Llinks Client Alert – November 2024
Personal Data Protection Compliance Audits: Are You Ready?

Since the issuance of the *Regulations on Network Data Security Management* on September 30, 2024, personal data protection compliance audits ("**PI Audits**") have become a hot topic. More and more companies began to ask whether they should conduct such audits, who should be responsible, and how to implement audits. In this edition of our Client Alert, we will address key questions regarding PI Audits that are currently top of mind for businesses[1].

1. Is the PI Audit a Legal Obligation?

- The *Personal Information Protection Law* ("**PIPL**") effective in 2021 mandates businesses to regularly audit their personal data processing activities, officially establishing the PIPL Audit as a legal obligation. However, the law does not specify how the PIPL Audit shall be carried out.
- In August 2023, the draft of the *Personal Data Protection Compliance Audit Management Measures* ("**Audit Measures**") was released by the Cyberspace Administration of China ("**CAC**"), outlining the practical requirements for PIPL Audits.
- On July 12, 2024, the *National Standard for Data security technology – Personal Information Protection Compliance Audit Requirements* ("**PI Audit Standard**") was issued by the National Technical Committee 260 on Cybersecurity of Standardization Administration ("**TC 260**") for public comment, adding further clarification.
- The *Regulations on Network Data Security Management,* effective September 30, 2024, reiterated the obligation for data controllers to conduct PI Audits.
- On November 12, 2024, TC 260 launched a pilot program for the launch of the PI Audit Standard in Beijing.
- Therefore, the answer to Question 1 is that the PI Audit has been a statutory obligation since the PIPL's enactment. With the *Regulations on Network Data Security Management* reaffirming this requirement and with audit standards now in place, government supervision and enforcement of these audits are imminent.

2. Who Must Conduct PI Audits?

- All personal data controllers are required to conduct PI Audits.
- According to the *Audit Measures*:

[1] This Client Alert is drafted based on effective laws, regulations and standards, as well as drafts of laws, regulations and standards published as of the date of this Client Alert. The statutory requirements contained in the official version of such draft laws may differ from the ones discussed herein.

  - Data controllers processing the personal information of over 1 million individuals must conduct an audit at least annually.
  - Those processing the personal information of below 1 million individuals should conduct an audit at least once every two years.
- Under the *Minor's Online Protection Regulations*, controllers processing minors' personal data must conduct PI Audits annually.
- The responsibility for conducting the PI Audit generally falls on data controllers, not processors, although processors may need to assist controllers in fulfilling this obligation. Furthermore, for any personal data they process on their own behalf (e.g., employees' data), processors must also conduct a PI Audit.

3. Who Should Initiate the PI Audit?

- **Self-initiated Audit:** A company can either use its internal teams or outsource the audit to a third-party professional agency.
- **Regulatory Audit:** If the regulators determine that there are risks in data processing or there is a specific data security incident, they may require the company to conduct a PI Audit.

4. Which Department Should Lead the PI Audit?

- Although termed an "audit", the PI Audit differs significantly from traditional financial audits.
- The audit requires knowledge in cybersecurity, data protection, privacy compliance and IT, which traditional auditors may lack.
- If the company has an internal data compliance department, they should lead the PIPL Audit. Legal or compliance departments responsible for data compliance can also take the lead.
- The department leading the audit must ensure independence, and avoid conflicts of interest where they are directly involved in data processing activities.
- For regulatory audits, the company cannot conduct the audit internally and must engage a third-party professional agency.

5. Are There Time Limits for PI Audits?

- **Self-initiated Audit:** There are no statutory time limits for self-initiated audits.
- **Regulatory Audit:** A regulatory PI Audit typically must be completed within 90 working days, though this may be extended for complex cases.

6. Do PI Audit Results Need to Be Submitted for Government Approval?

- **Self-initiated Audit:** Results are kept within the company and are not submitted to regulators, though it is advisable to retain records for potential regulatory inspections.

- **Regulatory Audit:** The third-party auditor must submit the audit report to the relevant regulators. After rectifying any compliance issues identified in the report, the company must report back to the regulators on their corrective actions.

7. What Is the Scope of a PI Audit?

- The PI Audit evaluates the compliance of the entire lifecycle of personal data processing activities.
- For businesses that have not previously conducted a PI Audit, it is recommended to audit all personal data processing activities.
- For those who have already conducted a comprehensive audit, subsequent audits should be conducted according to the statutory frequency (once a year or every two years). PI Audits should also be done when changes in data processing activities occur (e.g., introducing new data processing activities).

8. What Are the Key Focuses of a PI Audit?

- Legal bases for data processing: consent, contract necessity, legal obligations, etc.
- Data processing rules: form, content, and compliance with notification requirements.
- Special data processing scenarios: joint processing, outsourcing, cross-border transfers, processing of sensitive data, data related to minors, etc.
- Protection of individual rights: how data subjects' rights are protected and how requests are handled.
- Adequacy of data protection policies and governance.
- Technical measures for data protection.
- Incident response and handling procedures.
- Special considerations for major internet platforms.

9. What Is the Process for Conducting a PI Audit?

- **Planning:** Define audit objectives and scope, and prepare an audit plan.
- **Preparation:** Set up an audit team, conduct preliminary investigations, and develop an audit scheme.
- **Execution:** Collect audit evidence, prepare audit working papers, and confirm audit findings.
- **Reporting:** Draft and deliver the audit report.
- **Corrective Actions:** Identify issues, rectify them, and verify the effectiveness of corrections.
- **Archiving:** Maintain audit-related records.

10. What Should Be Audited in a PI Audit?

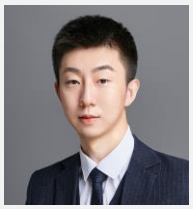
- **Internal policies:** Corporate charter, regulations, data protection policies, standards.

- **Agreements:** Privacy policies, user agreements, data processing/sharing agreements, cross-border data transfer agreements.
- **Records:** Data processing activity logs, and privacy impact assessment records.
- **Network logs:** Access logs, storage logs, transmission logs, deletion logs.
- **Certificates:** Protection certification, data security management certification.
- **Test reports:** Vulnerability detection reports, penetration testing reports, and stress testing reports.
- **Interviews:** Discussions with relevant personnel to understand the implementation of data protection measures.

We hope this overview helps you prepare for upcoming PI Audits and ensure that you are in compliance with evolving data protection laws.

Please feel free to reach out with any further questions or for assistance in preparing your compliance strategy.

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD