金融业数字化转型合规“金”点
——从《关于银行业保险业数字化转型的指导意见》说开去

作者：潘永建 | 朱晓阳 | 王雪莹 | 左嘉玮

近日，为推进金融机构的数字化转型，中国银行保险监管委员会(“银保监会”)印发了《关于银行业保险业数字化转型的指导意见》(“《意见》”)。《意见》指出，各机构应当加强风险管理，特别是应当强化网络安全防护以及加强数据安全和隐私保护。本文中，通力大合规团队将探讨银行保险业机构面临的主要网络安全与数据合规挑战，以期帮助企业在数字化转型的落地过程中，有效防范、化解数字化条件下的各类合规风险。

一. 《意见》概览

近年来，随着金融科技的发展，银行保险业机构逐步推进了数字化场景运营体系建设，在数字化转型方面取得了一定的进展。为强化顶层设计，加强政策规范，银保监会于近日出台了《意见》，以期在机制、方法和行动步骤等方面予以规范和指导。

《意见》包括总体要求、战略规划与组织流程建设、业务经营管理数字化、数据能力建设、科技能力建设、风险防范、组织保障和监督管理等七部分，共三十条内容。除了建设技术能力之外，《意见》对银行保险机构的组织和管理能力也提出了明确要求：各机构应加强顶层设计和统筹规划，改善组织架构和机制流程；健全数据治理体系，增强数据管理能力，加强数据质量控制，提高数据应用能力；加强战略风险、创新业务的合规性、流动性风险、操作风险及外包风险等管理，同时防范模型和算法风险，强化网络安全防护，加强数据安全和隐私保护。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

二. 金融业数字化转型合规要点

近年来，我国相继颁布了《网络安全法》《数据安全法》《个人信息法》三部核心法律，配套的行政法规和规范性文件也正在陆续制定之中，网络空间治理的法律框架基本形成。金融机构在数字化转型过程中，强化网络安全防护，加强数据安全和隐私保护是企业依法应当履行的义务，围绕这一点，《意见》强调了若干具体的法定义务。

金融机构进行业务创新和数字化转型固然值得鼓励，但作为服务国家、社会、大众的重要企业类型，其遭遇网络安全事件的危害后果往往远超金融机构本身的利益，而是可能会影响到国家安全、社会利益及民众权益，因此金融机构在数字化转型的过程中，尤其需要注重网络安全防护，履行网络安全义务。结合《意见》，我们提示企业应对下述网络安全及数据合规义务应当进行重点关注:

1. 网络安全等级保护

根据《网络安全法》，国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行网络安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。为推进数字化转型，各机构的业务信息均以数据的形式保存在各类信息系统中。因此，在建设、运营、维护和使用系统的过程中，企业应当切实履行网络安全保护义务，主要包括:

- 确定网络安全负责人，落实网络安全保护责任。
- 建立完善的网络安全事件管理制度、形成完整的书面制度。
- 监测、追踪网络活动和事件，并保存网络运行日志不少于 6 个月;
- 网络产品、服务以及网络关键设备和网络安全专用产品应当符合国家标准的强制性要求。
- 制定应急预案，根据预案及时处置安全风险并按照规定向有关主管部门报告。

同时，金融业所涉系统如果受到破坏，可能对公民、法人或其他组织的合法利益造成较为严重的侵害，通常定级会达到三级或以上。企业应当根据《信息安全技术 - 网络安全等级保护基本要求》及其相关国家标准文件的要求，聘请专业评测机构协助测评并向公安机关备案。

2. 关键信息设施运营者(“CIIO”)

根据《网络安全法》，对于金融等其他 7 个重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，国家在网络安全等级保护制度的基础上实行重点保护。《关键信息基础设施安全保护条例》提出，相关主管部门应当结合本行业、本领域实际情况，制定关键信息基础设施认定规则，根据认定规则负责认定本行业、本领域的关键信息基础设施，并将认定结果通知相关运营者。

