保险行业数据安全布局策略

程战战 | 资深互联网保险人士

第一章　背景情况

金融数据安全治理

合规性要求

国家和行业监管机构对金融数据安全有严格的法律法规要求，金融机构必须严格遵守，以避免法律风险和行政处罚。

维护金融系统稳定

数据安全事件可能导致金融系统中断、资金损失，甚至引发系统性风险，金融数据安全治理是维护金融系统稳定运行的关键。

防范金融犯罪

通过加强数据安全治理，可以有效防范和打击金融欺诈、洗钱等金融犯罪活动，保障金融市场的健康发展。

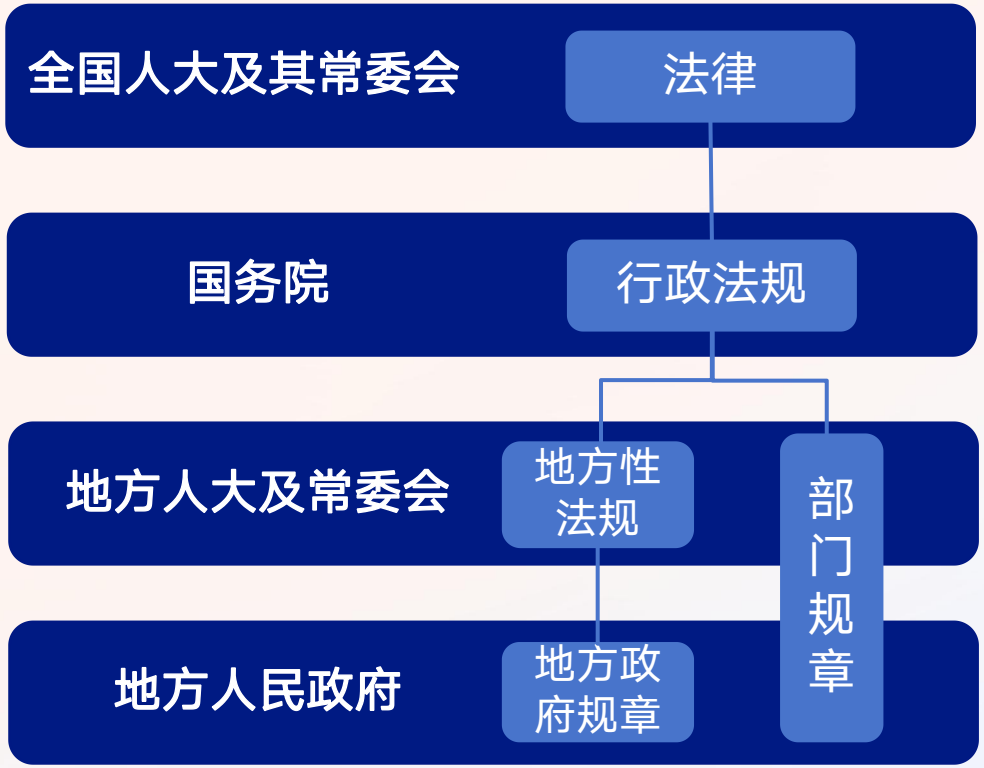
保护客户隐私和提升信任度

良好的数据安全治理能够提升客户对金融机构的信任度，提高客户满意度和忠诚度，有助于机构的长远发展。

支持业务创新和数字化转型

数据安全治理为金融机构开展创新业务和推进数字化转型提供坚实的基础，确保在引入新技术和业务模式时，数据安全能够得到充分保障。

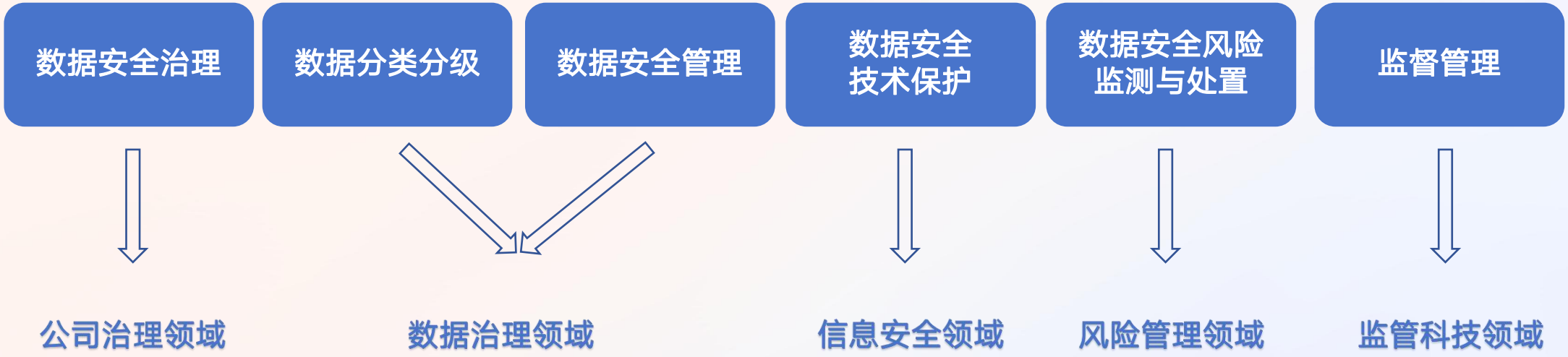
国内不断健全完善的数据合规、数据安全法律法规体系



法条名称	发布机构	施行时间
《中华人民共和国网络安全法》	**全国人大常委会**	**2017/06/01**
《儿童个人信息网络保护规定》	网信办	2019/10/01
《中华人民共和国密码法》	全国人大常委会	2019/10/16
《关键信息基础设施安全保护条例》	国务院	2021/09/01
《中华人民共和国数据安全法》	**全国人大常委会**	**2021/09/01**
《中华人民共和国个人信息保护法》	**全国人大常委会**	**2021/11/01**
《网络安全审查办法》	网信办	2022/02/15
《数据出境安全评估办法》	网信办	2022/09/01
《个人信息出境标准合同办法》	网信办	2023/07/01
“数据要素x”三年行动计划(2024-2026年)	国家数据局	2023/12/31
《促进和规范数据跨境流动规定》	网信办	2024/03/22
