数据安全意识培训

客户版

中国外贸金融租赁有限公司

2026年1月

目录

01

章节 PART

开篇：为何数据安全 “无小事”？

2020年3月30日，中共中央、国务院印发**《关于构建更加完善的要素市场化配置体制机制的意见》**，首次明确数据成为继土地、劳动力、资本、技术之外的**第五大生产要素**，这也预示着加快构建数据基础制度体系，促进数据要素市场培育，已经成为我国数字化改革发展的重要方向。

《关于构建更加完善的要素市场化配置体制机制的意见》

生产要素

土地　劳动力　资本　技术　**数据**





推进政府数据开放共享

优化经济治理基础数据库，加快推动各地区各部门间数据共享交换，制定出台新一批数据共享责任清单。

提升社会数据资源价值

培育数字经济新产业、新业态和新模式，支持构建农业、工业、交通、教育、安防、城市管理、公共资源交易等领域规范化数据开发利用的场景。

加强数据资源整合和安全保护

探索建立统一规范的数据管理制度，提高数据质量和规范性，丰富数据产品。

“数据”作为第五大生产要素，只有**流动、分享、加工处理**才能创造价值。数据安全是数据走向开放共享过程中的基础与必要保障！

数据：是指任何以电子或者非电子形式对信息的记录。《数据安全法》《银行保险机构数据安全管理办法》
业务数据：指中国人民银行业务领域内产生和收集的不涉及国家秘密的网络数据。《业务领域数据安全管理办法》
网络数据指是指通过网络处理和产生的各种电子数据。《网络数据安全管理条例》

电子形式	非电子形式
数字文件：如文档（Word、PDF）、表格（Excel）、图片（JPG、PNG）、音频（MP3）、视频（MP4）等。 数据库：存储在服务器中的结构化数据（如用户信息、交易记录）。 电子存储介质：硬盘、U盘、光盘、云存储（如百度云、阿里云）等。	纸质记录：书籍、合同、笔记、报纸、档案袋等。 物理介质：胶片（老照片、电影胶片）、石刻、竹简、石碑、绘画（壁画、油画）等。

数据安全，是指通过采取必要措施，**确保**数据处于有效保护和合法利用**的状态，以及保障**持续安全状态的能力

保密性

工作中接触到的敏感数据要保密，不能泄露给他人，例如银行客户联系名单、客户交易流水、公司财务信息等。

完整性

工作中不能未授权修改客户资料、篡改交易日志等。

可用性

工作中不能未授权删除客户资料或者是非法破坏数据文件，导致其不可用。

监管要求：2025年，全国多地央行分支机构密集公布对金融机构的行政处罚决定。从披露案例来看，数据安全管理缺失、网络防护漏洞、征信违规成为三大高频雷区，最高单笔罚款超百万元。这些案例再次敲响警钟：在数字化加速推进的今天，数据安全已成为金融机构的生命线！

如客户的姓名、身份证号码、联系方式、账户信息等，这些信息直接关系到客户的个人隐私和财产安全，是银行必须严格保密的内容。

计算机系统、网络架构、加密技术等方面的信息，这些技术是银行开展业务的基础，一旦泄露可能被黑客/黑产利用，影响银行的业务和数据安全。

银行的各类业务交易数据、财务数据、风险管理数据等，这些数据对于银行的经营决策和风险控制具有重要意义，泄露可能导致银行的利益受损。

金融业综合统计数据、监管报送、反洗钱等数据，监测经济运行、评估政策效果、预警潜在风险的核心工具。数据安全漏洞可能导致监管部门无法准确识别风险信号，延误处置时机，甚至引发系统性风险。

案例警示

某农商行

- 提供个人不良信息未事先告知本人
- 未采取防计算机病毒技术措施
- 未保障数据安全
- 未开展风险评估和报送

（13项违规丨罚48.3万）

金融监督管理局

信息科技风险监管
业务合规监管
银行业保险机构数据安全监管办法

公安部

等级保护测评
护网
重保

JRT 0071-2020
金融行业网络安全等级保护实施指引

人民银行

金融行业标准制定
支付系统安全监管
征信合规监管
业务领域数据安全管理办法

JR/T 0171—2020
个人金融信息保护技术规范
JR/T 0223-2021
金融数据安全 数据生命周期安全规范
JR/T 0197-2020
金融数据安全 数据安全分级指南
金融数据安全 数据安全评估规范（征求意见稿）

