迈林法律评论

2025 年 3 月

MYLINK
迈林律师事务所

数据合规

新规出台，企业如何开展个人信息保护合规审计?

How Should Enterprises Conduct Personal Information Protection Compliance Audits under the New Released Regulation?

前言

Preamble

2025 年 2 月 14 日，国家互联网信息办公室发布《个人信息保护合规审计管理办法》（以下简称“**《办法》**”），该《办法》自 2025 年 5 月 1 日起正式施行。该《办法》旨在通过对合规审计的细化规定，进一步压实个人信息处理者个人信息保护主体责任，加强个人信息处理活动风险控制和监督。

On February 14, 2025, the Cyberspace Administration of China issued the *Administrative Measures for the Personal Information Protection Compliance Audit* (hereinafter referred to as the "**Measures**"), which will officially come into effect on May 1, 2025. The Measures aim to further implement the personal information protection responsibilities of personal information processors and enhance the risk control and supervision of personal information processing activities through detailed provisions on compliance audits.

本文将通过一问一答的形式，解读该《办法》对个人信息处理者的合规审计要求，以为企业理解和落实个人信息保护合规审计工作提供参考。

This article provides a Q&A analysis of the compliance audit requirements under the Measures to assist enterprises in understanding and implementing personal information protection compliance audits.

I. 该《办法》具体规定了哪些内容?
What are the specific provisions of the Measures?

个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。2021 年，《中华人民共和国个人信息保护法》（以下简称“**《个人信息保护法》**”）首次提出“个人信息保护合规审计”的概念。

Personal information protection compliance audits refer to the supervisory activities that examine and evaluate whether personal information processors comply with laws and administrative regulations in their personal information processing activities. In 2021, the "Personal Information Protection Law of the People's Republic of China" (hereinafter referred to as the "**Personal Information Protection Law**") first introduced the concept of

"personal information protection compliance audit."

为有效实施该制度，《办法》对个人信息保护合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定，旨在为合规审计提供可操作性的规范。
To effectively implement this system, the Measures provide detailed regulations on the conduct of personal information protection compliance audit activities, the selection of compliance audit institutions, the frequency of compliance audits, and the obligations of personal information processors and professional institutions in compliance audits, aiming to provide operable standards for compliance audits.

II. 哪些情况下，企业应当开展针对个人信息保护的合规审计？ In which cases should enterprises carry out personal information protection compliance audits?

该《办法》适用于所有在中华人民共和国境内开展个人信息处理活动的组织和个人，但国家机关及具有公共事务管理职能的组织不适用。
The Measures apply to all organizations and individuals conducting personal information processing activities within the territory of the People's Republic of China, except for state organs and organizations with public affairs management functions.

企业在下述情形下必须进行强制审计：
Enterprises must conduct mandatory audits in the following circumstances:

A. 自行开展合规审计：
Conducting compliance audits on their own:

处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。
Personal information processors handling personal information of more than 10 million people should conduct at least one personal information protection compliance audit every two years.

涉及处理未成年个人信息的，应当自行或者委托专业机构每年对处理未成年人个人信息的情况进行合规审计。
Entities that process minors' personal information must conduct an annual personal information protection compliance audit of such processing activities. The audit may be performed internally or commissioned to a professional institution.

B. 依照保护部门要求开展合规审计：
Conducting compliance audits in accordance with the requirements of the Protection Department:

履行个人信息保护职责的部门（下称“**保护部门**”）在履行职责中，发现如下情形的可以要求企业委托专业机构对其个人信息处理活动进行合规审计：
When the department performing personal information protection duties (hereinafter

referred to as the "**Protection Department**") finds the following circumstances in the performance of its duties, it may require enterprises to entrust a professional institution to conduct a compliance audit on their personal information processing activities:

1. 发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；
   When it is found that the personal information processing activities pose significant risks to personal rights and interests or seriously lack security measures;
2. 个人信息处理活动可能侵害众多个人的权益的；
   When the personal information processing activities may infringe upon the rights and interests of a large number of individuals;
3. 发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。
   When a personal information security incident occurs, resulting in the leakage, tampering, loss, or destruction of personal information of more than 1 million people or sensitive personal information of more than 100,000 people.

C. 除上述特定情形外，其他个人信息处理者也应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计，但是可以根据自身情况合理确定合规审计的频次。
In addition to the above specific circumstances, other personal information processors should also regularly conduct compliance audits on their personal information processing activities in accordance with laws and administrative regulations, but they may reasonably determine the frequency of compliance audits according to their own situations.