《银行保险机构数据安全管理办法》	**金融监管总局**	**2024/12/27**

第二章 数据安全管理办法认识心得

框架解读和分析


数据安全治理
数据分类分级
数据安全管理
数据安全
技术保护
数据安全风险
监测与处置
监督管理
公司治理领域
数据治理领域
信息安全领域
风险管理领域
监管科技领域

1. 数据安全治理

第九条

银行保险机构应当建立覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的**数据安全管理组织**架构，明确岗位职责和工作机制，落实资源保障。

第十条

银行保险机构应当建立**数据安全责任制**，党委（党组）、董（理）事会对本单位数据安全工作负主体责任。银行保险机构主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人，**明确各层级负责人的责任，明确违规情形和责任追究事项，落实问责处置机制**。

第十二条

银行保险机构应当按照“**谁管业务、谁管业务数据、谁管数据安全**”的原则，明确各业务领域的数据安全管理责任，落实数据安全保护管理要求。

工作一 制度建设

1. 建立《数据安全管理办法》(总纲)。
2. 建立数据安全责任制。
3. 数据安全管理职责落实到董事会/党委会。
4. 明确各业务部门承担数据安全责任。

工作二 会议组织

1. 制度发布通过董事会。
2. 定期汇报机制。

工作三 协同机制

1. 数据安全与信息科技组织从属关系。
2. 数据安全与风险管理协同机制。

第十一条

银行保险机构应当指定**数据安全归口管理部门**，作为本机构负责数据安全工作的主责部门。其主要职责包括：

（一）组织制定数据安全管理原则、规划、制度和标准；

（二）组织.....

第十四条

银行保险机构信息科技部门**是数据安全的技术保护主责部门**，其主要职责包括：

（一）建立数据安全技术保护体系，建立数据安全技术架构和保护控制基线，落实技术保护措施。

（二）制定.....

