

个人信息保护合规审计之我见

作者：杨迅 | 刘莉莎

自 2025 年 5 月 1 日《个人信息保护合规审计管理办法》(以下简称《个保审计办法》)正式生效, 个人信息保护合规审计(以下简称“个保审计”)已从“可选项”逐渐成为企业合规体系的“必答题”。有的企业迅速响应, 投入大量资源搭建审计体系; 但更多企业仍处于观望状态, 对审计的核心逻辑、实操要求和实际价值一知半解。

结合为多家跨国公司、金融机构提供个保审计服务的实践经验, 以及日常咨询中企业高频关注的问题, 本文将从由来、意义、主体、实施方、标准、深度六个维度, 为大家拆解个保审计的核心要点, 让这项看似“玄学”的合规工作变得清晰可落地。

一. 个保审计要求的由来

个保审计是对个人信息处理者遵守法律法规情况进行审查评价的监督活动, 其制度根源可追溯至欧盟《通用数据保护条例》(GDPR)中的“Accountability”(责任担当)要求。GDPR 第五条第 2 款明确, 控制者应当负责, 并能够证明其符合第 1 款的要求(即个人信息保护的七项原则), 在此基础上, GDPR 建立了个人信息控制者的合规负责义务, 即开展定期审查、记录和内部检查, 以确保个人信息处理符合法定义务。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

我国《个人信息保护法》(以下简称《个保法》)中的个保审计要求, 既继承了 GDPR “动态合规、风险平衡”的核心逻辑, 又融入了更多行政监管特色, 不仅明确了监管审计的情形, 《个保审计办法》更细化了审计程序和核心要点, 这与 GDPR 以私权为中心、强调控制者自我负责的思路存在一定差异, 但更贴合我国监管实践。

二. 为什么要做个保审计?

- 法定义务不可违

个保审计是法定义务。《个保法》第五十四条明确要求个人信息处理者定期开展合规审计;《未成年人网络保护条例》进一步规定,处理未成年人个人信息的企业需每年进行专项审计。需说明的是,未开展审计并非必然直接触发行政处罚,但对于重点监管企业,监管机关会主动核查审计情况;而一旦发生网络安全事件,未履行审计义务将成为重要追责依据。

- 风险排查“防护盾”

个保合规义务贯穿企业采购、生产、销售、管理、人事等全生命周期,不同于针对单一环节的专项合规要求。开展个保审计相当于给企业做全面的合规“体检”,能系统评估风险点,及早发现并解决潜在合规问题,避免小隐患演变成大风险。

- 纠纷应对“自证清白”利器

《个保法》第六十九条确立了过错推定责任原则,若因处理个人信息侵害他人权益造成损害,个人信息处理者不能证明自己无过错的,需承担侵权责任。而由专业机构出具的客观合规审计报告,可作为证明企业行为合法合规的关键证据,有效阻断侵权指控。

- 商誉积累与商机赋能

随着公众个人信息保护意识觉醒,涉及个人信息转移的商业合作中,合作方更倾向选择合规体系完善的企业。例如企业采购员工体检服务、保险公司寻求再保险合作时,合规审计结果往往成为重要考量因素,良好的合规记录能帮助企业积累商誉、赢得竞争优势。

三. 谁需要做个保合规审计?

理论上,所有处理个人信息的企业均需履行审计义务,但优先级因企业类型而有所区别,以下三类企业需要重点予以关注:

- 监管重点关注企业

海量数据处理者:《个保审计办法》明确要求,处理个人信息超过 1000 万的信息处理者,每两年必须开展一次审计;

敏感信息处理者:如处理未成年人、医疗健康、金融账户等敏感个人信息的企业,尤其是《未成年人网络保护条例》要求每年开展针对处理未成年人个人信息的专项审计;

重点行业企业：从过往监管实践看，金融、保险、教育、旅游、健康、娱乐、通讯、快消等行业会作为监管重点，需优先落实审计工作。

- **数据驱动型企业**

以数据为核心盈利资产的企业：如大数据公司，通过数据许可、数据产品销售实现盈利，由于该类企业的主要价值在于其处理的数据，因而其客户也通常关注其处理个人信息的合法合规性；

数据赋能型企业：如平台型企业、广告公司、基于个人信息的 AI 开发企业等，数据是其业务开展的核心基础。这类企业的客户高度关注其数据合规水平，审计报告是赢得客户信任的重要凭证。