工信部

移动APP个人信息保护监管

GBT 41391-2022
信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

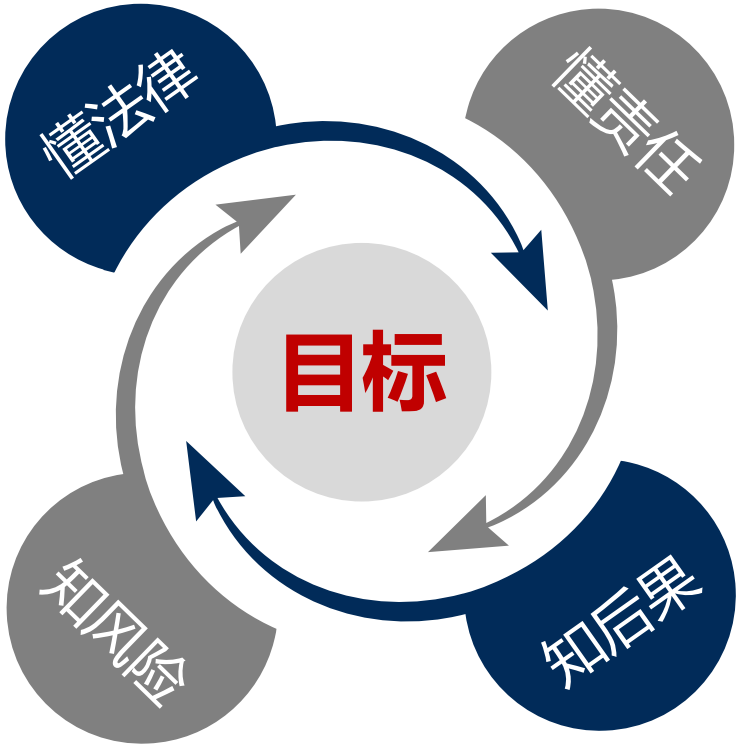
网信办

数据安全合规统筹协调

数据安全管理条例
数据出境安全评估办法

掌握数据安全核心法规要求，数据收集的合法性、存储的安全性、使用的合规性等方面的具体操作边界，确保每一项数据活动都有法可依、有规可循，从根源上筑牢合规防线。

识别日常工作中的高风险行为，例如私下拷贝敏感数据、使用公共网络处理涉密信息，还是纸质文件随意堆放等看似微小的行为，都可能成为数据泄露的突破口，均需要懂得识别这些风险点