落实方式一 信息安全全部主责

优势：统一管理，信息安全传统防护经验经过扩展应对数据方面防护较为得心应手。

劣势：对数据管理和评估领域不熟悉，专业跨度大。

落实方式二 数据管理全部主责

优势：数据安全评估工作和数据治理具有高度相似性，人员技能相近。

劣势：传统数据人员面对传统安全领域，专业跨度更大。

落实方式三 分工协同

劣势：具有较多的交叉领域。

2. 数据分类分级

识别重要数据，有效管控

分类分级数据安全体系的基石，它决定了数据安全管理策略的制定和执行。

数据分类标准

一级分类	二级分类	说明
客户数据	个人数据	个人自然信息、个人身份鉴别信息、个人标签信息等
	单位数据	单位基本信息、单位身份鉴别信息、单位标签信息等
业务数据	保单数据	保单基本信息数据、保单标的信息、核保信息、批改信息等
	理赔数据	理赔案件信息、理赔调查信息、赔付结果信息等
	再保险数据	再保险合同信息、再保险业务明细信息、再保险赔案信息、再保险账单信息等
	交易信息	交易通用属性信息、收付费信息等
经营管理数据	财务数据	财务收支、预算及费用分配等
	营销服务	产品信息、渠道信息、品宣信息等
	运营管理	客户服务信息
	综合管理	战略规划、招聘信息、员工信息、培训信息、机构信息、办公数据
	风险管理数据	风险损失数据、风险限额、风险模型、内控管理数据
	投资数据	投资管理数据
	法律合规数据	合同管理、机构与个人处罚等数据
	监管数据	数据报送、数据收取
系统运行	系统运行数据	项目管理信息、系统管理信息、科技外包信息等
安全管理	安全管理数据	安全管理信息

数据分级标准

数据安全级别	具体特征
核心数据	核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。
重要数据	特定领域、特定群体、特定区域或者达到一定精度和规模的数据，一旦被泄露或者篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全
敏感数据	一旦被泄露或篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或对组织自身或公民个体造成严重影响的数据
一般数据	除以上数据之外的数据为其他一般数据

3. 数据安全管理

以数据安全治理为主

第二十一条	银行保险机构应当**建立企业级数据架构**，统筹开展对全域数据资产登记管理，**建立数据资产地图**，以数据分类分级为基础明确数据保护对象，围绕数据处理活动实施安全管理。

步骤一 建立数据资产地图

打好基础

第二十三条	银行保险机构应当**建立企业级数据服务管理体系，制定数据服务规范，建立专职数据服务团队**，统筹内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动。
第二十九条	银行保险机构应当对**数据共享使用进行集中安全管控，明确企业级数据共享策略**，评估数据共享使用的必要性、合规性、安全性及伦理道德规范的符合度。 银行保险机构应当建立银行母行、保险集团或者母公司与其子行、子公司数据安全隔离的“防火墙”，并对共享数据采取有效保护措施。银行保险机构与其母行、集团，或者其子行、子公司共享敏感级及以上数据，应当获得数据主体的授权同意，法律、行政法规另有规定的除外。不得以数据主体拒绝同意共享敏感数据而终止或者拒绝单家子行、子公司对其提供金融服务，所共享数据属于提供产品或者服务所必需的除外。

