Arrow is Drawn:
Purpose, Method, and Suggestion for PI Protection Audit

By Xun Yang | Echo Li | Yara Yang

Recently, the *Management Measures for Personal Information Protection Compliance Audits* ("**Audit Measures**") have been officially introduced and will take effect on May 1, 2025.

From the promulgation of the *Personal Information Protection Law* ("**PIPL**") in 2021, which formally introduced the obligation of compliance audits in the field of personal information protection at the legislation level, to the public consultation draft *Management Measures for Personal Information Protection Compliance Audits* in 2023, the introduction of the *Regulations on the Management of Network Data Security* ("**Network Data Regulations**") in 2024, which confirmed the obligation of personal information protection compliance audits for network data processors, and now to the official implementation of the Audit Measures recently, the personal information protection compliance audit system is poised and ready to launch.

This article briefly outlines the audit requirements under the Audit Measures and provides operational suggestions for enterprises based on industry characteristics and practical experiences.

I. Purpose of Personal Information Protection Compliance Audits

Personal information protection compliance audits are not only a compliance obligation under the PIPL but also a powerful proof of the enterprise's compliance with personal information protection requirements.

First, conducting personal information protection compliance audits is a legal obligation for personal information processors. Article 54 of the PIPL clearly stipulates that "personal information processors shall regularly conduct compliance audits on their processing of personal information in accordance with laws and administrative regulations." Article 64 of the PIPL further states that "in cases where personal information processing activities pose significant risks or personal information security incidents occur," relevant regulatory authorities may "require personal information processors to entrust professional institutions to conduct compliance audits of their personal information processing activities." Article 27 of the Network Data Regulations also explicitly stipulates the obligation of regular compliance audits.

Second, conducting personal information protection compliance audits helps personal information processors demonstrate that they have diligently carried out personal information protection, serving as a defense in case of cybersecurity incidents. According to Article 69 of the PIPL, "if the processing of personal information infringes on personal information rights and causes damage, and the personal information processor cannot prove that it is not at fault, it shall bear liability for damages and other tort liabilities." This means that the liability for personal information infringement is based on the principle of presumed fault, requiring the personal information processor to prove its innocence, and the relevant reports and legal opinions of personal information protection compliance audits can serve as important evidence. Additionally, the relevant reports and legal opinions of personal information protection compliance audits may also play a role in proving compliance during cooperation with business partners and investigations by regulatory authorities.

Finally, conducting personal information protection compliance audits helps enterprises organize personal information and data processing activities, proving the legality and determinacy of data collection, and serving as the basis for determining data ownership, thereby realizing data assetization. As a new production factor, the value of data is self-evident. Through personal information protection compliance audits, enterprises can organize and standardize the collection, storage, use, sharing, and deletion of personal information throughout its lifecycle, remedy personal information protection loopholes, and confirm the legality and ownership of data processing, laying the foundation for future data assetization.

II. Key Points of Personal Information Protection Compliance Audits

The Audit Measures and its appendix, the *Guidelines for Personal Information Protection Compliance Audits* ("**Guidelines**"), provide systematic and operational guidance for conducting personal information protection compliance audits, including:

1. Regular Audits

According to Article 4 of the Audit Measures, "personal information processors that process the personal information of more than 10 million people shall conduct personal information protection compliance audits at least once every two years." For personal information processors that do not meet the processing scale of 10 million people, the Audit Measures do not specify the period for

"regular" audits. We suggest that enterprises determine the period based on industry regulatory requirements and their personal information processing situation. For example, Article 66 of the *Data Security Management Measures for Banking and Insurance Institutions* requires the audit departments of banking and insurance institutions to conduct comprehensive data security audits at least once every three years and to conduct special audits after major data security incidents.

2. Audit Subject

Compliance audits can be conducted by the internal organization of personal information processors or by professional institutions. If the risk situations listed in Article 5 of the Audit Measures occur or personal information security incidents occur, regulatory authorities have the right to require personal information processors to engage professional institutions to conduct compliance audits. Law firms are generally considered professional institutions, and the reports and legal opinions issued by law firms can serve as objective evaluations of the enterprise's personal information protection level and as evidence for the enterprise to legally carry out personal information processing activities and for data assetization.

