君合研究简讯

JUNHE

2024 年 7 月 30 日

个人信息保护法律热点问题

个人信息合规审计落地又进一步——国家标准发布征求意见

《个人信息保护法》（下称“《**个保法**》”）生效近三年，相关制度也逐渐落地。其中，《个保法》设立的个人信息保护合规审计制度仍有待具体细则的出台。《个保法》规定，个人信息合规审计按照触发情形分为“定期自主审计”以及“不定期强制审计”（即监管部门认为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时的审计）两类。

相关行政法规及部门规章文件也重申个人信息合规审计要求。例如，《未成年人网络保护条例》第三十七条规定，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。《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》规定，要求落实APP开发运营者主体责任，定期对个人信息保护措施及执行情况等进行合规审计。

在此基础上，2023年8月3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（征求意见稿）》（下称“**《审计办法征求意见稿》**”），对《个保法》个人信息合规审计的原则性要求进行了细化与补充，例如处理超过100万人个人信息的个人信息处理者每年应至少开展一次个人信息保护个人信息合规审计；其他个人信息处理者应当每两年至少开展一次，并详细列举了审计点。对于《审计办法征求意见稿》的主要内容，请见《个人信息保护合规审计管理办法（征求意见稿）》要点简析。

2024年7月12日，全国信息安全标准化技术委员会发布国家标准《数据安全技术 个人信息保护合规审计要求（征求意见稿）》（下称“**《审计标准征求意见稿》**”），于2024年9月11日前面向社会公开征求意见，进一步提供了个人信息合规审计的实操指引。

本文拟对个人信息合规审计的制度定位进行阐述，并就《审计标准征求意见稿》中规定的个人信息合规审计的流程、实施管理和人员要求、相关文件、审计内容要点进行简要分析，并向作为个人信息处理者的企业提供依法开展个人信息合规审计的建议。

一 个人信息合规审计制度定位

“审计（audit）”一词原本是指一种经济监督活动。《现代汉语词典》中的审计是指：“由专设机关依照法律对国家各级政府及金融机构、企业事业组织的重大项目和财务收支进行事前和事后的监督、检查。” 根据《中华人民共和国审计法实施条例》，审计法所称审计，是指审计机关依法独立检查被审计单位的会计凭证、会计账簿、财务会计报告以及其他与财政收支、财务收支有关的资料和资产，监督财政收支、财务收支真实、合法和效益的行为。

不同于传统财务审计，国际上尚无企业内部个人信息保护合规审计相关标准。尽管欧盟欧洲数据保护监督机构（EDPS）发布了 Audits conducted by the EDPS - Policy paper 及 EDPS Audit Guidelines，

但上述文件适用于 EDPS 基于其职权对公司数据处理进行审计调查的指引，而非企业内部合规审计指引。

我们理解在制度设计上，个人信息合规审计参考了传统财务审计的框架，以确保审计的权威性及独立性。但个人信息合规审计的审计依据、目的等与传统财务审计存在不同。《审计标准征求意见稿》将个人信息保护合规审计定义为针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。

目前我国已在银行、保险、中央企业等领域专门设立了企业内部审计制度。企业内部审计独立于合规管理。例如，《中央企业内部审计管理暂行办法》要求，企业应当按照国家有关规定，建立相对独立的内部审计机构，配备相应的专职工作人员，建立健全内部审计工作规章制度，有效开展内部审计工作，强化企业内部监督和风险控制。《保险公司合规管理办法》、《中央企业全面风险管理指引》将合规审计作为独立于风险管理职能部门的最后一道风险管理防线。发改委等七部委印发的《企业境外经营合规管理指引》（适用于开展对外贸易、境外投资、对外承包工程等“走出去”相关业务的中国境内企业及其境外子公司、分公司、代表机构等境外分支机构）指出企业合规管理职能应当与内部审计职能分离。从内容上看，日常合规管理工作是合规审计的对象。合规审计应对日常合规管理的执行情况、合规管理体系的适当性和有效性等进行独立评价和审计。日常合规管理工作所形成的评估报告、评测结果、处理记录亦为合规审计提供了重要的证据。例如，《商业银行合规风险管理指引》指出：包含合规性审计的内部审计方案应包括合规管理职能适当性和有效性的审计评价。

根据我们对《审计标准征求意见稿》的研究，目前个人信息保护合规审计制度尚未要求采用与上述央企等领域内部审计制度同样严格的独立性标准，《审计标准征求意见稿》也未强制要求设立独立的个人信息保护审计部门。

二　个人信息合规审计的流程

《审计标准征求意见稿》将个人信息保护合规审计分为审计准备、审计实施、审计报告、问题整改、归档管理五个阶段。各个阶段的主要工作步骤如下：

- **审计准备阶段**：包括建立审计组、开展审前调查、确定审计方式方法、编制和评审审计方案；
- **审计实施阶段**：包括发送审计通知、收集审计证据、采信审计证据撰写审计底稿、确认审计发现；
- **审计报告阶段**：包括异议解决、撰写审计报告、交付审计报告；
- **问题整改阶段**：审计人员应对审计中发现的不合规项进行跟踪，督促被审计方在规定期限内整改。必要时，对整改措施的完成情况及有效性进行跟踪审计；
- **归档管理阶段**：妥善保管个人信息保护合规审计底稿、报告等档案资料。

三　个人信息合规审计实施管理和人员要求

《审计标准征求意见稿》对个人信息合规审计的实施管理和审计人员做了相关要求：

在责任归属方面：个人信息处理者董事会（审计委员会）、个人信息保护负责人或者主要负责人应对个人信息合规审计体系的建立、运行与维护，以及个人信息合规审计的独立性和有效性承担最终责任。