步骤二 建立数据服务管理

1. 数据服务规范
2. 专职数据服务团队
3. 数据共享策略

第三十条	银行保险机构在**委托处理数据时**，应当明确所涉数据外部使用和处理的条件、场景、方式。委托处理数据时，应当以合同协议方式约定委托处理的目的、期限、处理方式、数据范围、保护措施、双方的数据安全责任和义务，以及受托方返还或者删除数据的方式等，**对数据处理活动进行记录和审计**，可对外公开披露的数据除外。银行保险机构应当要求受托方在未取得其同意时，不得转委托其他主体处理数据，不得对外共享数据，不得加工、训练、挪用数据，或者采取其他形式处理数据以谋取合同或者协议约定以外的利益。
第三十一条	银行保险机构应当将**数据委托处理纳入信息科技外包管理**范围，在实施过程中不得将信息科技管理责任、数据安全主体责任外包，涉及信息科技战略管理、信息科技风险管理、信息科技内部审计及其他有关信息科技核心竞争力的职能不得外包。供应链服务中涉及敏感级及以上数据处理的，银行保险机构应当加强对供应商的准入和安全管理。
第三十二条	银行保险机构与第三方机构进行**数据共同处理**时，应当按照“业务必要授权”原则制定方案并**采取有效管理和技术保护措施确保数据安全**，并以合同协议方式明确双方在数据处理过程中的数据安全责任和义务。
第三十三条	银行保险机构因合并、分立、解散、被宣告破产等需要转移数据的，应当明确数据转移内容，通过协议、承诺等方式约定数据接收方全面承接对应数据的安全保护义务，通过公告等方式告知数据主体。**数据转移**应当采用安全可靠方式进行，并确保转移过程可追溯。
第三十四条	银行保险机构向外部提供敏感级及以上数据，应当取得数据主体同意，法律、行政法规另有规定的除外。除国家机关依法履职外，银行保险机构核心数据跨主体流动应当按照国家相关政策要求通过风险评估、安全审查。
第三十五条	银行保险机构应当**建立对外公开披露数据的审批机制**，研判可能产生的影响，数据公开应当在机构官方渠道进行发布，确保数据真实、准确、防篡改，记录审批和发布情况。 敏感级及以上数据不得公开，法律、行政法规另有规定或者取得数据主体授权同意的除外。
第三十六条	银行保险机构**向境外提供**在中华人民共和国境内运营中收集和产生的重要数据和个人信息，应当承担数据安全主体责任，并按照国家有关政策要求进行安全评估。

步骤三 数据安全流程治理

1. 数据委托流程
2. 数据共同处理流程
3. 数据转移流程
4. 数据出境流程
5. 公开披露审批机制
6. 数据委托纳入外包管理

4. 数据安全技术保护

数据安全技术保护 - 体系建设

第三十九条	银行保险机构应当建立针对大数据、云计算、移动互联网、物联网等多元异构环境下的**数据安全技术保护体系，建立数据安全技术架构，明确数据保护策略方法**，采取技术措施，保障数据安全。
第四十条	银行保险机构应当将**数据安全保护纳入信息系统开发生命周期框架**，针对敏感级及以上数据明确安全保护要求，实现数据安全保护措施与信息系统的同步规划、同步建设、同步使用。
第四十一条	银行保险机构应当将**数据纳入网络安全等级保护**。银行保险机构应当根据数据安全级别，划分网络逻辑安全域，**建立分区域数据安全保护基线**实施有效的安全控制，包括内容过滤、访问控制和安全监控等，确保相关措施满足处理和存储最高级别数据的网络安全策略和数据安全保护策略要求。
第四十一条	存放或者传输敏感级及以上数据的机房、网络应当实施重点防护，设立物理安全保护区域，对网络边界、重要网络节点进行安全监控与审计。
第四十二条	银行保险机构应当将敏感级及以上**数据纳入信息系统保护**。在数据全生命周期内采取有效的访问控制管理措施，对于不同区域流转和共享中的数据，应当实施同等水平的安全防护措施。
第四十三条	银行保险机构应当严格实施对敏感级及以上数据的管理，**制定用户对数据的访问策略**，采取有效的用户认证和访问控制技术措施，规范数据操作行为，用户对数据的访问应当符合业务开展的必要要求并与数据安全级别相匹配。
第四十五条	敏感级及以上数据应当实施数据容灾备份，定期进行数据可恢复性验证
第四十八条	系统投产上线前应当开展安全测试，确保各项安全要求落实，有效防范数据安全风险。测试环境应当与生产系统隔离，敏感级及以上数据原则上未经脱敏处理不得进入测试环境，防止数据泄露。

项目一　建立数据安全保护体系

1. 重构网络区域，适应不同数据级别应用系统
2. 各类安全产品规划，包括权限控制、审计等
3. 制订应用系统相应的数据安全标准基线
4. 差异化防护措施

项目二　适应数据安全的SDLC

1. 项目阶段确定是否涉及数据共享、数据委托
2. 需求阶段确定数据分类分级、敏感数据保护要求
3. 开发阶段落实传输加密、存储加密、展示脱敏
4. 测试阶段落实数据安全专项测试用例
5. 上线阶段落实加密验证、日志记录、隐私协议

