银行个人信息保护合规体系构建要点分析(下)

2023-08-07

银行个人信息保护合规体系构建要点分析的上篇，笔者主要阐述了银行从内部制度建设出发，应当制定齐备的合规文本与建立完整授权体系。但因银行所掌握的个人金融信息蕴含巨大的商业价值，所以经常会面临数据泄露的风险以及与其他机构合作进行数据共享的情形。在这两类情形中，依法保护客户的个人信息安全、合规使用客户的个人信息是极为重要的。笔者将在下文详细介绍如何应对数据泄露以及防范数据共享风险并对监管机构在监督检查过程中重点关注的敏感个人信息、责任人制等几个方面予以阐述，以期帮助银行更好的进行客户个人信息保护，并将银行的合规风险降到最低。

三、应对数据泄露

银行作为“强合规”的代表，走在数据合规的第一线，但因用户的个人金融信息蕴含巨大的商业价值，一些商业机构或个人受自身利益驱使，会采取种种手段获取他人的金融信息，并催生了大量的数据灰色产业链。金融行业敏感信息泄露常见手段有黑客攻击、内部管理不善、内部人员作案等。银行一旦发生数据泄露事件，则将面临十分严厉的处罚结果。为应对数据泄露风险，银行可从以下两个方面着手进行建立防护机制。

第一，强化技术防护。建立全领域、纵深化的网络安全防御体系保护核心数据资产安全，通过在网络、系统、终端、应用等不同层面分别部署异构网络安全防御系统和工具，并集中纳入SIEM平台进行统一管控，防止金融信息等核心数据被非法窃取；持续完善数据泄露体系建设，通过重要文档加密、邮件过滤、终端保护等手段进行多层次、立体化的访问控制和数据保护；部署数据安全交付平台，确保科技部门向业务部门交付的金融数据不落地，不分流；建立统一的业务数据脱敏机制，保障测试数据和大数据平台的安全使用。

第二，规范人员管理。银行应对员工进行规范化管理，如对入职员工进行必要的背景调查，与个人金融信息处理职责相关的员工签订保密协议、员工离职后应立即收回访问权限，并再次明确告知有关信息保密的义务；落实以分级授权为核心的客户金融信息使用管理制度，严格控制员工的信息接触权限，规定无关人员不得以营销为目的，查询和复制客户个人金融信息，并严格规范接触客户信息的岗位范围和查询权限；对员工开展定期的“为客户保密”专项培训，提高从业人员金融信息保护意识和能力。

四、防范数据共享风险

客户个人信息的开发和共享，有利于降低市场交易成本和提升交易效率。但值得注意的是，一定要充分保障客户的知情权和决定权，在“共享客户信息”时，应当确保依法合规、风险可控并经客户书面授权或同意，防止客户信息被不当使用。

（一）集团或关联公司使用

在欧洲的全能银行制度下，一个法人主体可以从事不同种类的金融业务，个人信息可以在法人内部无障碍流动，被运用于不同的金融业务。但在我国分业经营情况下，银行收集的个人信息，要想被同一个集团内部的保险公司、证券公司运用，则需要经个人授权同意。

我国银行收集的信息在由集团或关联公司使用时应当注意满足以下要求：（1）在首次收集个人信息时，银行应当根据公开、透明原则，履行数据共享的告知、说明、披露义务。在网站首页或APP显著位置向用户清晰、明了地告知其数据可能

与金融控股公司及其子公司共享，包括共享的范围、目的和保存期限等，；（2）个人信息仅限被用于为各方持有的“金融许可证”所载明的经营范围之内的目的，因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意；（3）要注意个人信息处理者内部在共享和转让过程中的具体技术要求，例如开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益；应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺；部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。

（二）第三方机构使用

随着银行网上应用功能的日益丰富，软件开发工具包（SDK）越来越多地集成到了银行网络金融应用中。《银行第三方软件开发工具包（SDK）安全接入指南》第5条中明确SDK按照集成、工作方式可分为无交互类SDK（SDK完全嵌入到宿主应用中）、推送类SDK（SDK由嵌入到宿主应用部分和第三方服务端部分组成）和交互服务类SDK（SDK由嵌入到宿主应用部分和后台服务器部分组成），对于不同类型的SDK，银行应当采取差异化的安全规定。

无交互类SDK均由银行进行个人信息的收集、处理等行为，而对于推送类SDK和交互服务类SDK，会产生由第三方SDK进行个人信息收集、存储、使用等情形，会存在个人信息泄露或被违法使用的风险。故银行在选择选择SDK服务前，应调查第三方能力、信用，在确保金融信息安全前提下，和第三方签订保密协议，或是在服务协议中约定保密条款，设置信息共享“隔离带”。对于由第三方SDK为用户提供的服务，并且应当向客户明确标识由第三方提供并详细披露第三方公司名称、服务范围、个人信息处理目的等情况，保证出现问题后，能够及时追究第三方责任。