III. 自行开展合规审计时，企业应注意哪些事项？ What should enterprises note when conducting self-initiated compliance audits?

自行开展合规审计时，企业可以选择由内部机构自行开展，也可以委托专业机构开展:
When undertaking compliance audits internally, enterprises may either conduct such audits through internal departments or commission accredited professional institutions to perform the audit activities:

A. 企业内部机构自行开展合规审计应注意的事项
Key considerations for in-house compliance audits conducted by corporate internal departments

《办法》暂未对内部机构的人员组成、审计规则等作出详细规定，但结合其他相关标准文件，我们认为，内部机构应当基于合法性、独立性、客观性、全面性、公正性、保密性六项原则开展审计工作，尤其是独立性，即实施审计的人员应回避自身负责的业务内容，独立于具体被审计的个人信息处理活动。
While the Measures do not specify detailed requirements regarding the composition of internal departments or audit protocols, cross-referencing with other relevant standards suggests that internal audits should adhere to six fundamental principles: legality, independence, objectivity, comprehensiveness, impartiality, and confidentiality.

Particular emphasis must be placed on independence, that is, audit personnel shall recuse themselves from reviewing business operations under their own responsibility and remain institutionally separate from the personal information processing activities being audited.

企业亦可参考《办法》附件《个人信息保护合规审计指引》（以下简称“**《指引》**”）中列明的各项重点审查事项开展内部审计活动。
Enterprises may also refer to the key review items listed in the annex of the Measures, the "Personal Information Protection Compliance Audit Guidelines" (hereinafter referred to as the "**Guidelines**"), when conducting internal audit activities.

B. 企业委托专业机构开展合规审计应注意的事项
Key considerations for commissioning external professional institutions to conduct compliance audits

如企业拟委托专业机构开展合规审计，则应当确保该机构应当具备开展合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等，且保证审计的独立性，即同一专业机构及其关联机构、同一合规审计负责人不得连续三次审计同一对象。同时，在接受委托后，该机构不可再次转委托其他机构开展审计。
If an enterprise intends to entrust a professional institution to conduct a compliance audit, it should ensure that the institution has the ability to conduct compliance audits, with audit personnel, premises, facilities, and funds commensurate with the services, and ensure the independence of the audit, that is, the same professional institution and its affiliated institutions, and the same compliance audit person in charge shall not audit the same object continuously three times. Furthermore, upon acceptance of the entrustment, the institution shall not subcontract the audit to other institutions.

《办法》“鼓励”相关专业机构通过认证，即目前尚不存在某一网站或某一清单可以查询哪些专业机构具备认证资质（后续可能会进一步完善），企业可自行筛选在个人信息保护合规领域具备专业知识和经验的律师事务所或其他专业机构开展委托审计工作。
The Measures "encourage" relevant professional institutions to obtain certification, but currently, there is no website or list available to query which professional institutions have certification qualifications (which may be further improved in the future). Enterprises may independently select law firms or other professional institutions with professional knowledge and experience in the field of personal information protection compliance to conduct entrusted audit work.

IV. 依照保护部门要求开展合规审计时，企业应履行哪些法定义务？
What legal obligations should enterprises fulfill when conducting compliance audits in accordance with the requirements of the Protection Department?

A. 提供支持：保障合规审计正常进行，为专业机构开展审计工作提供必要支持，并承担审计费用。
Provide support: ensure the normal progress of the compliance audit, provide necessary support for the professional institution to conduct audit work, and bear the audit costs.

B. 选定委托机构完成审计：按照保护部门要求选定专业机构，在限定时间内完成合规审计，情况复杂的，经批准后可以适当延长。
Select the entrusted institution to complete the audit: select a professional institution as required by the Protection Department and complete the compliance audit within the time limit. If the situation is complex, it may be extended with approval.

C. 报送报告并整改：在完成合规审计后，将专业机构出具的个人信息保护合规审计报告报送保护部门，按照要求对发现的问题进行整改，在整改完成后 15 个工作日内，向保护部门报送整改情况报告。
Submit the report and rectify: after the completion of the compliance audit, submit the personal information protection compliance audit report issued by the professional institution to the Protection Department, rectify the problems found in accordance with the requirements, and submit a rectification report to the Protection Department within 15 working days after the completion of the rectification.

V. 合规审计中，将对企业的哪些活动进行重点审查?
What enterprise activities are subject to priority scrutiny in compliance audits?

附件《指引》结合此前已出台的个人信息保护相关法律法规，围绕个人信息处理活动的合法性基础、处理规则透明度、敏感信息处理等等 26 项重点内容，对合规审计工作进行了梳理和细化。
The annex Guidelines, in conjunction with previously promulgated laws and regulations on personal information protection, systematically organizes and elaborates compliance audit requirements by centering on 26 key areas such as the legal basis for personal information processing activities, transparency of processing rules, and handling of sensitive information.