项目三　扩大等级保护范围

1. 将数据平台纳入等级保护范围。
2. 按照数据分类分级标准，规划等保范围，将“重要数据”相关系统纳入等保范围。

项目四　灾备体系升级

1. 明确将敏感级及以上数据纳入灾备体系。

数据安全技术保护 - 专项防护工具(1)

第四十四条	银行保险机构敏感级及以上**数据传输**应当采用安全的传输方式，保障数据完整性、保密性、可用性。 银行保险机构之间进行数据交换时，参与数据交换的相关机构应当采取有效措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性。
第四十五条	银行保险机构应当对敏感级及以上数据采取**安全存储措施**，防止勒索病毒、木马后门等攻击。
第四十五条	**个人身份鉴别数据不得明文存储**、传输和展示。
第四十七条	银行保险机构应当开展**数据安全的技术基础设施建设**，支持用户身份管理、数据匿名化、行为监测、日志审计、数据虚拟化等功能的组件化、服务化，保障安全标准在信息系统中执行的一致性。
第四十九条	银行保险机构应当对**大数据平台**采取高可用设计、安全加固、数据备份等措施进行重点保护。
第四十九条	应当**建立大数据服务访问授权机制，动态监测与审计大数据访问行为**。

API接口安全监测工具

数据安全技术保护 - 专项防护工具(2)

第四十四条	银行保险机构敏感级及以上**数据传输**应当采用安全的传输方式，保障数据完整性、保密性、可用性。 银行保险机构之间进行数据交换时，参与数据交换的相关机构应当采取有效措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性。
第四十五条	银行保险机构应当对敏感级及以上数据采取**安全存储措施**，防止勒索病毒、木马后门等攻击。
第四十五条	**个人身份鉴别数据不得明文存储**、传输和展示。
第四十七条	银行保险机构应当开展**数据安全的技术基础设施建设**，支持用户身份管理、数据匿名化、行为监测、日志审计、数据虚拟化等功能的组件化、服务化，保障安全标准在信息系统中执行的一致性。
第四十九条	银行保险机构应当对**大数据平台**采取高可用设计、安全加固、数据备份等措施进行重点保护。
第四十九条	应当**建立大数据服务访问授权机制，动态监测与审计大数据访问行为**。

数据库敏感信息识别工具

建设目的 自动识别数据库敏感级数据

1. 敏感级数据识别，是数据安全防护、加密、防泄漏的基础。
2. 数据识别范围应该全面，覆盖IT系统全部数据库。
3. 识别速度应该快速，第一时间掌握准确数据。
4. 识别准确性必须高，否则失去了自动化的意义。

项目三 技术要求

1. 数据表覆盖全部，数据进行抽样。
2. 新旧数据识别。
3. 具有识别错误修正机制。

针对对象 全部数据存储

1. 常见关系型数据库。Oracle/DB2/MySQL/OB
2. NoSQL。ES/Redis/MongoDB
3. 大数据平台。
4. 文件日志。

项目四 应用范围

1. 数据暴露面分析。
2. 高权限账号预警。
3. 敏感数据自动屏蔽。
4. 自动化提取数据。

数据安全技术保护 - 通用防护工具

第四十四条	银行保险机构敏感级及以上**数据传输**应当采用安全的传输方式，保障数据完整性、保密性、可用性。银行保险机构之间进行数据交换时，参与数据交换的相关机构应当采取有效措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性。
第四十五条	银行保险机构应当对敏感级及以上数据采取**安全存储措施**，防止勒索病毒、木马后门等攻击。
第四十五条	**个人身份鉴别数据不得明文存储**、传输和展示。
第四十七条	银行保险机构应当开展**数据安全的技术基础设施建设**，支持用户身份管理、数据匿名化、行为监测、日志审计、数据虚拟化等功能的组件化、服务化，保障安全标准在信息系统中执行的一致性。
第四十九条	银行保险机构应当对**大数据平台**采取高可用设计、安全加固、数据备份等措施进行重点保护。
第四十九条	应当**建立大数据服务访问授权机制，动态监测与审计大数据访问行为**。