（三）合作方使用

为激活数据要素潜能、挖掘业务场景，银行可能会与第三方数据公司收集的个人信息进行汇聚融合,形成更多个人信息标签，如银行可能会将自有数据与电商、医疗等其他行业的数据融合,实现联合建模,构建更加精准的营销和风控模型。如确需进行数据共享的，银行应当充分重视信息安全风险，注意满足以下要求：

第一，遵循“告知-同意”原则。应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的名称、共享内容、使用用途、个人金融信息主体的权利等情况，只有在事先征得个人金融信息主体明示同意，才可共享、转让。

第二，部分数据限制共享、转让。银行对于传输至第三方的信息要按照最小范围、业务必须开展，严格控制超范围传输信息至第三方。对于用户C3类别信息以及C2类别信息中的用户鉴别辅助信息不应共享、转让。

第三，第三方能力评估。银行应对第三方进行个人金融信息接收方信息安全保障能力评估，确保其满足个人信息接收方准入和评价标准。同时，对于从合作方获取的个人信息应确认其来源合法，防止合作方违规引发银行业金融机构声誉危机或法律风险，通过协议明确双方职责和保密义务及违约责任。

五、其他

除以上要点之外，银行还应当对监管机构在监督检查过程中重点关注的敏感个人信息、责任人制、紧急处理机制、风险评估机制等方面予以高度重视，积极建立或完善相应的合规机制，以期更好的进行用户个人信息保护，并将银行的合规风险降到最低。

（一）注重敏感个人信息保护

严格落实个人信息分类分级保护制度。银行业金融机构应根据《个人信息保护法》的规定，结合《个人金融信息保护技术规范》、《金融数据安全　数据安全分级指南》等行业标准，实施个人金融信息分类分级保护措施，提高信息安全水平。特别提醒的是，敏感个人信息的衍生信息依然为敏感信息，应按照正确的分类分级采取保护措施。

（二）建立责任人制

银行应当建立责任人制度，由个人信息保护负责人对个人信息处理活动以及采取的保护措施等进行监督，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。应当注意，责任人是指银行应当设立相应的岗位，而并非具体的人员。设立个人信息保护负责人对企业落地数据合规制度至关重要，个人信息保护负责人既可以帮助企业在日常工作中未雨绸缪又可能在危机事件中力挽狂澜，提高企业防御风险的综合能力。

（三）建立紧急处理机制

银行应当将个人金融信息泄露等相关事件处理纳入机构信息安全事件应急处置工作机制，制定专门的流程和预案，定期评估应急处理流程和预案，及时、有效应对个人金融信息安全事件，降低安全事件造成的损失及不利影响。我国《个人信息保护法》第57条规定，在发生或可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知监管部门。以用户个人信息泄露为例，银行要制定相应的处理机制，第一步是要件减损，针对性的采取措施防止个人信息泄露损失进一步扩大，如因黑客入侵所致，则应当立即修复安全系统，清除病毒、恶意软件，更改密码等；第二步是向监管部门汇报并在需要的情况下配合监管部门的调查取证，第三步是采取纠正改正措施，及时对相关漏洞通过流程完善或技术加强等措施进行填补；第四步则是积极承担相应责任，绝不推诿逃避。

（四）建立风险评估机制

风险评估机制是指若银行遇到个人金融信息泄露等安全事件，银行要能够自身或者委托第三方机构评估再扩大风险。在出现个人金融信息泄露事件，造成一定经济损失（或社会影响）时，银行应自身或及时委托外部安全评估机构对本次风险事件进行相关安全评估与检查，同时制定补救措施、更新应急预案，防止风险的进一步扩散。倘若银行未事先建立风险评估机制，在出现问题时则难以把控，很容易出现陷入舆论漩涡等情况。如银行某员工离职时拷贝客户信息到一家理财公司，并用利用其拷贝的客户信息进行营销，被客户举报，此时再由银行行长牵头组建风险处置小组，对该问题进行处理，寻找解决办法则是非常被动的。

总结

银行作为受到严格监管的持牌经营机构，其行业特点造就其具有做好风险管理工作、维护机构良好社会形象的义务，而个人金融信息的保护正是风险管理工作中举足轻重的一环。银行应当在思想上高度重视客户信息保护，加强宣传教育，将保护个人信息的理念内化于心；同时围绕本文列举的要点，通过持续完善内部治理框架和优化技术措施等手段进行个人信息保护合规体系化建设，不断改进银行个人信息合规体系，持续提升银行的个人信息保护水平。

来源：

作者：肖斌 李茜

肖斌
合伙人

+8610 6184 8045
xiaobin@tiantailaw.com

相关标签

银行与金融