedures: Documented rules aligned with PIPL, covering data classification, retention periods, access controls, and incident response.
- Role clarity: Define responsibilities for the PI Protection Officer, internal audit teams, and senior management.
- Data classification: Categorize data based on sensitivity (e.g., biometrics, financial data) and implement tiered security measures.
- Impact assessments: Conduct regular risk evaluations for high-risk activities (e.g., automated decision-making, cross-border transfers).
- Training programs: Regular training for all employees, with emphasis on consent management, breach reporting, and processing individual rights requests.

Controllers must retain audit trails of policy updates and training records for regulatory inspections.

Q7: What are the obligations for processing individual rights requests?

A: Controllers must establish accessible channels (e.g., online portals, hotlines) to address requests for:

- Access/correction: Provide copies of PI or rectify errors within 15 working days.
- Deletion: Delete PI if retention is no longer necessary, consent is withdrawn, or processing is unlawful.
- Opt-out of automated decisions: Allow users to refuse profiling or demand human intervention.

Responses must be clear, timely, and free of charge. Refusals require detailed legal justifications.

Q8: How should historical PI processing activities be addressed?

A: Controllers must:

- Review legacy systems: Identify non-compliant practices (e.g., outdated consent mechanisms, excessive PI retention).
- Data deletion: delete unnecessary historical PI lacking a lawful basis.
- Re-consent: Where feasible, obtain new consent for ongoing processing of legacy PI.

Document all remediation efforts to demonstrate proactive compliance during audits.

Conclusion

Measures provide a robust framework for ensuring data privacy in China, with key focus areas spanning consent, different scenarios of data processing activities, security, and individual rights. Businesses, particularly FIEs, are recommended getting prepared for these audits by self-checks in advance, focusing on cross-border transfers and sensitive data management, to turn regulatory challenges into competitive advantages in China's high-stakes market.

Contact us for tailored advice.

For any additional information, please contact:

Isabelle DOYON
Senior Associate- Shanghai Office
doyon@dsavocats.com

ZHANG Beibei
Senior Associate - Shanghai Office
beibeizhang@dsavocats.com

2 April 2025