以个人信息跨境传输为例，根据此前出台的《个人信息保护法》和《促进和规范数据跨境流动规定》，数据出境至少应满足“安全评估、安全认证或标准合同”三项合规机制之一，并同时明确在“实施跨境人力资源管理”和“累计提供不满 10 万人个人信息”等情形下，可豁免上述三种出境合规机制。
Taking the cross-border transmission of personal information as an example, according to the previously issued "Personal Information Protection Law" and "Regulations on Promoting and Regulating the Cross-border Flow of Data," data export should at least meet one of the three compliance mechanisms of "security assessment, security certification, or standard contract," and it is also clearly stipulated that in circumstances such as "implementing cross-border human resource management" and "cumulatively providing personal information of less than 100,000 people," the above three export compliance mechanisms may be waived.

而附件《指引》中列明的数据出境合规审查项目，是基于前述规定，要求在合规审计中重点审查关键信息基础设施运营者等不同类型的数据处理者，在不同情形下是否按照法律规定采取了安全评估、安全认证或标准合同等合规机制。
The data export compliance review items listed in the Guidelines are based on the above regulations, requiring priority scrutiny in the compliance audit of whether different types of

data processors, such as operators of critical information infrastructure, have taken compliance mechanisms such as security assessment, security certification, or standard contract in accordance with the law under different circumstances.

VI. 未依法开展合规审计的企业可能面临哪些处罚?
What penalties may enterprises face for not conducting compliance audits in accordance with the law?

《办法》规定，未依法开展合规审计的，将对企业或接受委托的专业机构依照《个人信息保护法》、《网络数据安全管理条例》等法律法规进行处理：
The Measures stipulate that enterprises or professional institutions accepting the entrustment that do not conduct compliance audits in accordance with the law will be dealt with in accordance with the "Personal Information Protection Law," "Network Data Security Management Regulations," and other laws and regulations:

1. 行政处罚
   Administrative penalties

   责令改正，给予警告，没收违法所得。情节严重的，可能处以五千万元以下或者上一年度营业额百分之五以下罚款，并责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。
   Order corrective actions, issue a formal warning, and confiscate illegal gains. In cases of severe violations, a fine of up to 50 million yuan or up to 5% of the previous year's turnover may be imposed; the relevant business operations may be ordered to suspend or cease for rectification, and the competent authorities may be notified to revoke the relevant business permits or business licenses. The directly responsible supervisors and other liable personnel shall be fined between RMB 100,000 and RMB 1 million, and may be prohibited from holding positions as directors, supervisors, senior management, or personal information protection officers in relevant enterprises for a specified period.

2. 信用风险：依照规定记入信用档案，并予以公示。
   Credit risk: Recorded in the credit file and publicized in accordance with the regulations.

3. 构成犯罪的，依法追究刑事责任
   If a crime is constituted, criminal responsibility will be pursued in accordance with the law.

VII. 现阶段，企业需要为合规审计做哪些准备性工作?
What preparatory work do enterprises need to do for compliance audits at this stage?

1. 结合附件《指引》中列明的各项合规审计审查要点，全面梳理企业内部在人事管理、业务

经营等方面涉及到的个人信息处理活动，识别可能存在的风险点。必要时建立书面管理制度，将个人信息保护及其合规审计制度纳入企业内控体系。
In combination with the various compliance audit review points listed in the annexed Guidelines, comprehensively sort out the personal information processing activities involved in the enterprise's internal personnel management, business operations, and other aspects, identify potential risk points, and establish written management systems when necessary, incorporating personal information protection and its compliance audit system into the enterprise's internal control system.

2. 综合考虑企业的组织规模、业务种类、个人信息数量等因素，组建内部审计组。可从内审团队、安全团队、法务团队等具有审计或个人信息保护相关专业能力的团队中选派审计人员，并组织审前培训。
Comprehensively considering factors such as the enterprise's organizational size, business types, and the quantity of personal information, form an internal audit team. Audit personnel may be selected from teams with audit or personal information protection-related professional capabilities, such as internal audit teams, security teams, and legal teams, and pre-audit training should be organized.

3. 对于处理 100 万人以上个人信息的企业，应当指定个人信息保护负责人，负责合规审计工作。
For enterprises processing personal information of more than 1 million people, a personal information protection person in charge should be designated to be responsible for the compliance audit work.

4. 根据企业的个人信息处理数量和业务规模，合理确定合规审计的频率，必要时可委托外部专业机构进行独立的审计工作。建议形成书面合规审计报告并进行存档，以备监管部门的审查。
Reasonably determine the frequency of compliance audits based on the enterprise's personal information processing volume and business scale, and if necessary, entrust external professional institutions to conduct independent audit work. It is recommended to form a written compliance audit report and keep it on file for review by the regulatory department.

如您对本文有任何问题，请联系：
If you have any questions about this article, please contact us via:

陈祥龙，执行合伙人
Erex Chen, Managing Partner
Tel: +86 21 68556511
Email: erexchen@mylinklaw.com