3. Audit Scope and Key Points

The Guidelines list in detail the matters to be reviewed during compliance audits, corresponding to the requirements of the PIPL and the Network Data Regulations, covering the entire lifecycle of personal information processing, with key points as follows:

(1) Personal information processing rules (legal basis, personal information processing rules, notification obligations, joint processing, entrusted processing, transfer of personal information in mergers/reorganizations/splits/dissolutions/bankruptcies, provision of personal information, automated decision-making, public disclosure of personal information, collection of personal images/identity information in public places, publicly available personal information, sensitive personal information, personal information of minors)

(2) Cross-border transfer of personal information (conditions for providing personal information abroad, provision of personal information based on judicial enforcement, whether it involves restricted or prohibited lists of personal information provision)

(3) Protection of personal information subjects' rights (deletion rights, protection of personal rights, explanations of personal information processing rules)

(4) Obligations of personal information processors (internal management of personal information security, security technical measures, personal information protection officers, personal information protection impact assessments, emergency response)

(5) Special obligations for the protection of personal information by large internet platforms (platform rules, personal information protection social responsibility reports)

4. Audit Procedures

The Audit Measures do not mandate the audit process, but Article 8 of the Audit Measures explicitly states that personal information processors should provide necessary support for the normal audit work of professional institutions when regulatory authorities require compliance audits. Based on relevant national standards and operational practices, the audit process generally includes:

(1) **Audit Preparation**: Through pre-audit questionnaires, document reviews, inquiries, and interviews, understand the current state of the enterprise's personal information protection, determine the audit methods (e.g., a combination of on-site and off-site audits), and prepare an audit plan.

(2) **Audit Implementation**: Conduct interviews, on-site investigations, collect audit materials, carry out evaluation analysis, and prepare audit working papers.

(3) **Problem Identification**: According to legal regulations and industry practices, identify, analyze, and assess risks for issues found during the audit process.

(4) **Issuance of Audit Report**: In the audit report, explain the audit overview, audit conclusions, identified issues, and include rectification suggestions and follow-up on rectification.

5. Audit Results

Audit reports are written documents in which professional institutions express their audit opinions, focusing on, but not limited to, difference analysis, rectification suggestions, and follow-up on rectification. For compliance audits required by regulatory authorities, according to Articles 9 and 10 of the Audit Measures, they must be completed within the specified time and submitted to the regulatory authorities.

III. Suggestion

Based on observed industry characteristics and practical experience, we offer the following brief suggestions for conducting compliance audits:

1. Conduct Compliance Audits with a Focus on Industry Regulatory Requirements, Business Characteristics, and Scenarios

In addition to the detailed review items listed in the guidelines, compliance audits should take into account the business characteristics and scenarios of relevant businesses and align with industry regulatory requirements. For example, in the banking and insurance industry, regulatory requirements include the localization of production systems, effective security controls such as content filtering, access control, and security monitoring. For data, requirements include user access policies for sensitive data, effective user authentication and access control measures, and logging of operations including time and user identification. Additionally, there are security management requirements for service providers. In the securities and fund industry, requirements include isolating production

environments from office environments and the internet, retaining documents produced during system development, testing, deployment, changes, and maintenance, and establishing logging mechanisms to meet emergency response and audit needs. Customer information must be handled independently and not shared. For the pharmaceutical industry, especially clinical trials, personal information processors must comply with the Good Clinical Practice (GCP) guidelines, implement stricter informed consent requirements, protect the privacy of trial subjects, ensure the security and reliability of electronic data management systems, and adhere to minimum retention periods for clinical trial data.

2. Conduct Compliance Audits Based on Personal Information Protection Impact Assessments for Data Exports and Other Activities

Personal Information Protection Impact Assessments (PIAs), required under Article 55 of the PIPL for data exports and other data processing activities, focus on pre-event prevention and risk identification, while compliance audits focus on post-event supervision, difference analysis, and rectification. In practice, both involve a comprehensive review of personal information processing activities and complement each other in building a personal information protection system. For enterprises that have conducted PIAs for data exports as required by Article 55 of the PIPL, these assessments provide good preparation for compliance audits, making them more targeted. For example, if an enterprise has conducted data exports through standard contract filings, the compliance audit can focus on whether the actual export scenarios, fields, and scales match the filed content and whether there is a need for supplementary or re-filing. Additionally, if an enterprise has taken encryption measures during data transmission to ensure the safety of data exports and explained this in the PIA, the compliance audit can focus on whether the encryption measures are fully implemented in practice and whether their strength ensures the security and quality of transmission.

3. Use Compliance Audits to Further Improve Corporate Compliance Levels

Conducting personal information protection compliance audits as required by the Audit Measures is not the final goal. These audits further encourage personal information processors to enhance compliance levels, establish, and improve personal information protection compliance systems. For many enterprises, completing personal information protection compliance audits not only fulfills compliance obligations but can also be a selling point in their business activities.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
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

SHENZHEN
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
Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
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