汉坤法律评述
2023 年 8 月 4 日

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

《个人信息保护合规审计管理办法（征求意见稿）》要点解读

作者：数据合规组

2023 年 8 月 3 日，国家互联网信息办公室（“**国家网信办**”）发布了《个人信息保护合规审计管理办法》（征求意见稿）（“**《办法草案》**”）。《办法草案》细化落实了《个人信息保护法》提出的个人信息处理者合规审计要求，明确了个人信息保护合规审计触发条件、频次、流程、审计机构、审计活动规范等。《办法草案》还以附件形式详细列明了“个人信息保护合规审计参考要点”，为个人信息处理者开展合规审计工作提供指引。本文旨在简析《办法草案》及其附件提出的个人信息保护合规审计要求，并提示需关注的重点事项。

一、开展个人信息合规审计的两类情形

《办法草案》第 2 条规定了应开展个人信息合规审计工作的两类情形：

一是自行定期开展审计。对应《个人信息保护法》第 54 条，要求个人信息处理者定期对其处理个人信息遵守法律、行政法规的情况开展合规审计。

二是应监管要求审计。对应《个人信息保护法》第 64 条，履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。

二、个人信息合规审计流程

（一）自行开展的定期合规审计

- 审计频次：第 4 条明确，处理超过 100 万人个人信息的个人信息处理者，应当每年至少开展一次审计；其他个人信息处理者应当每二年至少开展一次审计；
- 审计方式：第 5 条规定，可根据实际情况，由组织内部机构或者委托专业机构按照《办法草案》要求开展。

（二）应要求开展的合规审计

- 审计方式：第 7 条规定，应要求开展的合规审计，必须由个人信息处理者委托专业机构进行，而不能自行开展。为保证专业机构的独立性与客观性，第 12 条强调，连续为同一审计对象开展个人信息保护合规审计不得超过三次；

- 配合义务：第 8 条规定了个人信息处理者对委托机构的配合义务，应保证专业机构能够查阅文件或资料、进行实地调查、检查设备与数据、访谈有关人员等；
- 审计时限：第 9 条要求在 90 个工作日内完成审计；情况复杂的，报经履行个人信息保护职责的部门批准后可适当延长；
- 报送与整改：根据第 10 条，个人信息处理者应将专业机构出具的审计报告报送履行个人信息保护职责的部门，报告应当由合规审计负责人、专业机构负责人签字并加盖专业机构公章。此外，第 11 条要求个人信息处理者按照整改建议进行整改，经专业机构复核后将整改情况再行报送。