鉴于金融行业已明确被列为七大重要行业之一，大型银行、保险机构及掌握大量个人信息的金融企业有较大的可能性被主管部门认定为 CIIO。一旦如此，则相关企业在履行网络运营者的一

般安全保护义务的基础上，还需履行 CIIO 的特殊义务，主要包括:

- 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施规划、建设、使用“三同步”;
- 在网络安全等级保护基础上，在责任主体界定、从业人员教育培训、容灾备份、应急预案等方面履行特别保护义务;
- 采购网络产品和服务履行国家安全审查义务，并与提供者签订安全保密协议;
- 重要数据和个人信息境内存储，出境应当安全评估;
- 建立健全安全评测制度，定期对关键信息基础设施进行检测评估;
- 按照法律要求，使用商用密码保护关键信息基础设施。

关于各项义务的具体内容和相应的法律责任，请见通力法评“《关键信息基础设施安全保护条例》企业合规速览”。

3. 数据分类分级管理

《数据安全法》明确，国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

因此，企业应当根据法律法规及企业自身实际情况，对所掌握的数据进行分类，并在分类的基础上，根据不同类别数据的重要程度及“灾害后果”严重程度，实施不同级别的管理措施。对于所涉的个人信息、重要数据，向境外提供时应遵循国家相关规定和相关标准的要求。

根据《数据安全法》，将由国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，各地区、各部门确定的重要数据具体目录。目前，相关目录尚未正式出台，国家标准《信息安全技术 重要数据识别指南(征求意见稿)》的给出了重要数据的定义，“指以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据”，并在“重要数据的识别因素”中列举了重点企业的金融交易数据，可供企业参考。此外，信安标委发布的《网络安全标准实践指南—网络数据分类分级指引》附录 C.3 和中国人民银行发布的《金融数据安全 数据安全分级指南》(JR/T 0197—2020)给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，可作为企业建设数据分类分级制度的参照。在需要的情况下，可以通过与行业主管部门积极沟通，以更好地履行重要数据的合规义务。

值得注意的是，银行业机构未履行网络、数据安全相关的合规义务还可能同时被认定为“严重违反审慎经营规则”，从而被行业主管部门根据《中华人民共和国银行业监督管理法》进行处罚。

江苏银保监局行政处罚信息公开表

(江苏江南农村商业银行股份有限公司)

行政处罚决定书文号			苏银保监罚决字〔2020〕20号
被处罚当事人	个人	姓名	
		单位	
	单位	名称	江苏江南农村商业银行股份有限公司
		法定代表人姓名	陆向阳
主要违法违规事实（案由）			网络安全工作严重不足
行政处罚依据			《中华人民共和国银行业监督管理法》第四十六条第（五）项
行政处罚决定			罚款人民币30万元
作出处罚决定的机关名称			中国银行保险监督管理委员会江苏监管局
作出处罚决定的日期			2020年6月16日

行政处罚决定书文号			银保监罚决字〔2021〕1号
被处罚当事人	单位	名称	中国农业银行股份有限公司
		法定代表人姓名	周慕冰
主要违法违规事实（案由）			（一）发生重要信息系统突发事件未报告 （二）制卡数据违规明文留存 （三）生产网络、分行无线互联网络保护不当 （四）数据安全管理较粗放，存在数据泄露风险 （五）网络信息系统存在较多漏洞 （六）互联网门户网站泄露敏感信息
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条第五项和相关审慎经营规则
行政处罚决定			罚款420万元
作出处罚决定的机关名称			中国银行保险监督管理委员会
作出处罚决定的日期			2021年1月19日

4. 个人信息保护义务

金融业作为数据密集型行业，在生产经营过程中积累了海量的数据资源。为推进数字化转型，企业需要通过信息技术挖掘数据价值，为业务赋能。例如，基于用户画像洞察客户需求、开展智能个人金融产品营销和服务、通过联邦学习技术建立 AI 模型实现风控管理等。其中，若涉及用户个人信息处理，必须依法履行《个人信息保护法》规定的义务。

