汉坤法律评述
2025 年 2 月 18 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约

《个人信息保护合规审计管理办法》五步合规方案

作者：段志超 | 王雨婷 | 苑卉

前言

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》**”）。《办法》细化落实了《个人信息保护法》的审计要求，为个人信息保护合规审计活动（“**个保审计**”）提供了重要参考依据，将自 2025 年 5 月 1 日起实施。随着数据成为新生产要素，各行各业对数据的需求与日俱增。依法开展个人信息保护合规审计活动不仅是个人信息处理者的法定义务，更是推动数字经济健康发展，实现多方共赢的重要举措。

我们在下文中将开展个保审计分为五个关键步骤，分别说明各环节的合规要求并提出我们的建议，供各行业企业参考。

第一步：识别本企业是否需要开展个保审计

原则上，所有个人信息处理者均需开展个保审计，《个人信息保护法》第 54 条规定，个人信息处理者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。《网络数据安全管理条例》第 27 条也提出了类似要求。

企业需统计其个人信息处理规模，以进一步识别对应的合规义务。若处理 100 万以上个人信息的，根据《办法》第 12 条规定，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；若处理 1,000 万以上个人信息的，应当每两年至少开展一次个人信息保护合规审计。

除企业主动依法开展个保审计外，企业还可能在下述情况下基于主管部门的要求被动开展个保审计：

- 主管部门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；
- 个人信息处理活动可能侵害众多个人的权益的；
- 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。

第二步：规划个保审计项目周期

根据《办法》的规定，企业在主动审计与被动审计情况下，需完成个保审计的时间要求各不相同：

- 对于个人信息处理规模未达到 1,000 万的企业，《办法》并未明确规定其开展个保审计的频率，因此该等企业在项目时间安排上具有更多的灵活性。我们建议相关企业可结合个人信息类型敏感情况、现有数据合规体系完备程度、既往安全事件处置情况综合判断。若企业此前从未开展个人信息盘点、个人信息保护影响评估等其他评估梳理工作，我们建议可将个保审计作为企业开展个人信息合规自查的契机。

- 对于处理超过 1,000 万人个人信息的企业，《办法》第 4 条规定每 2 年至少开展一次个人信息保护合规审计。理论上，企业应至迟于 2025 年 5 月 1 日新规生效后 2 年内完成审计。然而，个保审计是《个人信息保护法》项下的强制性合规义务，而非本次《办法》新创设的合规义务。又考虑到这类企业处理的个人信息规模大，若存在违规行为，可能对个人与社会公众造成严重的不利影响，因此，我们建议该等企业即刻着手个保审计的准备工作，并尽快完成个保审计，而非以两年作为规划周期。

- 对于个人信息处理者按照保护部门要求被动开展的个人信息保护合规审计，需在限定时间内完成，情况复杂的，报主管部门批准后，可以适当延长。值得注意的是，《办法》最终稿充分考虑了个保审计工作的复杂性，取消了征求意见稿的 90 日完成期限。

- 若企业属于特定行业或处理特定类型的数据，还需关注特别法的规定，例如《未成年人网络保护条例》第 37 条规定，个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。

第三步：审计前的准备工作

正式开展审计前的准备工作可以包含如下要点：

（一）成立个保审计工作组

我们建议企业全量梳理个人信息处理场景、统计用户量级，根据《办法》第 12 条判断适用的组织管理要求。具体而言：

- 个人信息处理规模超过 100 万人的，应在内部指定个人信息保护负责人，专门负责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、业务类型复杂的超级互联网平台，还应成立外部独立机构，对个人信息保护合规审计情况进行监督；

除领导、监督机构外，实践中，个保审计工作相关的部门通常包括法务部、合规部、各事业部、信息安全部等。

（二）选择专业机构

针对个人信息处理场景数量多、个人信息处理关系复杂的企业，开展个保审计可能需要集中的人力资源投入，该等企业通常会选择委托律师事务所等外部专业机构协助公司开展审计工作。在选择专业机构过程中，企业应将《办法》的相关规定纳入考虑范围：

- 应考虑专业机构的能力、人员、场所、设施、资金等是否支持对方开展相关审计工作（《办法》第 7 条）。值得关注的是，《办法》取消了征求意见稿曾提及的专业机构推荐目录，改为鼓励专业机构通过认证，以避免权力寻租。

- 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（《办法》第 15 条）。
- 按照主管部门要求被动展开个保审计的，应按照其要求选定专业机构（《办法》第九条）。

（三）专业机构聘用

选定机构后，企业可通过协议对专业机构进行约束，要求其按照法律法规规定与企业要求开展审计工作。根据《办法》第 13 条、第 14 条的规定，专业机构需履行如下法定义务：

- 开展个保审计工作过程中，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；
- 不得转委托其他机构开展个人信息保护合规审计。

（四）准备工作资料

在项目启动阶段，企业可将与个人信息处理及内部治理相关的各类文件资料整理备用，包括但不限于数据处理活动记录、APP 测评报告、隐私政策、用户授权记录等材料，并对专业机构以及其他工作组成员开放所需权限，以便工作组开展审计工作。

第四步：实施审计

《办法》第 6 条要求审计工作应参照《办法》附件《个人信息保护合规审计指引》开展。我们将《个人信息保护合规审计指引》所列 26 项合规事项重新梳理如下，以便企业快速了解个保审计的范围：

1	个人信息处理活动的合法性基础；	9	敏感个人信息处理；
2	个人信息处理规则；	10	不满十四周岁未成年人个人信息处理；
3	履行告知义务的方式；	11	向境外提供个人信息；
4	个人信息处理对外合作：共同处理；委托处理；个人信息转移；对外提供；	12	个人信息权利保障情况：删除权；个人信息处理活动中的权利保障；解释说明权；
5	自动化决策使用情况；	13	个人信息保护措施：组织措施；安全技术措施；教育培训；
6	个人信息公开；	14	开展个人信息保护影响评估的情况；
7	在公共场所安装图像收集或个人身份识别设备；	15	个人信息安全事件：应急预案；应急响应处置；
8	处理已公开个人信息；	16	超级互联网平台：平台规则；个人信息保护社会责任报告。

第五步：整改与闭环管理

审计工作完成后，个保审计工作组需编写审计报告，报告应包括但不限于审计概况、审计依据、审计结

论、审计发现、审计意见、审计建议等内容。同时，工作组需清晰记录并留存审计底稿。

如审计工作识别出需整改的事项，企业需协调资源开展相应整改工作，并针对整改措施的完成情况编写整改情况报告。必要时，企业还可以对整改措施有效性进行跟踪审计。

如果企业根据主管部门要求被动开展审计的，还需遵守如下特殊要求：

- 审计报告应由专业机构出具，由机构主要负责人和合规审计负责人签字、盖章后交给主管部门（《办法》第 10 条）；
- 整改完成后 15 个工作日内，向有关部门报送整改情况报告（《办法》第 11 条）。

结语

根据我们的观察，诸多企业在《办法》正式发布前已着手筹备个保审计工作，包括开展内部数据盘点、根据所处行业识别合规要求、起草审计问卷清单等。《办法》生效在即，企业需跳出“被动合规”的思维，主动布局体系化合规审计机制，方能在数据合规深水区行稳致远。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com