依据“谁主管谁负责、谁经手谁负责” 的原则，了解本岗位数据安全责任，数据处理人员要严格按流程操作敏感信息，技术人员需确保防护系统稳定运行。

落实 “预防为先、违规必究” 的安全理念，通过培训案例分享形成警示效应。让安全理念渗透到每一个工作细节，形成 “人人重视安全、人人维护安全” 的良好氛围。

02

章节 PART

法规红线：国家行业法律法规要点速递

网络安全法

数据安全法

个人信息保护法

对数据安全和个人信息保护制度作了基本规定。

网络数安条例

由国家网信办制定，国务院签发，三法配套的行政法规，对相关制度规定予以细化、补充、完善。

中国人民银行 THE PEOPLE'S BANK OF CHINA

《中国人民银行业务领域数据安全管理办法》

国家金融监督管理总局

《银行保险机构数据安全管理办法》

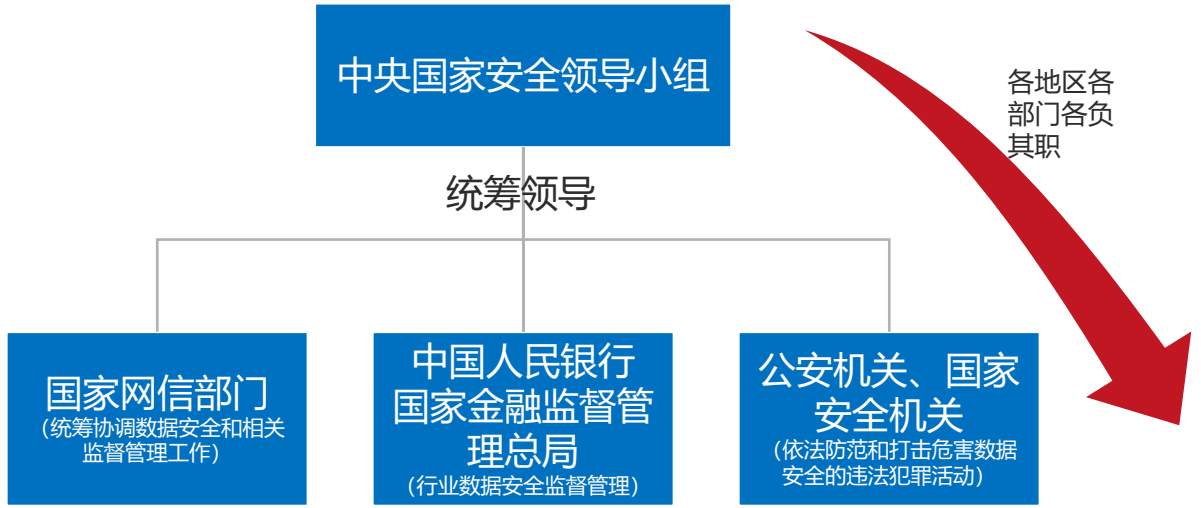
《数据安全法》

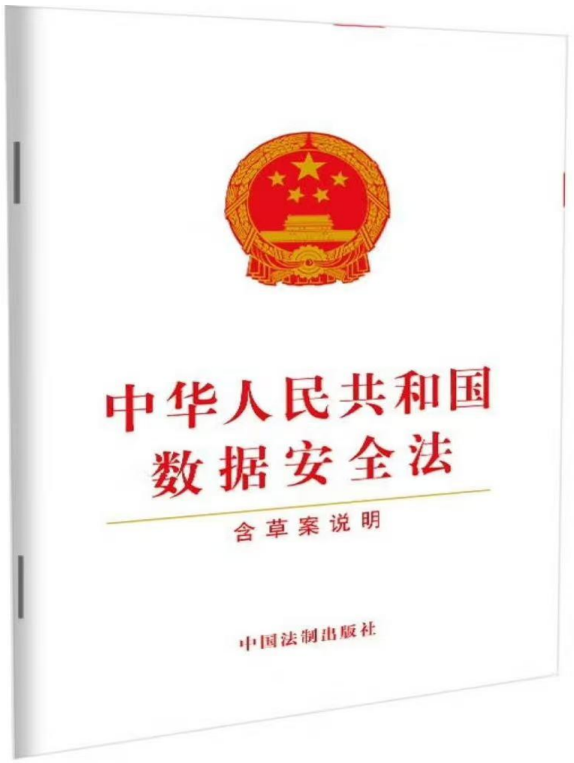
第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项 和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中产生、汇总、加工的数据及数据安全 负主体责任。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。



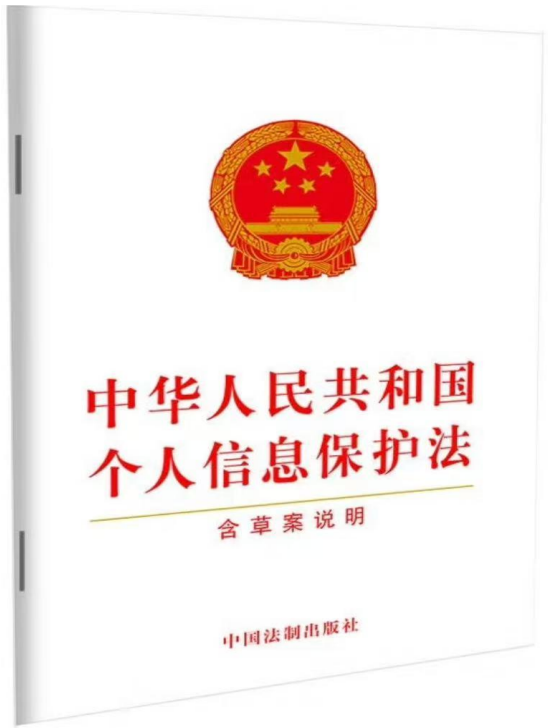


第二十七条开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

第三十二条任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

第五十二条违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。【参见刑法】

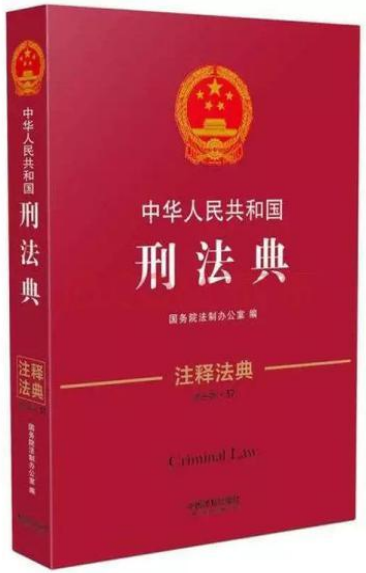


第十条任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第二十九条处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第六十六条违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；**对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款**。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。



