《个人信息保护合规审计管理办法（征求意见稿）》亮点导读

魏德华、李航程

《中华人民共和国个人信息保护法》（以下简称《个保法》）明确要求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；职责部门亦可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。国家互联网信息办公室起草的《个人信息保护合规审计管理办法（征求意见稿）》（以下简称《办法》）即是对《个保法》中合规审计要求的规则细化。

《办法》明确规定了开展合规审计的频次：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个人信息保护合规审计；其他个人信息处理者应当每二年至少开展一次个人信息保护合规审计。

《办法》将合规审计区分为自主审计和强制审计。
自主审计：个人信息处理者自行开展个人信息保护合规审计，由本组织内部机构或者委托专业机构开展。
强制审计：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，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。

《办法》未对自主审计作出细化规定，主要针对强制审计罗列了一系列要求。个人信息处理者在收到强制审计通知后应当尽快选定专业机构进行个人信息保护合规审计。关于专业机构的选定，《办法》第十三条指出，国家网信部门会同公安机关等国务院有关部门将建立个人信息保护合规审计专业机构推荐目录。专业机构应当保持独立性和客观性，且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。强制审计应当在 90 个工作日内完成，合规审计报告应当由合规负责人、专业机构负责人签字并加盖机构公章，报送相关职责部门。专业机构给出整改意见的，个人信息处理者应当依据整改意见进行整改，经专业机构复核后将整改情况报送职责部门。

《办法》另附有附件《个人信息保护合规审计参考要点》（以下简称《要点》），共计三十一条。《要点》以《个保法》等法律、行政法规和国家标准等强制性要求为依据列举了重点审查事项，为个人信息处理者开展合规审计活动提供参考，涵盖合法性基础、个人信息处理规则、涉及第三方处理者、自动化决策、公开个人信息、向境外提供个人信息、个人信息主体权利、个人信息处理者义务、针对大型互联网平台运营者的特别要求等各种个人信息处理活动情形。

《办法》尚处于征求意见稿阶段，未来正式稿或将更加细化和完善个人信息保护合规审计规则。《办法》征求意见截止时间为 2023 年 9 月 2 日。的近律师行将持续关注个人信息保护的立法状态，并对可能影响您业务的动态提供更新。如想了解个人信息处理风险管理的具体建议，请与我们联络。

欲了解更多资讯吗？

钟咏雪
合伙人
cynthia.chung@deacons.com
+852 2825 9297

朱敏慧
合伙人
machiuanna.chu@deacons.com
+852 2825 9630

陈艾姿
合伙人
elsie.chan@deacons.com
+852 2825 9604

廖海燕
合伙人
helen.liao@deacons.com
+852 2825 9779

麦思帆
合伙人
mark.stevens@deacons.com
+852 2825 5192

魏德华
资深顾问律师
edwarde.webre@deacons.com
+852 2825 9730