《个人信息保护合规审计办法》解读

敏于知

2025 年 02 月 12 日，国家互联网信息办公室（以下简称“网信办”）正式发布了《个人信息保护合规审计管理办法》（以下简称“《办法》”），并于 2025 年 5 月 1 日起正式施行。该《办法》完善了我国个人信息保护治理体系，规范了个人信息保护合规审计活动，为落实保护个人信息权益奠定了坚实的基础。

对于个人信息保护合规审计方面，虽然《中华人民共和国个人信息保护法》第五十四条、第六十四条及《网络数据安全管理条例》第二十七条对个人信息处理者开展个人信息保护合规审计作了相关规定，但并未明确详细的审计要求。《办法》的出台细化了个人信息保护合规审计的开展方式、频率、重点审查事项、个人信息处理者合规审计义务等，为企业提供了合规审计的标准和指引。

《办法》适用范围

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。《办法》适用于所有在中国境内处理个人信息的组织和个人，明确了审计的核心是对合规性的审查，其中第十九条规定对国家机关和法律、法规授权的具有管理公共事务职能的组织的个人信息保护合规审计，不适用本办法。

《办法》征求意见稿与正式版本的主要区别及解读

对比 2023 年 8 月 3 日网信办发布的《办法》征求意见稿和 2025 年 2 月 12 日发布的正式版本，我们发现 6 个关键的不同点，总结如下：

1 **适用范围更明确：**
正式版本明确规定了在中华人民共和国境内开展的个人信息保护合规审计活动适用本办法，而征求意见稿中没有明确提及地域限制。
解读：通过明确规定在中华人民共和国境内开展的活动适用本办法，进一步明确了法律的管辖范围，确保所有在中国境内的个人信息处理活动都受到相应的监管。

2 **调整了个人信息处理者的审计频率：**
正式版本将合规审计的标准从处理超过 100 万人的个人信息的适用主体需每年至少进行一次审计，其他至少两年一次变更为处理超过 1000 万人的个人信息的适用主体需每两年至少进行一次审计。
解读：此举表明政府希望集中资源对处理更大规模数据的企业实施更严格的监督，同时可能也考虑到了中小企业执行合规审计的实际困难。

3 **对专业机构的要求更具体：**
正式版强调了专业机构应具备相应的资质，包括与服务相适应的人员、场所、设施和资金，并鼓励通过认证；而在征求意见稿中并未详细提及这一点。
解读：此举有助于确保审计工作的质量和可靠性，同时也提高了行业门槛，促进了个人信息保护领域的专业化发展。

4 **提出整改期限：**

正式版明确了在完成合规审计后，对发现的问题进行整改并在 15 个工作日内向保护部门（此处指国家网信部门和其他履行个人信息保护职责的部门）报送整改情况报告的要求，这在征求意见稿中未具体说明。

解读：此举使得整改工作更具操作性和执行力，有助于快速响应和解决潜在的安全隐患，从而更好地保护个人信息权益。

5 **要求建立独立监督机制：**

针对处理 100 万人以上个人信息的个人信息处理者，正式版提出了应当指定个人信息保护负责人，并且对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，建议成立由外部成员组成的独立机构来监督合规审计情况，这是征求意见稿中所没有的。

解读：此举说明对大型个人信息处理者提出了更高的管理要求，确保责任到人，也体现了对企业内部治理结构的关注，旨在通过第三方视角加强监督，确保合规措施的有效实施。

6 **要求建立投诉举报机制：**

正式版增加了关于任何组织或个人有权对个人信息保护合规审计中的违法活动进行投诉、举报的规定，以及收到投诉、举报的部门应及时处理并将结果告知投诉人的条款。

解读：此举赋予了公众更多的参与权和监督权，增强了社会监督力量的作用，有助于形成全社会共同维护个人信息安全的良好氛围。

总体来说，这些调整不仅提升了个人信息保护的法律框架的严密性，还增强了执法的可操作性，体现了政府在个人信息保护方面的决心和行动力。这对于促进数字经济健康发展、保障公民信息安全具有重要意义。

个人信息保护合规审计开展方式

个人信息保护合规审计开展方式包括自行开展合规审计和监管合规审计。

自行开展合规审计：由个人信息处理者内部机构或者委托专业机构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。

监管合规审计：由国家网信部门和其他履行个人信息保护职责的部门要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计。

需要自行开展合规审计的情况

《办法》明确规定了处理超过 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。这对大规模数据处理者提出了更高的合规要求，确保其个人信息处理活动受到更严格的监督。对于其他个人信息处理者，虽《办法》未对其他个人信息处理者的合规审计频率提出要求，但企业应考虑公司所在行业、业务体量、业务发展速率、处理个人信息的敏感程度、合规工作成本等实际情况定期开展个人信息保护合规审计，以确保满足《中华人民共和国个人信息保护法》的合规要求。实际执行时，企业可以选择内部审计或外包专业机构，但必须确保审计的定期性和合规性。