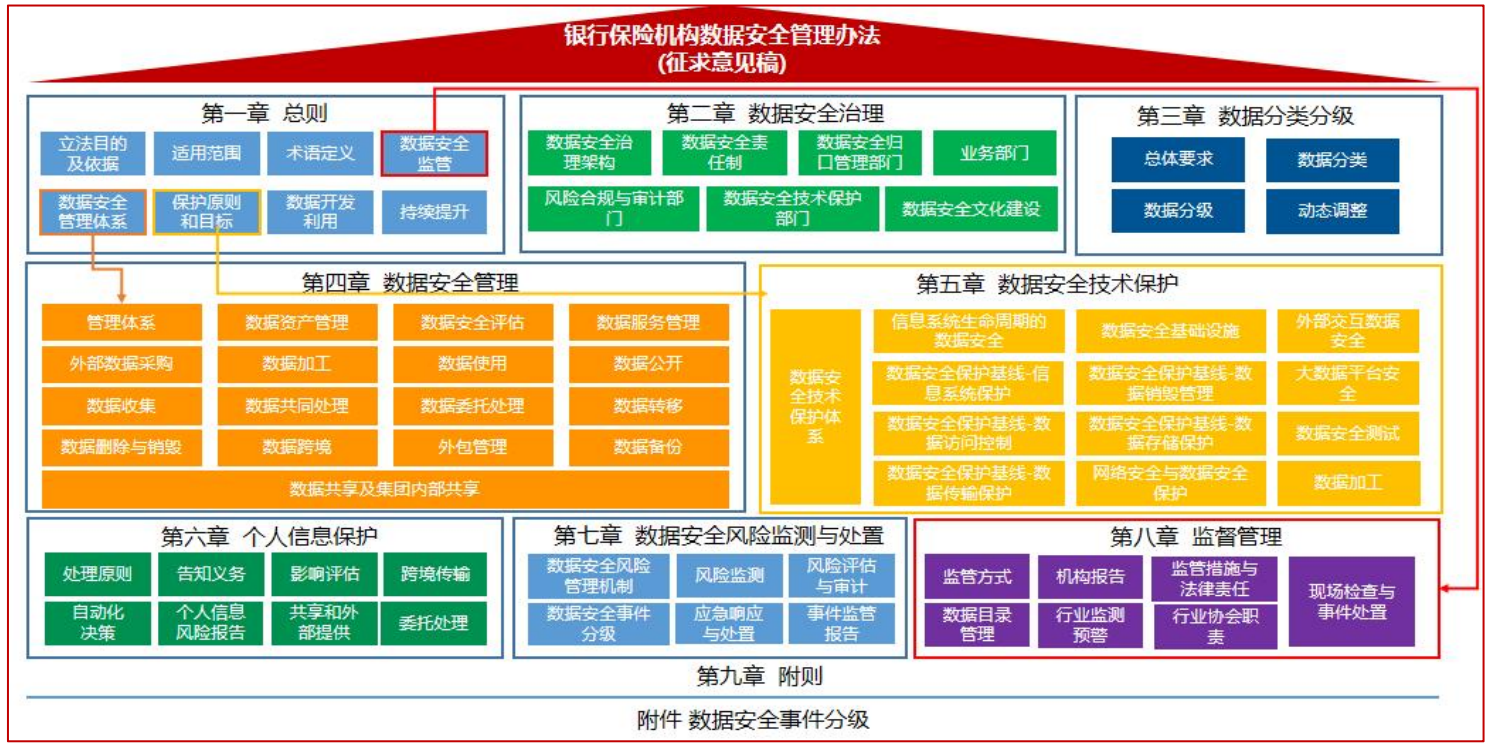
第二百五十三条之一

第一款：违反国家有关规定，向他人**出售**或者**提供**公民个人信息，**情节严重的**，处三年以下有期徒刑或者拘役，并处或者单处罚金；**情节特别严重的**，处三年以上七年以下有期徒刑，并处罚金。
第二款：违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。
第三款：窃取或者**以其他方法非法获取公民个人信息的**，依照第一款的规定处罚。
第四款：单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

第五条非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：
（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；
（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；
（三）**非法**获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；
（四）**非法**获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；
（五）**非法**获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；
（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；
（七）违法所得五千元以上的；
（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；
（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；
实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：
（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；
（二）造成重大经济损失或者恶劣社会影响的；
（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；

- 2024年12月27日，国家金融监督管理总局正式发布**《银行保险机构数据安全管理办法》（金规〔2024〕24号）**，旨在规范银行业保险业数据处理活动，保障数据安全、金融安全，促进数据合理开发利用，保护个人、组织的合法权益，维护国家安全和社会公共利益。



监管要点

- **落实数据安全治理组织**：建立数据安全责任制，指定归口管理部门负责本机构的数据安全工作;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；**每年开展全员的数据安全意识教育和培训工**作
- **建立数据分类分级制度**：**制定数据分类分级保护制度，建立数据目录和分类分级规范**，动态管理和维护数据目录，并采取差异化的安全保护措施。
- **强化数据安全管理**：根据自身发展战略**建立数据安全管理制度和数据处理管控机制**，在开展相关数据业务处理活动时应当进行数据安全评估。
- **健全数据安全技术体系**：**建立含分类分级、数据防泄露、数据摆渡、API安全审计、数据安全管控平台、数据流转监测及防护平台在内的数据安全技术架构**，明确数据保护策略方法，采取技术手段保障数据安全。
- **加强个人信息保护**：最小范围收集个人信息；共享和对外提供个人信息时，应取得个人同意；**开展个人信息保护影响评估。**
- **完善数据安全风险监测与处置机制**：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。

第三十条　重要数据的处理者应当明确**数据安全负责人和数据安全管理机构**。**数据安全负责人**应当具备数据安全专业知识和相关管理工作经历，**由数据处理者管理层成员担任**，有权直接向有关主管部门报告数据安全情况。掌握有关主管部门规定的特定种类、规模的**重要数据的数据处理者**，应当**对数据安全负责人和关键岗位的人员进行安全背景审查**，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

《银行保险机构数据安全管理办法》

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

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。

第十三条　银行保险机构风险管理、内控合规和审计部门负责将数据安全纳入全面风险管理体系、内控评价体系，定期开展审计、监督检查与评价，督促问题整改和开展问责。

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。

第十五条　银行保险机构应当建立良好的数据安全文化，开展全员数据安全教育和培训，提高数据安全保护意识和水平，形成全员共同维护数据安全和促进发展的良好环境。

主要内容：建立数据分类分级标准。要求银行保险机构制定数据分类分级保护制度，建立数据目录和分类分级规范，并采取差异化的安全保护措施。

数据分类

银行保险机构应对机构业务及经营管理过程中获取、产生的数据进行分类管理，数据类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。