在审计监督方面：个人信息处理者董事会（审计委员会）、个人信息保护负责人或者主要负责人是个人信息合规审计工作的监督人员。此外，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，还应当成立主要由外部成员组成的独立机构对个人信息合规审计情况进行监督。

在制度建设方面：应当制定个人信息保护个人信息合规审计相关管理制度，明确个人信息合规审计开展的形式、频率，以及个人信息合规审计人员的职责及权限，包括但不限于：查阅资料、进入场所、调查系统、检测设备、访谈人员等权限。

在审计独立性方面：一方面，应当为个人信息合规审计配备必要的人员、场地、系统和资金保障，另一方面，《审计标准征求意见稿》规定：就内部审计而言，内部机构审计人员应回避自身负责的业务内容，不应直接参与被审计对象的日常业务运营、个人信息安全保护工作。《审计标准征求意见稿》附录A又指出：未设置专职个人信息保护合规审计团队的，应在保持独立原则的前提下，分别从内审团队、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人员，来自各团队的人员比例应保持在合理范围内，并由审计组长审批人员名单。

《审计标准征求意见稿》还对审计人员的专业能力、独立性、客观性、公正性、保密性、实施要求进行了专条规定。

四　个人信息合规审计的相关文件

审计证据是审计人员获取的能够为个人信息审计结论提供合理基础的全部事实，包括个人信息保护合规审计过程中收集、使用或发现的记录、事实陈述或其他信息。《审计标准征求意见稿》附录B列举了个人信息合规审计证据的常见类型和有效性标准。

审计方案是个人信息合规审计实施时的步骤和安排的描述。《审计标准征求意见稿》明确了编制审计方案时应当参考的因素、基本内容和评审流程。

审计底稿是审计人员对制定的审计计划、实施的审计程序、获取的相关审计证据，以及得出的审计结论作出的记录。审计报告是审计人员在完成对审计证据的整理、归纳、评价及确定审计发现后，形成审计意见和建议，并以适当格式提交的书面文件。《审计标准征求意见稿》附录D和E分别提供了审计底稿和审计报告的模板。

五　个人信息合规审计的内容要点

《审计标准征求意见稿》附录C中列举了开展个人信息合规审计时审查内容、审计证据和审计方法。从内容上看，基本延续《审计办法征求意见稿》附件“个人信息保护合规审计参考要点”中的绝大多数内容。其整体架构与《个保法》中各章规定相对应，同时纳入了如《未成年人网络保护条例》《信息安全技术 个人信息安全规范》等行政法规和国家标准的要求，基本囊括了个人信息处理全流程各环节：

- **个人信息处理规则（C.1-C.13条）**：对应《个保法》第二章内容，对个人信息处理的合法性基础、必要性、处理规则、告知、共同处理、委托处理、合并/分立/重组/破产、提供、自动化决策、公开、公共场所采集、已公开信息、敏感个人信息等要求提出了审计要点。其中，对于共同处理、委托处理、对外提供等涉及第三方的处理场景，《审计标准征求意见稿》对相关场景下的审计证据和方法做了列举，包括但不限于：查验相关合同文档、查阅定期检查记录或监督记录、查看接收方提供的书面说明或检测评估认证报告、查验受托人是否严格按照委托合同的约定处理个人信息。
- **个人信息跨境提供规则（C.14-C.15条）**：对应《个保法》第三章内容，对个人信息出境活动所选择的合规路径、基于司法执法或条约协定的个人信息出境、为保障境外接收方处理个人信息的活动达到《个保法》规定标准所采取的措施等要求提出了审计要点。
- **未成年人信息保护（C.16-C.22条）**：与《审计办法征求意见稿》相比，《审计标准征求意见稿》大量补充细化了未成年人信息保护的审计内容，依据《未成年人网络保护条例》增加了未成年人真实身份审核、收集未成年人个人信息的最小必要、未成年人个人信息主体权利、未成年人个人信息安全事件应急响应处置、未成年人个人信息访问的最小必要、未成年人私密信息保护等审计模块。
- **个人信息主体权利保障（C.23-C.25条）**：对应《个保法》第四章内容，对个人信息删除权保障、个人行使个人信息权益的权利

保障、响应个人对个人信息处理规则解释说明的申请等提出了审计要点。

- **个人信息处理者的义务（C.26-C.33条）**：对应《个保法》第五章内容，对个人信息处理者主体责任、管理措施、技术措施、人员培训、个保负责人、个人信息保护影响评估、个人信息安全应急等要求提出了审计要点。
- **大型互联网平台特殊责任（C.34-C.37条）**：对应《个保法》第58条内容，对个人信息保护独立监督机构、互联网平台规则、平台内的产品或者服务提供者监督、个人信息保护社会责任报告等方面提出了审计要点。

六　观察和建议

《审计标准征求意见稿》对个人信息保护合规审计的原则、要求、流程、审计内容和方法、审计证据进行规定，并提供了审计底稿模板和审计报告模板，为支持《个人信息保护法》、《审计办法征求意见稿》落地实施提供了实践指引和支持。

我们理解，《审计标准征求意见稿》的出台，进一步体现了个人信息保护合规审计制度将趋于落地和成熟。

尽管《审计标准征求意见稿》正式版本的发布尚需一定时间，但是我们建议企业应尽早根据征求意见稿的要求，并结合自身业务与管理体系特点，完善个人信息保护的管理制度和措施，做好个人信息处理活动的记录和文件存档工作，并着手建立内部个人信息保护合规审计工作机制，为《审计办法征求意见稿》、《审计标准征求意见稿》正式实施后所需开展的个人信息合规审计在组织领导、人员配置、技术支持、外部合作等方面做好准备。

董潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com
王威华　律　师　电话：86 10 8519 1297　邮箱地址：wangweihua@junhe.com
[*感谢实习生庞怡凡对本文的贡献*]