工具1 数据库审计软件

检测并保存所有数据库操作SQL 。

- 对于发现误操作、非法操作、入侵、溯源帮助很大。
- 产品较成熟，实施难度小。
- 对于交易频繁的数据库需考虑存储问题。

工具2 数据库加密软件

对数据库内容自动加密。

1. 字段级加密和全库加密。
2. 如果能够稳定全面实施，对于数据保密作用很大。
3. 并非数据库原生功能，实施风险大、难度大。

工具3 数据库动态脱敏软件

在数据库直接使用者和数据库之间加了一层脱敏，使用者直接看到脱敏后的信息。

- 避免管理员，数据维护人员看到/下载敏感信息，减少泄露。
- 实施难度较小。
- 对于不同类型的数据库，各种特性的SQL，适应能力有限。

工具4 数据库静态脱敏软件

将生产环境数据批量脱敏后导出，导入测试环境。

1. 对于建立测试环境很有帮助。
2. 数据脱敏后，须能够维持生产环境的关联关系，否则测试环境无法使用。

工具5 数字水印软件

在电脑上无论传送文件还是打印，均带有姓名、IP等水印信息。

- 对于重要数据操作岗位，防止数据任意拷贝及打印。
- 根据不同场景，水印有多种形式。

工具6 数据防泄漏软件

监测终端数据泄露情况并预警。

1. 规则设置与维护对可用性影响较大。
2. 研判预警与阻断相结合。
3. 软件影响范围较大。

5. 数据安全风险监测与处置

第六十四条

银行保险机构应当将数据安全风险**纳入本机构全面风险管理体系**，明确数据安全风险监测、风险评估、应急响应及报告、事件处置的组织架构和管理流程，有效防范和处置数据安全风险。

工作1 纳入全面风险管理体系

- 数据安全风险指标制订
- 风险指标收集与监测
- 定期风险报告
- 风险处置机制

第六十六条

每年开展一次数据安全风险评估。
审计部门应当每三年至少开展一次数据安全全面审计，发生重大数据安全事件后应当开展专项审计。

工作2 数据安全评估专项
审计专项

- 要求简单而明确

第六十五条

银行保险机构……。监测内容包括：
（一）超范围授权或使用系统特权账号；
（二）内部人员异常访问、使用数据；
（三）对数据集中共享的系统或平台的网络安全、数据安全威胁；
（四）敏感级及以上数据在不同区域的异常流动；
（五）移动存储介质的异常使用；
（六）外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改；
（七）客户有关数据安全的投诉；
（八）数据泄露、仿冒欺诈等负面舆情；
（九）其他可能导致数据安全事件发生的情况。

工作3 数据安全监测体系

- 网络
- 应用系统
- 移动介质
- 客户
- 舆情

第六十八条

银行保险机构应当建立数据安全事件应急管理机制，建立机构内部协调联动机制，建立服务提供商、第三方合作机构数据安全事件的报告机制，及时处置风险隐患及安全事件。
（一）制定数据安全事件应急预案，定期开展应急响应培训和应急演练。
……

工作4 数据安全应急机制

- 应急演练制度
- 应急演练活动

6. 监督管理

第七十一条	国家金融监督管理总局按照国家数据分类分级要求，制定银行业保险业重要数据目录，提出核心数据目录建议，监督指导银行保险机构开展数据分类分级管理和数据保护。银行保险机构应当按要求向国家金融监督管理总局或者其派出机构**报送重要数据目录**。重要数据目录发生重大变化应当及时报备更新后的数据目录。
第七十三条	涉及**批量敏感级及以上数据的数据共享、委托处理、转让交易、数据转移，银行保险机构应当在处理、合同签署前二十个工作日向国家金融监督管理总局或者其派出机构报告**，法律、行政法规另有规定的除外。
第七十四条	银行保险机构应当于每年1月15日前向国家金融监督管理总局或者其派出机构**报送上一年度数据安全风险评估报告**，报告内容包括数据安全治理、技术保护、数据安全风险监测及处置措施、数据安全事件及处置情况、委托和共同处理、数据出境、数据安全评估与审查情况、数据安全相关的投诉及处理情况等。

三项工作

- **报送重要数据目录**
- **批量敏感级及以上数据活动上报**
- **报送上一年度数据安全风险评估报告**

结束语

数据保护始于心

数据安全践于行

谢谢观看