数据分类对比	银行保险机构数据安全管理办法	《金融数据安全 数据安全分级指南》（JR/T 0197-2020）	《数据安全技术 数据分类分级规则》（GB/T 43697-2024）
	客户数据	客户数据	用户数据
	业务数据	业务数据	业务数据
	经营管理数据	经营管理数据	经营管理数据
	系统运行和安全管理数据	监管数据	系统运维数据

数据分级

银行保险机构应当根据数据的重要性和敏感程度，将数据分为**核心数据、重要数据、一般数据**。其中，一般数据细分为敏感数据和其他一般数据。

- **核心数据**：是指对领域、群体、区域具有较高覆盖度或者达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或者共享，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益；
- **重要数据**：是指特定领域、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**：是指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据；
- **其他一般数据**：除以上数据之外的数据。

数据分级对比	银行保险机构数据安全管理办法	中国人民银行业务领域数据安全管理办法（征求意见稿）	《金融数据安全 数据安全分级指南》（JR/T 0197-2020）	《个人金融信息保护技术规范》（JR/T 0171-2020）
	核心数据	核心数据	-	-
	重要数据	重要数据	五级	-
	敏感数据	一般数据	四级	C3
			三级	C2
	其他一般数据		二级	C1
			一级	-

银行保险机构应当加强数据安全级别的时效管理，建立动态调整审批机制，当数据的业务属性、重要程度和可能造成的危害程度发生变化，导致原安全级别不再适用的，应当及时动态调整。

主要内容：强化数据安全管理。要求银行保险机构按照国家数据安全与发展政策要求，根据自身发展战略建立数据安全管理制度和数据处理管控机制。

数据安全管理体系：银行保险机构应当建立与本机构业务发展目标相适应的数据安全治理体系，**建立健全数据安全管理制度，构建覆盖数据全生命周期和应用场景的安全保护机制**，开展**数据安全风险评估、监测与处置**，保障数据开发利用活动安全稳健开展。银行保险机构利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度基础上，履行数据安全保护义务。

01

管理体系

银行保险机构应当按照国家数据安全与发展政策要求，根据自身发展战略，制定数据安全保护策略。银行保险机构应当制定数据安全管理办法，明确管理责任分工，建立包括数据处理全生命周期管控机制，落实保护措施。

银行保险机构应当对数据外部引入或者合作共享、数据出境等，制定安全管理实施细则。

02

数据资产管理

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

03

数据安全评估

银行保险机构在处理敏感级及以上数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，应当事先开展数据安全评估。

04

数据服务管理

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

主要内容：加强个人信息保护。要求银行保险机构按照“明确告知、授权同意”原则处理个人信息，收集个人信息应限于最小范围，不得过度收集。

处理原则

第五十二条

银行保险机构处理个人信息应按照“明确告知、授权同意”的原则实施，法律、行政法规另有规定的除外，并在信息系统中实现相关功能控制。

第五十三条

银行保险机构处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，收集个人信息应当限于实现金融业务处理目的的最小范围，不得过度收集个人信息。

告知义务

第五十四条、五十五条

银行保险机构处理个人信息前，应当真实、准确、完整地向个人告知其个人信息的处理目的、处理方式、保存期限，个人行使其信息权利的申请受理和处理程序，以及法律法规规定应当告 知的其他事项。
银行保险机构应当制定个人信息处理规则，个人信息处理规则应当公开展示、易于访问、内容明确、清晰易懂。
银行保险机构不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或者服务所必需的除外。

影响评估

第五十六条

银行保险机构在开展涉及处理个人信息的业务活动时，应当进行个人信息保护影响评估，评估内容包括个人信息处理的合法性、必要性，对个人权益的影响及安全风险和保护措施有效性。个人信息保护影响评估记录应当至少保存三年。

共享和外部提供

第五十七条

银行保险机构与其母行、集团，或其子行、子公司共享个人信息，及向外部提供个人信息，**应当向个人告知**共享对象的名称、 联系方式、处理目的、处理方式和个人信息的种类，**并取得个人的单独同意**，法律、行政法规另有规定的除外。

跨境传输

第五十八条

银行保险机构向中华人民共和国**境外提供个人信息**的，除满足第五十七条规定的要求外，还应**向个人告知**其向境外**接收方行使信息权利的方式和程序**等事项，法律、行政法规另有规定的除外。

委托处理

第五十九条

银行保险机构**委托第三方处理**个人信息的，应当在合同或协议条款内**明确受托人对个人信息的保护义务、保护措施和期限**等，并**严格监督受托人**以约定的处理目的、处理方式等处理个人信息，与第三方传输个人敏感数据必须确保安全，防范数据滥用和泄漏风险。**未经银行保险机构同意，受托人不得转委托他人处理个人信息**。

