21 世纪经济报道/2022 年/11 月/1 日/第 008 版
金融科技

个保法落地一周年

金融业数据合规缓慢推进　呼吁出台行业细则

本报记者　李览青

2022 年 11 月 1 日，《中华人民共和国个人信息保护法》（以下简称“ 个保法 ”）正式实施一周年，金融行业客户个人信息权益保护进一步加强。

在金融领域，2022 年 1 月 1 日起《征信业务管理办法》正式实施，今年 8 月银保监会下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，对金融机构个人信息权益保护也提出新要求。

一年来，随着有关部门对金融机构数据安全、个人信息保护、消费者权益保护的监管趋严，在合规前提下开展数据治理成为金融机构的必答题。

据 21 世纪经济报道记者多方了解，以银行保险为主的金融机构正在完善数据治理机制、数据分类分级制度、信息科技外包风险管理、APP 个人信息保护、金融消费者权益保护等一系列制度，并展开前沿金融科技应用，但金融行业数据合规落地工作依然道阻且长，行业呼吁个保法的金融业细则出台。

在金融信息合规逐步缓慢推进的当下，金融机构数据合规现状如何？以银行为代表的金融机构在近一年来如何应对个保法落地？金融科技手段为个人金融信息保护提供哪些新解法？

金融数据合规监管趋严

金融机构的个人信息合规治理并非一夕之功。在个保法正式落地前，央行就已对个人金融信息制定相关技术规范。

2020 年 2 月，中国人民银行正式下发《个人金融信息保护技术规范》，对个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化。规定个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，以标准化文件规范个人金融信息安全管理，保障个人金融信息主体合法权益。

此后，监管层又相继出台《金融数据安全 数据安全分级指南》《金融科技创新安全通用规范》《人工智能算法金融应用评价规范》《金融数据安全 数据生命周期安全规范》，以及在近日出台《金融领域科技伦理指引》，一系列标准化文件都对金融机构数据安全保护与个人权益保护提出要求。

今年 8 月，银保监会印发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求各银行保险机构全面摸排本机构自 2021 年以来与消费者个人信息处理活动相关的经营行为和管理情况，深入查找本机构个人信息保护方面存在的问题，列出问题清单，自查过程中要坚持立查立改。各银行保险机构应于 9 月 20 日前完成自查整改工作，并书面报告属地银保监局。

“ 从监管举措及机构实践来看，以商业银行为典型，个人金融信息保护和金融消费者保护工作很早就已开展，个保法存在大量合规要求，对从业机构的业务流程、内控治理、外部响应等多方面提出了多且严的要求。” 金诚同达律师事务所高级合伙人彭凯律师告诉记者，金融业的数据安全与个人信息保护，以《数据安全法》《个人信息保护法》为分水岭，逐步从既往的“ 消保 ”“ 系统安全 ” 等标签中分离，演化为“ 金融数据安全 ” 和“ 个人金融信息保护 ” 两大板块并自成体系。

在严监管下，今年 1 月伊始，东亚银行就因违反信用信息采集、提供、查询及相关管理规定被罚 1674 万元。

事实上，仅从今年上半年金融机构收到的罚单来看，与信息处理、个人信息保护相关的罚金总额就已超过 2021 年全年。

21 世纪经济报道记者结合企业预警通数据不完全统计，2022 年上半年，银行、保险、信托、汽车金融、第三方支付等机构收到相关罚单 66 张，处罚金额合计 6409.34 万元（相关统计表格见文末）。而记者年初统计的 2021 年全年相关罚单罚款金额合计约 4654 万元。

具体来说，在信息安全保护方面，金融机构出现的违规行为包括违反信用信息采集、提供、查询及相关管理规定，信息科技风险管理不到位；在个人信息权益保护方面，包括对提供个人不良信息未事先告知信息主体本人、未建立以分级授权为核心的消费者金融信息使用管理制度，未明示收集、使用消费者金融信息的目的、方式和范围。

数据合规难言“已有大成”，呼吁行业细则出台

“金融行业数据合规落地工作在缓慢而坚实地推进，目前来看难言‘已有大成’，但机构的合规投入与监管政策都在持续加码。”彭凯表示。

目前以银行保险业为主的金融机构，为进一步达到个保法要求，在数据合规方面的探索包括：金融类 APP 数据合规、数据分类分级制度、数据合规制度建设、开展个人信息保护影响评估、人脸识别合规、金融消费者信息安全教育等。