1) 遵守最小化原则，避免过度收集

《个人信息保护法》要求，处理个人信息应当与处理目的直接相关，采取对个人权益影响最小的方式。《个人信息安全规范》对该项法律规定作出了补充说明:

- 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现;
- 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率;
- 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

此外，其他多个部门规章、国家标准也对此予以明确(尽管关注点大多落在 App 合规)，例如《常见类型移动互联网应用程序必要个人信息范围规定》以及《移动互联网应用程序个人信息保护管理暂行规定》(征求意见稿)等。金融企业在落实最小化原则时可以参考上述要求和标准，避免收集与产品和服务不相关的用户个人信息，且不得欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息。

例如，在移动金融类 APP 权限获取方面，建议企业参考《网络安全标准实践指南—移动互联网应用程序(App)系统权限申请使用指南》，不建议企业收集用户 GPS、短信等功能产生的个人信息，尤其是短信权限。用户的短信可能涉及的内容广泛，银行实时消费余额提醒、医疗挂号排队回执、快递物流最新位置等短信都零散地潜藏着用户信息，当零碎的信息累积达到一定的数量，信息的可识别性会大大提升。

2) 处理生物识别信息的特殊要求

根据《个人信息保护法》，生物识别信息属于敏感个人信息，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下方允许处理。

同时，《个人信息保护法》规定国家网信部门未来将对人脸识别、人工智能等新技术、新应用制定专门的个人信息保护规则、标准。随后颁布的《上海数据条例》规定，公共场所或者区域，不得以图像采集、个人身份识别技术作为出入该场所或者区域的唯一验证方式。《网络数据安全管理条例(征求意见稿)》进一步规定，数据处理者利用生物特征进行个人身份认证的，应当对必要性、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个人身份认证方式，以强制个人同意收集其个人生物特征信息。

出于保护用户财产等目的，金融企业倾向于在各类信息系统中使用人脸、指纹作为用户登录的验证方式。但是，相关信息的收集和使用并非严格的充分必要，因为从理论上来说，使用密码、短信验证等方式也可以实现处理目的。如确需利用生物识别信息进行验证，结合《个人信息保护法》及相关标准，我们建议企业应当注意以下要求:

- 通过弹窗、即时提示等方式，就生物识别信息的收集和使用征得用户的单独同意;
- 避免将生物识别作为唯一的验证方式，为用户提供其他替代选择;

- 原则上不应存储原始个人生物识别信息(除非获得个人的单独书面授权)，可仅存储仅存储个人生物识别信息的摘要(特征)信息 ；
- 采取安全措施存储和传输生物识别信息，方式包括但不限于：加密存储和传输人脸信息，采用物理或逻辑隔离方式分别存储人脸信息和个人身份信息等。

3) 用户画像与自动化决策

金融企业通过收集用户各类基础数据，对用户进行分类并画像，从而进行精准营销并提供个性化的产品和服务，这种应用模式在行业中已是常态：银行根据客户的风险偏好、风险承受能力、资产基础等，向客户量身推荐个性化的理财产品和银行服务；第三方支付平台如支付宝，参考用户消费频率、网购金额、转账记录、会员等级等，决定花呗的消费限额。

在用户画像为企业带来营销便利的同时，须注意《个人信息保护法》和国标《个人信息安全规范》对用户画像的使用提示:

- 应当在个人信息保护政策中明确披露，收集个人信息是否将用于形成直接用户画像及其用途;
- 利用个人信息进行自动化决策的，应当保证自动化决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇;
- 在用户同意的使用目的之外，使用个人信息时应消除明确身份指向性，尽量使用群体画像而非个体画像;
- 在依据用户画像进行信息推送、商业营销时，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式;
- 有义务就个人提出的、有关自动化决策影响其个人权益的决定予以说明，并提供替代性措施。

4) 超范围使用数据

2022 年 3 月 2 日，中国人民银行长沙中心支行发布的处罚信息显示，邮储银行湖南省分行因“未经书面同意查询个人征信信息”、“未经消费者申请、授权或同意擅自收集、使用消费者个人金融信息办理 ETC 业务”等多项违规行为被处以 187.7 万的罚款，相关责任人员一同受罚。