自动化决策

第六十条

银行保险机构在算法设计、训练数据选择和模型生成时，应当采取有效措施，保障个人合法权益。利用个人信息进行自动化决策，应当**保证决策的透明度和结果公平、公正**；银行保险机构通过自动化决策方式作出对个人金融业务有重大影响的决定，个人**有权要求银行保险机构予以说明，并有权拒绝**银行保险机构仅通过自动化决策的方式对其开展业务。

个人信息安全事件

第六十一条

发生或者可能发生个人信息泄露、篡改、丢失的，银行保险机构应当立即采取补救措施，同时通知个人并报送国家金融监督管理总局或其派出机构。
通知应当包括下列事项:
(一)发生或者可能发生个人信息泄露、篡改、丢失的信息 种类、原因和可能造成的危害;
(二)银行保险机构采取的补救措施和个人可以采取的减轻危害的措施。

主体	违法行为	监管机构	罚则
银行业金融机构	违反《银行保险机构数据安全管理办法》规定	国家金融监督管理总局及其派出机构	● 根据其违规情况，对银行保险机构依法采取风险提示、监管谈话、监管通报、责令改正等监管措施；对涉及违规处理行为的系统或者应用，责令暂停或者终止服务； ● 对有重大违法违规情形，或者迟报、瞒报数据安全事件和案件，或者产生重大数据安全风险、事件、案件的第三方机构进行行业通报，责令银行保险机构暂缓或者停止合作。
			● 依据《中华人民共和国银行业监督管理法》相关规定，责令银行业金融机构改正，并处以二十万以上五十万以下罚款； ● 情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证。 ● 根据违规情况，可以责令银行业金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分； ● 银行业金融机构的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员给予警告，处五万元以上五十万元以下罚款； ● 取消直接负责的董事、高级管理人员一定期限直至终身的任职资格，禁止直接负责的董事、高级管理人员和其他直接责任人员一定期限直至终身从事银行业工作。 ● 构成犯罪的，依法追究刑事责任。

章节 PART 03

以案为鉴：监管部门处罚案例解析

处罚案例：2024年10月，某银行APP隐私政策不清晰，被公安处罚

违法违规事实：

1.App未开展安全评估报备；

2.App存在未公开收集、使用规则，未明示收集使用个人信息的目的、方式和范围等情况。

处罚结果：

责令改正、给予警告并处以5万元罚款，同时对直接负责的主管人员给予警告

个人信息保护法

第十七条个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第六十六条违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

处罚案例：2025年3月，某银行未按照规定落实数据安全相关管理规定，被人行处罚

违法违规事实：

1.违反金融统计相关规定；2.违反账户管理规定；3.未按规定落实反电信网络诈骗相关管理规定；
4.未按照规定落实数据安全相关管理规定；
5.违反反假币业务管理规定；
6.违反信用信息采集、提供、查询及相关管理规定；
7.未按规定履行客户身份识别义务；
8.未按规定报送大额交易报告或可疑交易报告

处罚结果：

警告，罚款184万元

数据安全法

第二十七条开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

第四十五条开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由**有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款**，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

《中国人民银行业务领域数据安全管理办法》第四十九条数据处理者未履行本办法规定的数据安全保护义务，有下列情形之一的，中国人民银行及其分支机构依照《中华人民共和国数据安全法》第四十五条予以处罚：

（一）未依照法律、行政法规对应规定，建立健全全流程业务数据安全管理制度的。

（二）未依照法律、行政法规对应规定，组织开展业务数据安全教育培训的。

（三）未依照法律、行政法规对应规定，采取相应的技术措施和其他必要措施，保障业务数据安全的

处罚案例：2024年7月某银行嘉兴市分行违规泄露客户信息，被人行处罚

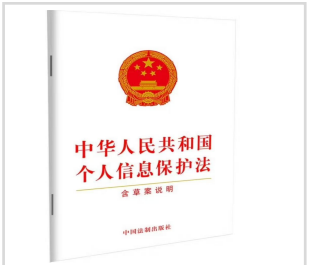
违法违规事实：

一、贷后管理不到位，贷款资金实际用途与约定不符；
二、贷后管理不到位，贷款资金挪用于购房；
三、项目资本金管理不到位；
四、固定资产贷款用途管理不到位；
五、贴现资金回流；
六、违规泄露客户信息。

处罚结果：
罚款210万，相关责任人分别作出警告

哪些场景属于违规泄露客户信息？

- 未经授权，擅自将客户个人账户信息提供他人
- 委托第三方公司处理保单数据时，未签订安全协议，导致数据被用于营销推广
- 将上一单位客户信息带到下一个单位使用的
- 违反公司数据安全管理要求，未授权将客户信息留存到个人电脑或U盘，造成数据泄露的
- 未经授权将客户信息发布到互联网的（朋友圈、微博、网盘、官网）



个人信息保护法

第二十一条个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

第二十三条个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

第二十五条个人信息处理者不得公开其处理的个人信息*（指个人信息处理者将所处理的个人信息向不特定的多数人或特定范围外的主体披露、展示的行为）*，取得个人单独同意的除外。

违反这些规定的后果如下：
一般情节：由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
情节严重：由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

