个人信息保护合规审计管理办法

国家互联网信息办公室令第18号

《个人信息保护合规审计管理办法》已经2024年5月20日国家互联网信息办公室2024年第15次室务会会议审议通过，现予公布，自2025年5月1日起施行。

国家互联网信息办公室主任 庄荣文

2025年2月12日

第一条

为了规范个人信息保护合规审计活动，保护个人信息权益，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条

在中华人民共和国境内开展个人信息保护合规审计，适用本办法。

本办法所称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。

第三条

个人信息处理者自行开展个人信息保护合规审计的，应当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。

第四条

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。

第五条

个人信息处理者有以下情形之一的，国家网信部门和其他履行个人信息保护职责的部门（以下统称为保护部门），可以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。

对同一个人信息安全事件或者风险，不得重复要求个人信息处理者委托专业机构开展个人信息保护合规审计。

第六条

个人信息处理者自行开展或者按照保护部门要求委托专业机构开展个人信息保护合规审计的，应当参照本办法附件《个人信息保护合规审计指引》。

第七条

专业机构应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等。
鼓励相关专业机构通过认证。专业机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。
第八条

个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当为专业机构正常开展个人信息保护合规审计工作提供必要支持，并承担审计费用。
第九条

个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当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。
第十条

个人信息处理者按照保护部门要求开展个人信息保护合规审计的，在完成合规审计后，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。
个人信息保护合规审计报告应当由专业机构主要负责人、合规审计负责人签字并加盖专业机构公章。
第十一条

个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求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。
第十二条

处理100万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。
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，应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。
第十三条

专业机构在从事个人信息保护合规审计活动时，应当遵守法律法规，诚信正直，公正客观地作出合规审计职业判断，对在履行个人信息保护合规审计职责中获得的个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供，在合规审计工作结束后及时删除相关信息。
第十四条

专业机构不得转委托其他机构开展个人信息保护合规审计。
第十五条

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。
第十六条

保护部门对个人信息处理者开展个人信息保护合规审计情况进行监督检查。

第十七条

任何组织、个人有权对个人信息保护合规审计中的违法活动向保护部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

第十八条

个人信息处理者、专业机构违反本办法规定的，依照《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第十九条

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。

第二十条

本办法自2025年5月1日起施行。