金融机构个人信息保护合规审计流程探索

作者：杨迅 | 夏雨薇

近年来，国家互联网信息办公室(“**网信办**”)逐步完善个人信息保护法律体系建设，多维度丰富个人信息保护立法的内涵。去年8月发布的《个人信息保护合规审计管理办法(征求意见稿)》(“**《合规审计办法》**”)，与多部个人信息相关的法律、法规、条例、国家标准有机衔接，意图规范了企业在其个人信息处理活动中的持续性监督与审查义务。

虽然**《合规审计办法》**尚在征求意见中，但是我们注意到不少金融机构，包括公募基金、保险等掌握大量个人信息的单位，已经开始着手准备个人信息合规审计。本文将结合我们观察到的金融机构的需求，介绍个人信息保护合规审计的常见问题。

一. 个人信息保护合规审计的目的

为什么要开展个人信息保护审计?

首先，显而易见，开展个人信息保护合规审计有益于发现个人信息保护中的漏洞，提高个人信息保护水平。对于掌握大量个人信息的公募基金、开展个人业务的保险公司而言，保护个人信息水平也可以是商业卖点之一。

其次，开展个人信息保护审计是公司尽职保护个人信息，反驳侵犯个人信息指控的抗辩。《个人信息保护法》第69条规定：“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。”换而言之，就个人信息侵权责任而言，法律采取的是“过错推定责任”，需要信息处理者自证清白，而个人信息保护合规审计，则可以作为重要的证据。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

最后，开展个人信息保护审计是一项合规要求。个人信息保护合规审计并非《合规审计办法》首创。《个人信息保护法》第 54 条要求，“*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*。”而《合规审计办法》则是对《个人信息保护法》下的审计要求的细化。

二. 个人信息保护合规审计的基本要求

《合规审计办法》对个人信息保护合规审计的要求体现在以下方面:

定期审计:《合规审计办法》规定，处理超过 100 万人个人信息的处理者，合规审计应每年至少一次。对于其他处理者，合规审计应每两年至少一次。对于已经运行的公募基金和开展个人业务的保险公司而言，100 万个人的标准很容易达到。

审计主体：个人信息处理者可由内部机构自行开展或委托专业机构开展合规审计；履行个人信息保护职责的部门(“**监管部门**”)同时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，其审计后出具的法律意见，被认为是对被审计企业个人信息保护水平的背书，以及对个人信息侵权指控的抗辩。

审计范围：《合规审计办法》提供了若干合规审计参考要点，这些要点覆盖个人信息处理全周期[1]，包括个人信息权益保障与个人信息安全内控管理部分。

审计方式：《合规审计办法》并没有规定具体的审计方式和范围。但列明了处理者被监管部门要求委托专业机构进行审计的，应当允许专业机构进行以下审计工作：包括对文件、资料的查阅和工作人员访谈，还需对处理活动所涉场所、信息系统、设备设施、活动数据和信息进行调查测试等[2]。至于其他没有被明确要求委托专业机构进行合规审计的处理者而言，前述审计方式同样具有指引价值。

审计结果：审计机构应当进行差异分析，出具审计报告。被监管部门要求委托专业机构进行审计的，需要出具正式的审计报告报送监管部门，整改情况同样需要报送监管部门。

合规审计义务的持续性质意味着企业需要一套落地的合规审计义务制度，结合企业的核心业务运营情况与企业信息安全工作建设情况，开展多部门配合，识别合规审计的重点场景，合理安排合规审计流程，高效反馈审计结果，排查个人信息处理活动风险。特别是，金融机构作为受监管机构，除一般的个人信息处理活动风险外，需兼顾重点考虑行业监管意见，兼顾信息技术管理工作的需求。基于此，我们也从金融机构个人信息处理活动视角出发，试探索金融机构落地个人信息合规审计制度的要点。