“现在个人信息保护、数据安全合规是银行展业的底线红线，各家机构都在强化，但涉及面很广，要全面堵塞漏洞道阻且长。”华东某银行金融科技部门相关人士向记者表示，目前银行的相关机制建设愈加完善，包括成立数据治理委员会，制定数据分类分级、消费者保护等管理办法，同时持续开展数据保护宣贯教育等。

一位从事金融行业超过 20 年的技术架构专家告诉记者，金融机构近两年增加了数据隔离措施，例如将退出客户的信息打标，不使其进入人工智能训练的数据集，完善 APP 的开发要求等。“但更细节的落实举措，还要等待央行的个保法行业细则出台。”他向记者坦言。

在记者的采访中，多位采访对象提到，期待针对金融行业的个人信息保护规范出台。

彭凯向记者介绍，从既往金融行业信息安全相关罚单来看，较多地与“金融消费者保护”“外包机构管理”“征信违规”等问题交织在一起。但从 2021 年开始发生了变化，诸如信息收集、信息保护机制不健全之类的问题开始出现在处罚案例中，但依据《数据安全法》《个人信息保护法》（以下简称“相关法律”）进行处罚的案例尚未见到，不过这其实并非金融行业所特有，全行业来看，依据相关法律进行处罚的案例都是极为少见的。

“从立法情况来看，我国并未专门对金融领域的个人信息保护进行立法。虽然《中国人民银行法》《商业银行法》《证券法》《保险法》等金融领域基本法律法规都涉及个人金融信息保护内容，但总体上金融业尚未形成完整统一的个人金融信息保护规范，因此针对行业的个人金融信息相关活动的监管依据较为薄弱。”马上消费金融研究院相关人士表示。

值得关注的是，据记者了解，2020 年末，时任央行副行长陈雨露公开透露，国家正在制定个人信息保护法和数据安全法，下一步，中国人民银行会根据国家将要颁布的个人信息保护法、数据安全法等新的法律，及时推出《个人金融信息保护暂行办法》。由央行牵头的该暂行办法，在 2019 年曾有过内部征求意见稿，但至今尚无更新消息，2022 年的央行工作计划也删掉了这一条例。

新兴科技能否成为新解法？

对于尚未迎来细分行业管理办法的金融业而言，数据安全领域的新兴技术正在成为市场热点。

据记者了解，近两年在数据安全保护应用的热门技术包括区块链、DLP（数据防泄露）与隐私计算等。

隐私计算解决了数据“可用不可见”的问题，区块链与隐私计算技术的联合应用，实现多方合作的可信网络，同时可以解决中心依赖、单点诈骗的问题，同时，在个保法“专数专用”“可

算不可识”匿名化的要求下，基于密态计算的隐私计算帮助机构在数据合规的前提下进一步挖掘数据价值。

而 DLP 产品为数据生命周期中的数据传输、数据存储环节提供了针对性的防控手段，配合数据脱敏、数据加密、数据访问控制等数据安全组件、产品，构建数据安全的技术底座。

此外，超自动化流程也成为近两年资本关注的热点。在数据采集、数据传输、数据分析等流程上，以 RPA 机器人代替人工可以在一定程度上杜绝人为操作风险。“过去一些银行业务可能需要人工进行审核、复审，如运营管理部通过员工完成转账流程，需要一系列信息审核，一旦相关员工出现道德风险，可能会引发数字资产或客户信息泄露。”弘玑解决方案及卓越运营总监梁一纲告诉记者，RPA 机器人可以在自动化前提下完成跨流程节点、跨部门的工作流程，从而规避人工带来的部分道德风险。

不过人为带来的风险问题并不能完全依靠技术解决。

“知易行难，金融机构数据安全保护最大的风险在于人。”前述华东某银行金融科技部门人士坦言，健全的数据治理机制与新兴科技手段可以在一定程度上规避人为的道德风险，但难以完全“根治”。

以隐私计算为例，其本身不能解决个人信息保护中的“告知同意”等问题，只是加强了信息和数据互联互通的安全性。

某四大行科技部门相关人士告诉记者，该行隐私计算技术的应用痛点是机构之间数据开放意愿不足，该行实际应用的场景主要是在集团内部子公司之间。

“长期以来，隐私计算一揽子解决个人信息保护合规问题的认知是偏颇的。”彭凯表示，部分金融机构隐私计算的前沿应用仍在央行的监管沙盒体系下进行。