

箭已在弦：个人信息保护合规审计的目的、方法和建议

作者：杨迅 | 李依然 | 杨蕾

近日，《个人信息保护合规审计管理办法》(“《**审计办法**》”)正式出台，并将于 2025 年 5 月 1 日起施行。

从 2021 年《个人信息保护法》(“《**个保法**》”)出台，在法律层面正式提出个人信息保护领域的合规审计义务，到 2023 年《个人信息保护合规审计管理办法(征求意见稿)》公开征求意见，2024 年《网络数据安全管理条例》(“《**网数条例**》”)出台并且确认网络数据处理者的个人信息保护合规审计义务，再到近日《**审计办法**》正式落地，个人信息保护合规审计制度箭已在弦、蓄势待发。本文简要梳理《**审计办法**》下的审计要求，并且结合行业特点与实操为企业提出建议审计的操作建议。

一. 个人信息保护合规审计的目的

个人信息保护合规审计，既是《**个保法**》下的合规义务，也是企业个人信息保护合规性的有力证明。

首先，开展个人信息保护合规审计是个人信息处理者的法定义务。《**个保法**》第 54 条明确规定，“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。”《**个保法**》第 64 条，进一步针对“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”，相关监管部门可以“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。”《**网数条例**》第 27 条也明确规定了定期合规审计的义务。

.....
For more Llinks publications,
please contact:

Publication@llinkslaw.com

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

其次,开展个人信息保护合规审计有利于个人信息处理者证明自身已尽职开展个人信息保护,作为在发生网络安全事件时的抗辩。根据《个保法》第 69 条,“处理个人信息侵害个人信息权益造成损害,个人信息处理者不能证明自己没有过错的,应当承担损害赔偿等侵权责任。”也就是说,个人信息侵权责任采取的是“过错推定责任”,需要个人信息处理者自证清白,而个人信息保护合规审计的相关报告、法律意见书可以作为重要的证据。此外,个人信息保护合规审计的相关报告、法律意见书还可能在企业与商业伙伴的合作中、监管机构的调查执法中作为合规性证明发挥作用。

最后,同样重要的是,开展个人信息保护合规审计有利于企业梳理个人信息和数据处理活动,证明数据收集的合法和确定,并作为确权的基础,从而实现数据的资产化。作为一种新型的生产要素,数据的价值不言而喻。通过个人信息保护合规审计,企业能够梳理和规范化个人信息的收集、存储、使用、共享、删除等全生命周期,补救个人信息保护的漏洞,进而确认数据处理的合法性和权利属性,为未来的数据资产化奠定基础。

二. 个人信息保护合规审计的要点

《审计办法》及其附件《个人信息保护合规审计指引》(“《指引》”)为个人信息保护合规审计的开展提供了系统性、可操作性的规范指引,具体包括:

1. 定期审计

根据《审计办法》第 4 条的要求,“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。”针对未达到 1000 万人处理规模的个人信息处理者,《审计办法》暂未明确“定期”的期限,我们建议企业结合行业监管要求以及自身个人信息处理的情况综合确定。例如,《银行保险机构数据安全管理办法》第六十六条要求银行保险机构的审计部门每三年至少开展一次数据安全全面审计,发生重大数据安全事件后开展专项审计。

2. 审计主体

合规审计可由个人信息处理者的内部机构自行开展,或者委托专业机构。如果出现《审计办法》第 5 条所列的风险情况、个人信息安全事件的,监管机构有权要求个人信息处理者委托专业机构进行合规审计。律师事务所一般被认为是专业机构之一,律所出具的相关报告、法律意见书可以作为对企业个人信息保护水平的客观评价,也可以作为进一步企业合法开展个人信息处理活动的证据,以及数据资产化的基础。

3. 审计范围和要点

《指引》中详细列举了合规审计时的审查事项,基本与《个保法》、《网数条例》的要求对应,涵盖了个人信息处理的全生命周期,具体考察要点如下:

(1) 个人信息的处理规则(合法性基础、个人信息处理规则、告知义务、共同处理、委托处理、

合并/重组/分立/解散/破产等转移个人信息的、个人信息的提供、自动化决策、个人信息的公开、公共场所收集个人图像/身份识别信息的、已公开的个人信息、敏感个人信息、未成年人个人信息)

- (2) 个人信息的跨境提供(向境外提供个人信息的条件、基于司法执法的个人信息出境、是否涉及限制或者禁止个人信息提供清单)
- (3) 个人信息主体的权利保障(删除权、个人行使权利的保障、对个人信息处理规则解释说明)
- (4) 个人信息处理者的义务(个人信息安全内控管理、安全技术措施、个人信息保护负责人、个人信息保护影响评估情况、应急响应处置情况)
- (5) 大型互联网平台的个人信息保护特别义务(平台规则、个人信息保护社会责任报告)