企业选择内部审计时，内部审计团队可通过由个人信息保护负责人牵头，多部门参与的方式组建。

企业委托专业机构时，应选择具备开展个人信息保护合规审计能力的专业机构，以提升审计的专业性和可信度，但需注意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以上对同一审计对象开展个人信息保护合规审计。

需要开展监管合规审计的情况

《办法》第五条规定了保护部门可以就以下情形要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计：

（一） 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；

（二） 个人信息处理活动可能侵害众多个人的权益的；

（三） 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。

常见的个人信息处理活动可能侵害众多个人权益的情形包括：平台未告知用户其聊天关键词（如疾病、财务状况）被用于广告定向，且未提供个性化推荐关闭选项；算法模型存在性别歧视倾向，导致女性用户频繁收到母婴产品广告，引发群体投诉；自动化决策导致个人在交易价格等交易条件上遭遇不合理差别待遇的“大数据杀熟”问题。

需注意在特定高风险情况下，监管部门会避免对同一个人信息安全事件或者风险进行重复审计，以减轻企业负担。个人信息处理者在上述情形下按照保护部门要求选定专业机构，在限定时间内完成个人信息保护合规审计；情况复杂的，报保护部门批准后，可以适当延长。这既能确保审计活动高效进行，同时又给予复杂情况一定的灵活性。

在完成合规审计后，个人信息处理者应当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。《办法》第十条要求审计的报告需要外部专业机构的签字盖章，以确保审计报告的权威性和法律责任。后续个人信息处理者应及时对合规审计中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。

个人信息保护合规审计通用流程

（一） 审计准备阶段

- **建立审计小组**
  成立审计小组，成员应包括合规专家、法律顾问、个人信息安全人员以及相关业务部门的代表。审计小组负责制定审计计划、分配任务、确保审计的独立性，并协调各部门的配合。
- **制定审计计划**
  在充分调研组织架构、内部流程制度、主要业务流程、数据处理活动、信息系统和安全控制的前提下，制定详细的审计计划，明确审计的目标、范围、方法和时间安排。审计范围应涵盖所有个人信息的处理环节，包括数据采集、存储、传输、使用和销毁等。
- **审计方案评审**
  对审计计划和方案进行评审，确保其符合企业的实际情况和法律法规要求。方案评审时要特别关注审计的重点领域、方法是否合理、时间安排是否充足等，确保审计的高效和准确。

（二） 审计实施阶段

- **收集审计证据**
  通过文档审阅、访谈以及技术手段检查来收集审计证据，了解个人信息的处理流程和对应安全控制。

- **确认审计发现**
  确保所有发现的问题和潜在风险具有实际依据，并与相关部门核实证据的准确性，同时应评估发现问题的严重性和可能带来的影响，形成审计结论。

（三）审计报告阶段

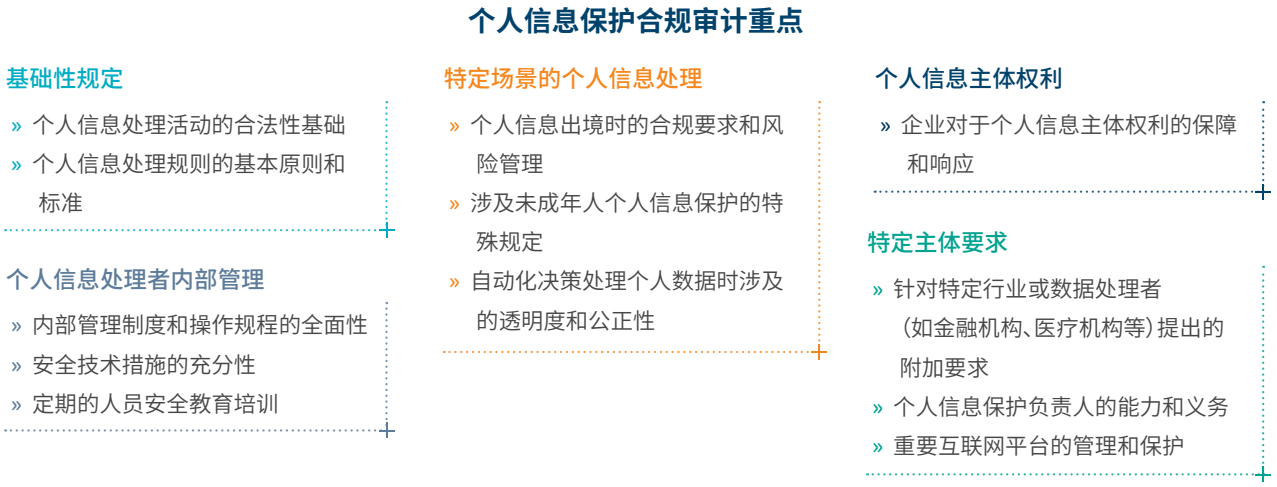
- **编写审计报告**
  根据审计过程中的发现，编写详细的审计报告。报告应包括审计目标、审计方法、审计结果、识别的问题及其影响、整改建议等内容。
- **报告审查与确认**
  完成报告后，审计团队应与相关部门和负责人共同审查报告内容，确保报告的准确性和完整性。如有需要，可对报告进行修订和完善。
- **交付审计报告**
  将审计报告正式交付给相关方（如企业高层、合规部门或审计委员会），并确保报告的内容得到相关方的理解和认可。