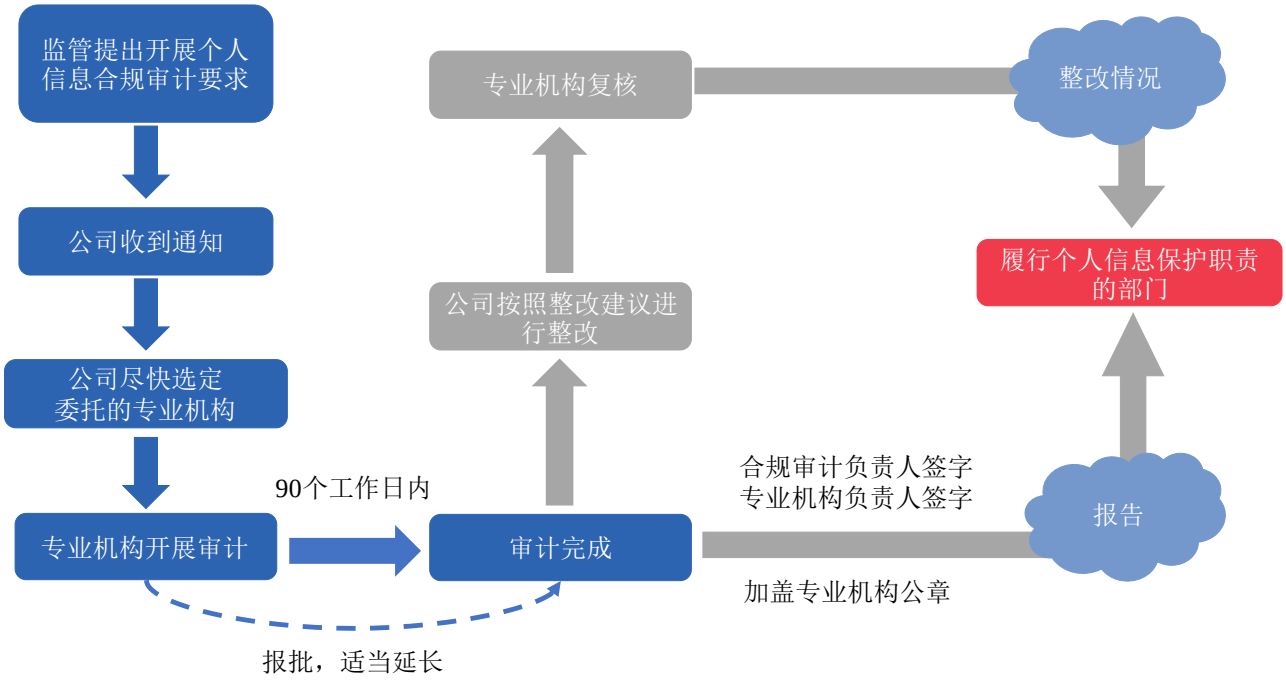

图 1 应监管要求审计的具体流程要求

三、专业机构行为规范

应监管要求开展审计时，个人信息处理者需委托专业机构开展合规审计，个人信息处理者定期自行开展审计时亦可委托专业机构开展。《办法草案》对专业机构的选聘和行为规范着墨颇多：

- **专业机构名录**：国家网信办会同公安机关等国务院有关部门按照统筹规划、合理布局、择优推荐的原则建立个人信息保护合规审计专业机构推荐目录，每年组织开展个人信息保护合规审计专业机构评估评价，并根据评估评价情况动态调整个人信息保护合规审计专业机构推荐目录；
- **独立性和客观性**：同一专业机构连续为同一审计对象开展个人信息合规审计不能超过 3 次；
- **不得转委托**：专业机构不能转包委托第三方开展相关审计工作；
- **数据保密义务**：专业机构在审计工作中获得的信息不能用于其他用途，且应采取措施保障数据安全；
- **审计真实性**：如出具虚假报告等违规行为，将被永久禁止列入推荐目录。

四、个人信息合规审计内容要点

本次《办法草案》附件《个人信息保护合规审计参考要点》（“**《要点》**”）列明了个人信息保护合规审计的主要控制项，涵盖了个人信息全生命周期各环节。征求意见稿版本《要点》第 1 条明确，《要点》仅为开展个人信息保护合规审计提供参考，并非强制要求依照该模板开展审计工作。这些要点主要如下：

- 合法性基础条件：同意的作出，重新取得同意，撤回同意，禁止强制获取用户同意等（第 2 条）；
- 充分告知：告知事项与告知的方式（第 3 条 – 第 4 条）；
- 易引发风险的特殊处理场景：共同处理，委托处理，因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息情形，向第三方提供个人信息，自动化决策，公开个人信息，在公共场所安装图像采集、个人身份识别设备，处理已公开个人信息的，处理敏感个人信息，处理不满十四周岁未成年人个人信息，向境外提供个人信息（第 5 条 – 第 16 条）；
- 保障个人信息权益：个人删除权、个人行使个人信息主体的权利（第 17 条 – 第 19 条）；
- 内部个人信息安全保护制度、组织管理与技术措施：履行主体责任情况，个人信息保护内部管理制度和操作规程，安全技术措施，教育培训计划，个人信息保护负责人，个人信息保护影响评估，安全事件应急预案与应急响应处置情况（第 20 条 – 第 27 条）。

除上述通用审计内容外，《要点》还细化了《个人信息保护法》第 58 条[1]的规定，针对大型互联网平台运营者规定了单独的审计事项，包括审计大型互联网平台运营者的设置个人信息保护监督独立机构情况、大型互联网平台的平台规则、相关平台是否履行对平台内产品或服务提供者履行监督义务以及每年发布个人信息保护社会责任报告的内容披露情况等。《办法草案》与《要点》没有界定大型互联网平台运营者的定义，参考《网络数据安全管理条例（征求意见稿）》第 73 条，大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

五、总结与展望

《办法草案》旨在进一步落地《个人信息保护法》中规定的个人信息合规审计要求，为个人信息处理者以及第三方专业机构开展个人信息合规审计工作提供了具体指引。企业应持续关注《办法草案》更新动态，在《要点》基础上根据相关行业特定合规要求制定内部个人信息合规审计制度，细化审计评估事项。在审计过程中，企业应充分梳理和记录个人信息处理活动，加强企业内部跨部门、跨专业领域的沟通与配合，及时整改合规审计过程中发现的合规风险。此外，由于审计是企业个人信息处理合规性的直接有力证明，未来在网络安全审查、个人信息出境安全评估过程中监管部门可能要求企业提供相关合规审计报告以“自证清白”，因此合规审计制度与其他现有网络安全、个人信息保护制度方面的衔接值得我们进一步重点关注。

[1] 《个人信息保护法》第 58 条：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，应当履行下列义务：（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；（四）定期发布个人信息保护社会责任报告，接受社会监督。

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

蔡克蒙

电话： +86 10 8516 4289
Email： kemeng.cai@hankunlaw.com

解石坡

电话： +86 10 8524 5866
Email： angus.xie@hankunlaw.com