[1] 《个人信息保护合规审计管理办法(征求意见稿)》 附件：个人信息保护合规审计参考要点

[2] 《个人信息保护合规审计管理办法(征求意见稿)》 第八条 个人信息处理者按照履行个人信息保护职责的部门要求委托专业机构开展个人信息保护合规审计的， 应当保证专业机构能够正常行使下列权限(一)要求提供或者协助查阅相关文件或资料；(二)进入个人信息处理活动相关场所；(三)观察场所内发生的个人信息处理活动；(四)调查相关业务活动及所依赖的信息系统；(五)检查、测试个人信息处理活动相关设备设施；(六)调取、查阅个人信息处理活动相关数据或信息；(七)访谈与个人信息处理活动有关的人员；(八)就相关问题进行调查、质询和取证。

三. 识别重点审计场景

《合规审计办法》虽提供了“个人信息保护合规审计参考要点”，但这些要点在不同场景中应各有侧重，毕竟不同个人信息处理场景适用的合规义务不同、关注的合规风险不一。故合规审计的首要任务，应当是识别重点审计场景，进而筛选核心的合规审计参考要点，设计相适应的合规审计方案。就金融机构而言，我们认为可以从以下几个角度识别重点审计场景。

- **特殊处理渠道**：金融机构近年不断利用互联网拓展业务，建立移动应用端的金融服务端口，包括网页、App，公众号，小程序，H5 服务端口(统称“**移动客户端**”)。移动客户端处理个人信息近年来问题频发，受到多部门的重点关注。通过移动客户端提供服务的金融机构，需额外考虑移动客户端处理个人信息的法律要求与执法动态。

- **特殊信息类型**：除了一般性的针对敏感个人信息的要求外，金融机构处理部分敏感个人信息可能受到监管限制。例如，《证券期货业网络和信息安全管理办法》对金融机构处理敏感个人信息有特殊要求，不得将生物特征作为唯一的客户身份认证方式[3]；通过非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等敏感个人信息进行脱敏处理。[4]

- **特殊处理情况**：个人信息流转存在对外提供、委托处理、公开、共同处理、跨境传输等特殊情形，这些情形的法律要求皆不相同，还涉及到了金融行业的行业监管，例如针对所涉信息系统、传输渠道的安全措施，对信息科技外包或信息技术系统服务机构等的审查义务。

- **特殊处理方式**：部分金融机构可能利用特殊工具向客户提供服务并处理个人信息，例如提供智能投顾、智能问答机器人、个性化展示等的对客功能，此时金融机构极有可能受到《互联网信息服务算法推荐管理规定》，《互联网信息服务深度合成管理规定》等法律的监管，故需要进一步满足算法合规的相关义务。

- **特殊业务场景**：金融机构部分个人信息处理场景与公司业务和运营息息相关，例如客户身份识别、反洗钱风险筛查等。此时除了一般性的个人信息合规审计要点外，也需要协调并充分考虑金融行业的监管要求和行业特点。

四. 设计合理的审计方式

根据《合规审计办法》的要求[5]，当监管部门要求处理者委托专业机构进行合规审计时，专业机构可能涉及的合规审计工作范围不但包括核查公司文件、资料，采访工作人员，进行必要的质询和取证，

[3] 《证券期货业网络和信息安全管理办法》第 35 条 核心机构和经营机构利用生物特征进行客户身 份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息。

[4] 《证券期货业网络和信息安全管理办法》第 34 条 核心机构和经营机构通过短信、邮件等非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等敏感个人信息进行脱敏处理。

还需要有调查、检查、测试处理个人信息的场所、信息系统、设备设施和活动流程的权限。无论处理者的合规审计活动是否受到监管部门的直接要求，完整的合规审计工作范围可能包含以下部分:

- 现场访谈、了解和调查个人信息处理活动以及相关文件或资料;
- 了解公司处理个人信息的具体活动流程与处理场所;
- 调查处理个人信息的信息系统、相关设备设施的可用性;
- 核查涉及信息系统处理数据的情况例如网络日志、权限分配等记录。