4. 审计程序

《审计办法》并没有强制规定合规审计的流程,但是《**审计办法**》第8条明确,针对监管机构要求开展合规审计的,个人信息处理者应当为专业机构正常的审计工作开展“提供必要支持”。结合相关的国家标准和操作惯例,合规审计的流程一般包括:

- (1) 审计准备:即通过审计前的调查问卷、文件审查、问询、人员访谈等方式了解企业目前的个人信息保护情况,确定审计的方式方法(例如现场审计和非现场审计相结合),编制审计计划。
- (2) 审计实施:即实施人员访谈、现场调查等,收集审计材料、开展评价分析,撰写审计底稿。
- (3) 问题发现:即按照法律法规的要求和参照行业实操,对审计过程中发现的问题进行定性、分析和风险评估。
- (4) 出具审计报告:即在审计报告中对于审计概况、审计结论、审计发现的问题等进行说明,并且包括整改建议、整改情况的跟踪等。

5. 审计结果

审计报告是专业机构发表审计意见的书面文件,其中重点包括但不限于差异分析、整改建议、整改情况跟踪等。针对监管机构要求开展合规审计的,按照《**审计办法**》第9条、第10条的规定,需在限定时间内完成并且报送监管机构。

三. 建议

结合我们观察到的行业特点与实操,针对合规审计的开展简要提出建议如下:

1. 结合行业监管要求、业务特点和场景,有侧重地开展合规审计

除了《**指引**》中详细列举的审查事项之外,在开展个人信息保护合规审计需要考虑相关业务的业务特点和场景等因素,并结合相关行业的监管要求。

以银行保险行业为例，银保监在系统方面要求生产系统本地化部署，要求“有效的安全控制，包括内容过滤、访问控制和安全监控”；在数据方面要求，要求“对敏感级及以上数据.....制定用户对数据的访问策略，采取有效的用户认证和访问控制技术措施，.....进行日志记录，包括操作时间、用户标识”；对数据的外包管理，也有对服务提供商的“准入和安全管理。”

以证券基金行业为例，证监会对证券、基金行业的信息系统和数据从业务管理角度提出要求，比如要求生产环境与办公环境和互联网的隔离，要求“保存信息系统开发、测试、上线、变更及运维过程中产生的文档，并建立日志留痕机制，确保满足应急处置和审计需要”；对客户信息要求独立处理和不得分享的要求。

又例如，针对医药行业，尤其是临床试验，个人信息处理者需要结合《药物临床试验质量管理规范》（“GCP”）的要求，落实更加严格的知情同意要求、开展受试者隐私保护、确保电子数据管理系统的安全性和可靠性、遵守临床试验数据的最短保存期限等，而非仅仅对照《指引》中的审查事项开展审计。

2. 结合已开展的数据出境和其他活动的个人信息保护影响评估，更有针对性地开展合规审计

个人信息保护影响评估作为《个保法》第五十五条有关数据出境和其他数据处理活动的“事前”评估，与《审计办法》要求的“事后”合规审计，侧重点略有不同：个人信息保护影响评估侧重于事前的预防和风险识别，合规审计侧重于事后的监督、差异分析和整改。而在实施过程中，两者都涉及对于个人信息处理活动的全面梳理，并且相辅相成、共同构筑个人信息的保护体系。

对于已经开展数据出境活动、按照《个保法》第五十五条要求进行了个人信息保护影响评估的企业来说，个人信息保护影响评估为合规审计提供了良好的前期准备，使得合规审计更有针对性。例如，已经通过个人信息出境标准合同备案开展数据出境的，合规审计可以重点关注实际出境的场景、字段、规模等是否符合备案内容、是否存在需要补充或者重新备案的情况。再例如，企业为保障数据出境活动的安全，在数据传输过程采取了加密的技术措施并在个人信息保护影响评估中说明，那么合规审计开展时则可以重点检查实际操作中加密措施是否全面落实、强度是否能够确保传输安全和传输质量等。

3. 以合规审计为抓手，进一步提升企业合规水平

依据《审计办法》开展个人信息保护合规审计，并不是唯一的终点；该审计将进一步促使个人信息处理者提高合规水平，建立和完善个人信息保护的合规体系。对于很多企业而言，完成个人信息保护合规审计，不仅仅是满足合规义务，也可以是其经营活动中的卖点。

如您希望就相关问题进一步交流，请联系：



杨 迅

+86 21 3135 8799

xun.yang@llinkslaw.com

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