《个人信息保护法》对企业提出“公开个人信息处理规则，明示处理的目的、方式和范围”“个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意”等要求，旨在约束企业在约定/法定范围内处理个人信息。行业法规层面，为规范金融机构使用金融信息(尤其是个人信息)的行为，《中国人民银行金融消费者权益保护实施办法》要求“银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用”；《征信业务管理办法》进一步强调“信息使用者应当……保障查询个人信用信息时取得信息主体的同意，并且按照约定用途使用个人信用信息”。我们提示企业，

由于金融相关的个人信息于个人权益的影响较大，业务过程中宜谨慎处理，确保处理活动(的目的、方式和范围)已获得相关个人信息主体的同意或存在其他合法性基础。

5) 数据的汇聚融合

为激活数据要素潜能、挖掘业务场景，企业将所有或部分关联企业，以及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的需求旺盛。就信息的汇聚融合问题，提请企业注意以下方面:

- 应确保汇聚融合的数据来源的合法性。建议企业与第三方数据公司签署的合作协议中要求第三方数据公司承诺其已获得个人信息处理的授权同意范围，且授权同意的范围包括与第三方数据汇聚融合并用于合作目的，企业在条件允许的情况下应对第三方数据公司的个人信息保护政策或相关授权文件进行核查确认;
- 汇聚融合的数据不应超出收集时所声明的使用该范围。因业务需要确需超范围使用的，应再次征得个人信息主体明示同意;
- 应根据汇聚融合后的个人信息类别及使用目的，开展个人信息安全影响评估，并采取有效的技术保护措施。

2022 年 1 月 10 日，东亚银行因违反信用信息采集、提供、查询及相关管理规定被中国人民银行上海分行处以罚款人民币 1674 万元，责令限期改正。值得一提的是，这是 2022 开年以来央行系统开出的第一张千万级别银行罚单。

序号	当事人名称（姓名）	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	东亚银行（中国）有限公司	上海银罚字〔2022〕3 号	违反信用信息采集、提供、查询及相关管理规定。	处以罚款人民币 1674 万元，责令限期改正。	中国人民银行上海分行	2022 年 1 月 6 日	

2021 年 8 月，交通银行、华夏银行、兴业银行因违反信用信息采集、提供、查询及相关管理规定，分别被中国人民银行处以罚款 62 万元、486 万元、5 万元。同时，直接责任人员也被给予警告并处罚款。

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	交通银行股份有限公司	银罚字〔2021〕23号	违反信用信息采集、提供、查询及相关管理规定。	罚款62万元	中国人民银行	2021年8月13日	
2	沈奕栋（时任交通银行太平洋信用卡中心风险管理和控制部操作风险管理团队经理、资深综合管理顾问）	银罚字〔2021〕24号	对交通银行以下违法违规行为负有责任：违反信用信息采集、提供、查询及相关管理规定。	罚款7万元	中国人民银行	2021年8月13日	

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	华夏银行股份有限公司	银罚字〔2021〕25号	违反信用信息采集、提供、查询及相关管理规定。	罚款486万元	中国人民银行	2021年8月13日	

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	兴业银行股份有限公司	银罚字〔2021〕26号	违反信用信息采集、提供、查询及相关管理规定。	罚款5万元	中国人民银行	2021年8月13日	

在上述邮储银行湖南省分行的处罚决定中，除银行本身被处以 187.7 万元罚款以外，未经书面同意提供查询个人征信信息的直接责任人员(副行长、查询授权员和征信查询员)也分别被处以 4000 元人民币的罚款。

三. 结语

《意见》要求，到 2025 年银行业保险业数字化转型取得明显成效，数字化经营管理体系基本建成，数据治理更加健全，科技能力大幅提升，网络安全、数据安全和风险管理水平全面提升。在接下来的几年时间中，金融机构在根据《意见》指引，积极推进数字化转型合规体系建设的过程中，务必要注意各项网络安全及数据合规义务的落实，以有效防范数字化转型过程中的风险。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@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