

通力合规评论(2024 年 11 月) 个人信息保护合规审计“风雨欲来”——你做好准备了吗？

自 2024 年 9 月 30 日《网络数据安全管理条例》公布以来，个人信息保护合规审计(“个保审计”)成为一个热点话题。越来越多的企业开始关注个保审计要不要做，谁来做，以及怎么做的问题。因此，在本期通力合规评论中，我们特以问答的形式，对企业关注的个保审计相关重点问题进行简要的回答¹。

1. 个保审计是一项法定义务吗？

- 2021 年生效的《个人信息保护法》(“个保法”)要求企业对个人信息处理活动进行定期审计，正式将个保审计确定为法定义务，但并未规定审计的细节要求
- 2023 年 8 月，国家网信办发布了《个人信息保护合规审计管理办法》(“个保审计办法”)的征求意见稿，规定了个保审计的实施细则
- 2024 年 7 月 12 日，全国网络安全标准化技术委员会公布了国家标准《数据安全技术 个人信息保护合规审计要求》的征求意见稿，对个保审计进一步提出细化要求
- 2024 年 9 月 30 日生效的《网络数据安全管理条例》再次重申数据处理者履行个保审计的义务
- 2024 年 11 月 12 日，全国网络安全标准化委员会在北京召开了《数据安全技术 个人信息保护合规审计要求》的试点启动会
- 个保审计自个保法以来已经是个人信息处理者的一项法定义务，随着网数条例对个保审计义务的重申以及审计标准的发布，个保审计即将迎来正式的政府监管和执法

2. 哪些企业要做个保审计？

- 所有个人信息处理者都要进行个保审计
- 根据个保审计办法：

处理超过 100 万人个人信息的个人信息处理者，应当每年至少进行一次个保审计

处理不满 100 万人个人信息的个人信息处理者，应当每两年至少进行一次个保审计

¹ 本快讯的起草基于截至定稿之日生效的法律、法规，标准，以及已发布但尚未生效的法律、法规和标准或其草案。相关草案正式发布后的要求可能会与本文所述有所不同。

- 根据《未成年人网络保护条例》：

处理未成年人个人信息的个人信息处理者应当每年进行个保审计

- 个保审计的主体原则上是“个人信息处理者”，而非受托处理方，但受托处理方可能需要协助个人信息处理者履行个保审计义务。此外，对于受托处理方作为个人信息处理者处理的个人信息部分(如其自身员工的个人信息)，受托处理方仍然需要进行个保审计

3. 个保审计应当由谁发起？

- 自行审计：由企业内部机构，或者企业自行委托第三方专业机构进行个保审计
- 监管审计：监管部门认为个人信息处理活动存在风险或者针对具体的个人信息安全事件，可以要求个人信息处理者进行个保审计

4. 哪个部门来主导个保审计？

- 尽管名称中带有“审计”，但个保审计与传统的(财务)审计有很大区别
- 个保审计要求审计者具备网络安全、数据保护以及 IT 技术相关知识和技能，而传统的审计人员(无论内部或外部)通常不具备这些知识和技能
- 如果有专门的内部数据合规部门，建议由数据合规部门主导个保审计工作；内部日常负责企业的数据合规工作的法务或合规部门也可作为主导部门
- 选择主导个保审计的部门应注意独立性问题，内部从事个保审计的部门应回避自身业务内容
- 对于监管审计而言，企业不得自行审计，只能委托第三方专业机构进行个保审计

5. 个保审计是否有时限的要求？

- 自行审计：没有时限的要求
- 监管审计：个保审计通常应该在 90 个工作日内完成，情况复杂的可适当延长

6. 个保审计结果是否需要向政府提交备案或审批？

- 自行审计：结果由企业自行保存，无需提交监管部门。但建议留存相关记录，以备监管监察
- 监管审计：第三方专业机构出具的审计报告需要报送监管部门。企业按照审计报告中的整改建议进行整改后，整改情况应报监管部门

7. 个保审计的范围是什么？

- 个保审计的本质是对企业个人信息全生命周期处理活动的合规性的检查
- 从未进行过个保审计的企业，建议对企业所有个人信息处理活动进行审计

- 已经进行过全面个保审计的企业，除根据法定的频率(一年一次或两年一次)进行后续的全面个保审计外，还建议在个人信息保护活动情况发生变化时(例如新增了个人信息处理活动)，针对变化的部分进行专项审计

8. 个保审计的要点是什么？

- 个人信息处理活动的合法性基础：同意？履行合同必要？履行法定义务？...
- 个人信息处理规则：形式与内容、是否履行告知义务
- 特殊情形的个人信息处理活动：共同处理个人信息、委托处理个人信息、对外提供个人信息、合并/分立等情形下的个人信息转移、自动化决策处理个人信息、公开个人信息、处理公开个人信息、处理敏感个人信息、处理未满十四岁未成年人的个人信息、向境外提供个人信息
- 个人信息主体权利的保障：具体权利的保障、对权利要求的响应
- 个人信息保护制度和组织架构的完善程度
- 个人信息保护所采取的技术措施
- 对于个人信息安全事件的应对：应急预案、响应情况
- 针对大型互联网平台运营者的特殊审计要点：独立机构、平台规则、对平台内运营者的监督、社会责任报告

9. 个保审计的流程是什么样的？

- 审计计划阶段：确定审计目标和范围、编制审计计划
- 审计准备阶段：建立审计团队、开展审计前调查、编制审计方案
- 审计实施阶段：收集审计证据、撰写审计底稿、确认审计发现
- 审计报告阶段：起草、交付审计报告
- 问题整改阶段：提出问题、整改问题、复核整改情况
- 档案管理阶段：审计相关文档的留存

10. 个保审计应该审计哪些内容？

- 内部制度：章程、企业规章、数据保护制度、标准
- 协议：隐私政策、用户协议、数据处理/共享协议、数据出境协议
- 工作档案：个人信息处理活动记录、个人信息保护影响评估记录
- 网络日志：系统访问日志、存储日志、传输日志、删除日志
- 资质证照：等级保护证书、个人信息标准合同备案证明、个人信息保护认证、数据安全认证
- 测试报告：漏洞检测报告、渗透测试报告、压力测试报告
- 人员访谈：通过与相关人员的访谈，了解个人信息保护的具体落实情况

我们希望本期合规评论能帮助您更好地理解个保审计并为实施个保审计做好准备。

如果您希望了解更多有关个保审计的信息，或者希望了解我们有关个保审计和网安数据领域的其他法律服务，欢迎与我们联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@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 2024