- **特殊发展阶段企业**

处于数据交易、企业上市等关键阶段的企业，个人信息合规性是数据交易平台、证券交易机构的核心考察项，合规审计结果直接影响交易或上市进程，需提前布局落实。

四. 谁来做个保审计？

- **内部审计 vs 外部审计**

根据《个保法》及《个保审计办法》，企业可选择内部人员开展自我审计，也可委托外部机构实施审计。从合规义务履行角度看，内部审计完全合法，尤其适合法律合规能力较强的企业；但需注意，内部审计报告属于“自制证据”，在民事诉讼中的证明效力相对有限。

而独立外部机构出具的审计报告，类似知识产权诉讼中的技术鉴定意见，虽非绝对不可辩驳，但具有更强的初步证明效力，更能满足“自证清白”，赢得合作信任的需求。

- **外部审计机构的选择标准**

我国目前并未对个保审计机构设定法定资质要求，《个保审计办法》仅要求专业机构具备相应审计能力、人员、场所和资金，并鼓励通过认证；虽然《个人信息保护合规审计专业机构服务能力要求》中对专业审计机构有专业要求，但该团标不具有法律约束力。选择外部机构时，建议重点关注三点：

法律判断能力：个保审计虽名为“审计”，实则是对企业相关行为合法合规性的专业判断。“审计”对应英文“Audit”，其内涵并非仅限财务审计，还涵盖对行为是否符合法律法规或合同约定的审核，本质是一项法律判断。因此，个保审计机构需具备出具法律意见的能力。

行业专业信誉：个保审计并非仅为满足监管要求，若仅需合规达标，内部审计即可实现，其更核心的价值在于从独立视角证明企业个人信息处理行为的合法合规性。因此，优先选择在个人信息保护领域有丰富经验、良好口碑的机构，确保审计的独立性和权威性；

行业场景认知：由于个保审计需对被审计单位业务与经营的全生命周期开展全面审查，且要就行业个人信息保护实践水准作出判断，因此，除个人信息保护相关法律知识外，机构还需了解行业特性，才能做出贴合实际的合规判断。

五. 个保审计的标准是什么？

既然个保审计要对被审计的企业处理个人信息的行为的合法、合规性做出判断，那么这个判断的标准(benchmark)是什么？

- **法律法规**

尤其是《个人信息保护法》以及《未成年人个人信息保护条例》。《网络安全法》和《数据安全法》虽然也是相关的法律，但可参考的条款并不多。

- **部门规章**

即《个保审计办法》及其附件《个人信息保护合规审计指引》(下称《审计指引》)。显然，《个人信息保护法》的条文较为原则，难以满足审计实操需求，而《审计指引》在很大程度上整合了监管机构执行《个保法》的实践落地要求，具有较强的指引价值。

- **国家标准**

针对《个保法》的模糊条款，我国已颁布大量个人信息保护相关国家标准(基本为推荐性国标)，涵盖“单独同意”“匿名化”“敏感个人信息”“隐私计算”等个人信息保护各环节。此类标准虽非强制性，却不乏参考价值。

- **行业实践**

理论上，个保审计作为合法合规性判断，与行业实践并无直接关联，但个人信息保护的诸多要求需结合行业背景考量其合理性。例如临床试验中，若受试者撤回同意后便不再使用已收集数据，可能影响实验科学性，这并不为行业实践所接受；类似地，在资管行业中，投资者个人信息需提供给登记结算机构，而全国实际仅有一家该类机构，此时开展一般意义上的个人信息保护影响评估亦不现实。

六. 个保审计要做到什么程度？

个保审计旨在客观判断被审计企业个人信息保护实践的合法合规性，那么该审计需达到何种程度？

个保审计与尽职调查颇为相似，却又有所不同。尽职调查在很大程度上依赖被调查方的陈述，而个保审计虽包含“访谈”环节，核心却在于对被审计企业的行为作出独立判断，需通过穿行测试、日志分析、控制性测试等技术手段，深入业务系统与数据库，独立获取审计证据，以保障审计结论的客观性与可靠性。

如前文所述，个保审计并非简单满足合规需求，而应体现出客观证明被审计企业个人信息处理行为合法合规的效果。出具个保审计报告的专业机构，并不具备公证机关那般的法律推定权威，其结论很大程度上需凭借专业性与严谨性，获得法院、执法机关及交易对方的认可，进而成为证明被审计企业行为合法合规的有效证据。因此，个保审计需留存充足审计证据，通过严谨论述形成审计结论。

当然，个保审计终究是平等主体间的专业服务，无需也不可能达到公安机关取证那般“排除一切合理怀疑”的程度。尤其对于个人信息处理量较大的情形，设定与行业或业务相匹配的一定比例抽查，是较为合理的选择。

如您希望就相关问题进一步交流，请联系：



杨 迅
通力律师事务所
+86 21 3135 8799
xun.yang@llinkslaw.com



刘莉莎
北京超成律师事务所

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025