处罚案例：2021年3月某银行未授权查询客户敏感信息，被国家金融监督管理局处罚

违法违规事实：

一、客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力；

二、客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息；

三、对客户敏感信息管理不善，致其流出至互联网；违规存储客户敏感信息；

四、系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷。

处罚结果：

罚款450万，支行行长撤职

数据安全法

第二十七条开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

第四十五条开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

《银行保险机构数据安全管理办法》

- 谁管业务、谁管业务数据、谁管数据安全”的原则，各业务部门应指定本部门业务数据相关管理机制。
- 明确数据收集和处理的目的、方式、范围、规则，不超范围收集客户信息。
- 按照“业务必要授权”原则，对敏感级及以上数据严格实施授权管理，制定数据访问闭环管理机制。
- 处理个人信息前，应当真实、准确、完整地向个人告知其个人信息的处理目的、处理方式、处理的个人信息种类、保存期限。

信息，获利27万余元获刑后被终身禁业

国家金融监督管理总局 天津监管局

无障碍浏览 | 繁 |

请输入您要搜索的内容...

机构概况 | 新闻资讯 | 政务信息 | 在线服务 | 互动交流 | 统计数据 |

当前位置：首页 > 政务信息 > 公告通知

发布时间：2024-07-23 来源：天津监管局 文章类型：原创 打印 微博 微信 更多

天津金融监管局行政处罚决定书送达公告

武威、李忠志、张恪：

因采取直接送达、邮寄送达等方式无法送达，我局于2024年5月7日向武威、李忠志、张恪公告送达了《行政处罚事先告知书》（津金罚告字〔2024〕53号、55号、69号），依法告知了拟作出行政处罚的事实、理由、依据及依法享有的权利。法定期限内武威、李忠志、张恪未向我局提出陈述申辩和听证意见。

经查，武威、李忠志对中国建设银行天津市分行员工管理不到位、员工从事违法活动事项负有直接责任，张恪对中国农业银行天津南开支行违规办理汽车分期业务事项负有直接责任。根据《中华人民共和国银行业监督管理法》第四十八条第（三）项规定，我局决定分别给予武威、李忠志、张恪禁止终身从事银行业工作的行政处罚。2024年6月26日，我局分别向武威、李忠志、张恪作出《行政处罚决定书》（津金罚决字〔2024〕79号、80号、78号）。

因采取直接送达、邮寄送达等方式仍无法送达，现依法向武威、李忠志、张恪公告送达《行政处罚决定书》（津金罚决字〔2024〕79号、80号、78号）。请在本公告发出之日起三十日内到我局领取，逾期视为送达。

如不服上述处罚决定，可以在收到行政处罚决定书之日起六十日内向国家金融监督管理总局申请行政复议，也可以在收到行政处罚决定书之日起六个月内向有管辖权的人民法院提起诉讼。复议、诉讼期间本决定不停止执行。

联系人：天津金融监管局

联系电话：022-83866860

联系地址：天津市和平区长春道18号

2024年7月23日

李忠志，原中国建设银行天津市分行河东支行职工。2016年7月25日被金华市公安局江南分局刑事拘留，同年8月30日被依法逮捕。

从公开信息来看，李忠志的犯罪行为被发现，属于“拔出萝卜带出泥”，系警方侦查其他案件时顺手进行调查，最终牵连至这名建行员工。法院方面也指出，浙江省金华市公安局江南分局在办理徐某、蒙某等人犯罪案件中，发现李忠志贩卖大量公民信息和银行信息，且李忠志与徐某、蒙某犯罪案关联，遂于2016年7月将李忠志抓获归案。

最终，金华市婺城区人民法院一审认定，李忠志违反国家有关规定，非法获取公民个人信息，并出售给他人，情节严重，其行为已构成侵犯公民个人信息罪。李忠志自愿认罪，在本案审理过程中，已退出违法所得人民币24950元，可酌情从轻处罚。具体判决如下：李忠志犯侵犯公民个人信息罪，判处有期徒刑二年，并处罚金人民币五万元。追缴违法所得，上缴国库。

法律依据：根据《刑法》第二百五十三条之一第一款：违反国家有关规定，向他人**出售**或者**提供**公民个人信息，**情节严重的**，处三年以下有期徒刑或者拘役，并处或者单处罚金；

同时行业监管机构作出行政处罚，禁止终身从事银行工作。

04

章节 PART

实操指南：日常工作如何 “守好数据”

决策层

管理层

执行层

监督层

《银行保险机构数据安全管理办法》第九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。

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。。

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。组织制定数据安全管理原则、规划、制度和标准;组织建立和维护数据目录，推动实施数据分类分级保护;组织开展数据安全评估和审查;统筹建立数据安全应急管理机制，组织开展数据安全风险监测、预警与处置;组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能;建立和维护内部数据共享、外部数据引入、数据对外提供、数据出境的统筹管理机制，牵头对外部数据供应商进行安全管理，统筹大数据应用、数据共享项目的安全需求管理;向党委(党组)、董(理)事会、高管层报告数据安全重要事项; 其他须统筹管理的数据安全工作事项。