金融机构本身涉及处理个人信息的业务系统较多，步骤复杂，其中不但涉及对于法律风险的判断，还包含了对信息系统、设备设施的技术检查与风险排查。在一年或两年至少一次的频率要求下，如何联合多部门，提高合规审计效率、合理规划合规审计的工作量也是一大难点。

例如，中国证监会起草的《证券期货业信息系统审计指南》等一系列文件，可以作为特定金融机构个人信息保护合规审计活动中“调查业务活动所依赖的信息系统”、“检查、测试个人信息处理活动相关设备设施”、“调取、查阅个人信息处理活动相关数据或信息”的具体工作指南。

此外，金融机构可以将金融机构已经存在的涉及信息系统的相关检查、审计以及报告纳入合规审计参考的文件范围内，减少对相关事实的反复确定以及对同一情形的重复核查。例如，根据《证券基金经营机构信息技术管理办法》的要求，证券基金经营机构委托信息技术服务机构提供产品或服务前，需要对相关机构进行内部审查，确定相关信息系统的安全合规性并形成审查意见。前述过程极有可能涉及金融机构和信息技术系统服务机构之间的个人信息流转，从而也成为了个人信息保护合规审计的必要部分。因此，金融机构内部对于信息技术服务机构产品或服务的内部审查工作，可以作为个人信息流转过程中的合规审查的重要参考材料。进一步地，金融机构定期进行的信息技术管理审计工作，重要信息系统投产及变更等评估工作时所形成的报告和工作文档也有助于具体分析处理个人信息所涉系统的事实情况。

五. 梳理合规要点

《合规审计办法》列举了上百项“个人信息保护合规审计参考要点”，但从考察对象上而言，合规审计大致可以归为以下两类。

1. 权益保护

权益保护重视处理者与个人信息主体的交互关系。例如，处理个人信息是否满足“合法性”“必要性”“正当性”要求，是否有一定的处理个人信息合法基础，个人信息处理规则是否完整，个人信息权益响应渠道是否通畅，如果涉及特别多渠道多层面的个人信息收集的，公司采取的合规方案是否满足每一个处理渠道的要求。

此外，涉及特殊个人信息处理的，例如使用算法、进行人脸识别验证的，是否可以满足算法合规、人脸识别合规的相关监管要求。

2. 内控管理

公司存储、内部运营大量个人信息时，需要有足够的管理措施、技术措施以预防个人信息的泄露、篡改、或损毁并确保所处理的个人信息的质量与准确性。

内控管理能力要求公司有合理的个人信息保护组织架构与内部个人信息保护政策。从实操层面考虑，公司至少应当有成熟的个人信息保护委员会与负责人，明确划分各类个人信息的归口部门以及其所对应的管理职责。

在管理流程上，金融机构需要有安全事件应急预案、个人信息分类管理、个人信息保护影响评估等的相关流程。除此之外，公司还需要采取配套的风险监测、网络防护、传输存储加密等必要的技术措施。

从系统设置上，金融机构的也有一定的隔离要求，比如保险中介机构的信息系统和客户信息和关联机构的隔离，基金公司的投研系统和 OA 系统的隔离等。

六. 及时评估整改

根据《合规审计办法》的规定，被监管部门要求委托专业机构开展合规审计的个人信息处理者，需要在指定时间(90 个工作日)内完成审计，且审计报告以及对应的整改情况均需报送履行监管部门。对于其他处理者而言，虽没有硬性的报送要求，但并不能排除监管部门会不时核查各机构的个人信息保护合规审计开展情况。此外，正如第一部分所述审计报告也是信息处理者没有过错的证据。

所以，建议金融机构除了定期进行合规审计，还应当保留合规审计进行的底稿、合规审计报告，并据此制定针对性的合规审计问题与整改清单。问题与整改清单补单能够清晰呈现合规审计中公司存在的个人信息处理风险，还能帮助金融机构更好把握责任部门的整改方向与整改进度，有效提高合规审计的效率与成果。

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	北京	深圳
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	伦敦	
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	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