（四）整改与后续跟踪阶段

- **整改计划制定与落实**
  企业应根据审计报告中的整改建议，制定具体的整改计划，并明确整改的负责人和时间表。整改工作需要确保在规定时间内落实，并且符合合规要求。
- **整改结果验证与复审**
  审计团队在整改完成后，需进行复审，验证整改措施是否到位，是否能够有效解决发现的问题，此外也可以根据需要进行第二轮的现场检查或技术评估，确保整改工作的有效性。
- **持续监控与合规管理**
  企业应建立长期的合规监控机制，定期进行合规自查，确保个人信息保护措施持续符合最新的法律法规要求，并及时修正出现的任何问题。

个人信息保护合规审计重点

在《个人信息保护审计管理办法》的附件《个人信息保护审计指引》中，明确了 26 个审计重点事项，具体可以分类为基础性规定、特定场景的个人信息处理、个人信息主体权利、个人信息处理者内部管理和特定主体要求，这也是个人信息保护合规审计过程中，重要且容易被忽视的部分。深入审视这些领域，能够帮助确保审计工作的全面性，并有效降低潜在风险。



企业实践建议

- **个人信息资产梳理：**尽快系统化地梳理其所处理的个人信息类型、数量、存储位置，以及相关部门和业务线。通过这种方式，可以确定个人信息保护合规审计所涉及的范围，确保所有相关方能够参与并对齐审计标准和流程。这一步骤有助于明确责任人和审计对象，为后续合规工作奠定基础。
- **设立个人信息保护负责人：**若处理个人信息达到 100 万人以上，应尽快指定个人信息保护负责人，负责个人信息保护合规审计工作。个人信息保护负责人需具备一定的合规知识和管理经验，协调各部门的个人信息保护工作，定期检查合规情况，并确保合规措施落实到位。
- **个人信息保护相关政策完善：**尽快梳理现有的个人信息保护政策，确保所有相关文件齐全并且符合当前法规要求。若现有政策存在滞后或不完善之处，应提前修订并更新，以确保审查时政策的一致性和完整性。
- **建立特殊场景下个人信息处理指南:** 对于涉及特殊场景（如跨境传输、敏感数据处理等）下的个人信息，企业应尽快制定针对性合规指南。这些指南需要明确合规要求、操作流程及风险防控措施，确保这些场景下的信息处理符合相关法律法规。
- **个人信息保护合规审计团队选择：**若选择内部审计，审计团队应具备扎实的个人信息保护专业知识，并保持审计过程的独立性；若选择外部专业机构，需确保其作为客观的第三方进行评估，以确保审计结果的公正性和准确性。

达于行

甫瀚咨询可提供的服务

个人信息保护相关服务

个人信息保护合规审计

基于最新个人信息保护合规审计管理办法的要求，为客户提供定制化的合规审计方案，以确保合规审计对业务及场景的全覆盖。

法律法规专项合规评估

针对客户业务的不同需求，对适用的个人信息保护相关法律法规（如个保法、GDPR等）提供合规评估，并制定改善提升路线图。

安全软件开发流程

在软件开发的早期阶段开始，提供网络安全、隐私保护及个人信息保护相关的咨询服务，以确保安全及隐私保护相关需求得以实现。

关于甫瀚咨询

甫瀚咨询（上海）有限公司是一家具有全球视野的咨询机构。我们在中国开展业务至今已逾二十年，分别在上海、北京、深圳、成都和香港设有五个区域团队。依托甫瀚全球网络，我们能迅速汇聚甫瀚全球超过 25 个国家 90 个分支机构的资源与洞见，灵活调动更适合的专业团队为客户带来高质量的交付，并支持中国企业的海外拓展。

甫瀚咨询的业务遍及运营与财务管理绩效优化、风控与合规、内部审计、信息技术咨询、数字化转型，以及气候变化与可持续发展等领域。我们为中国各行业优秀企业、世界 500 强企业、全球各地资本市场的上市公司以及拟上市公司提供成熟及定制化的解决方案，亦为成长型企业提供陪伴式服务。

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区虹桥路 1 号
港汇恒隆广场办公楼 1 座
2301+2310 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

成都
锦江区红星路三段 1 号
国际金融中心 1 号
办公楼 25 楼

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚

关注甫瀚咨询
获取更多资讯