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负责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；制定数据安全技术标准规范制度，组织开展数据安全技术风险评估；组织开展信息系统的生命周期安全管理，确保数据安全保护措施在需求、开发、测试、投产、监测等环节得到落实；建立数据安全技术应急管理机制，组织开展数据安全风险技术监测、预警、通报与处置，防范外部攻击、内外部破坏等危害数据安全活动；组织数据安全技术研究与应用。

风险管理、内控合规和审计部门：负责将数据安全纳入全面风险管理体系、内控评价体系，定期开展审计、监督检查与评价，督促问题整改和开展问责。

各业务部门：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。

职工：需严格遵守数据安全管理制度和操作规程，保护好自己账号密码等访问权限，不随意泄露、篡改、损毁所接触到的客户数据和机构内部数据，发现数据安全隐患或违规行为及时报告。

- 禁止泄露公司敏感数据

禁止行为

典型场景

- 未经审批流程，业务部门员工私自将银行客户交易数据、市场份额数据等提供给外部咨询公司用于市场调研项目。

后果

违反规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
若涉及资金交易，追究刑事责任。

法律依据

《网络数据安全管理条例》第六十一条违反本条例规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

《个人信息保护法》第十三条取得个人的同意，个人信息处理者方可处理个人信息：

《银行保险机构数据安全管理办法》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。

- 禁止超权限查询数据

禁止行为

典型场景

- 利用同事临时离岗未锁屏，登录其系统查询高净值客户资产配置信息，用于个人营销对比。

后果

严重未授权使用敏感数据，触发系统权限预警，责任人记过处分。若对客户造成重大影响，可能承担民事责任。

法律依据

《网络数据安全管理条例》第九条：网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用；

《中国人民银行业务领域数据安全管理办法》第十四条数据处理者应当严格管理处理业务数据相关信息系统数据库管理员账号等特权账号和各类业务处理账号的权限，人员变动时应当立即调整权限。数据处理者应当与可使用高敏感性数据项账号的人员签订保密协议。

《银行保险机构数据安全管理办法》第二十八条银行保险机构应当按照“业务必要授权”原则，对敏感级及以上数据严格实施授权管理，制定数据访问闭环管理机制，并对数据访问行为实施审计。

- 禁止泄露业务系统访问凭证

禁止行为

典型场景

- 为方便“快速登录”，将业务系统密码写在工位便签，被其他同事或外部人员意外获取尝试登录。
- 或直接将个人业务系统账号密码告知他人使用。

后果

密码泄露导致客户信息被批量下载，银行需赔偿客户损失，责任人面临解除劳动合同+行业禁入。

法律依据

《网络数据安全管理条例》第九条：网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用；

《中国人民银行业务领域数据安全管理办法》第十四条数据处理者应当严格管理处理业务数据相关信息系统数据库管理员账号等特权账号和各类业务处理账号的权限，人员变动时应当立即调整权限。数据处理者应当与可使用高敏感性数据项账号的人员签订保密协议。

《银行保险机构数据安全管理办法》第二十八条银行保险机构应当按照“业务必要授权”原则，对敏感级及以上数据严格实施授权管理，制定数据访问闭环管理机制，并对数据访问行为实施审计。

案件过程

2017年10月，被告人崔某2015年12月至2016年3月期间，利用在永州市建设银行分行担任外包人员的职务之便，通过盗用管理人员陈某操作码，查询外地个人信用报告3678笔，判处有期徒刑三年，缓刑三年，并处罚金人民币三万七千元。

建行永州分行重新调查得知，**陈某的征信查询用户和密码并非被盗用，而是其主动给予信用卡外包合作公司团队**，该团队中有六人知道。2017年11月9日，陈某在谈话笔录中承认其于2016年将征信查询用户和密码委托过外包内勤人员查询。2017年12月8日，调查外包工作人员伍某，进一步确认大部分外包人员知道陈某的征信查询用户和密码，陈某将修改后的密码告诉过外包人员。

处罚结果

陈某2015年开始将其**征信查询用户和密码委托他人使用**，并被信用卡外包合作公司团队成员崔某获取，2016年1月至2016年3月期间，崔某利用陈某的征信查询用户和密码违规查询客户个人信用报告3460份，引发客户投诉，形成严重风险事故；**建行永州分行根据总行违规违纪管理办法送出《关于给予陈某行政开除处分的决定》和《解除劳动合同通知书》。**

同时，建行永州分行被中国人民银行罚款10万元，崔某罚款0.9万元。

- 禁止非加密渠道传输敏感数据

禁止行为	典型场景	后果
 严禁通过微信、QQ、私人邮箱等未加密工具，发送客户身份证、银行卡号等敏感信息（含截图、文档）。	■ 客户经理为赶时间，用微信传输客户房产抵押合同扫描件给合作评估机构，被聊天记录云端备份留存风险。	数据在传输中被第三方拦截，引发客户信息贩卖案件，银行被罚百万级罚单，责任人承担刑责。

法律依据

《网络数据安全管理条例》第九条：网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用；

《个人信息保护法》第四十七条：处理目的已实现、无法实现或者为实现处理目的不再必要，个人信息处理者应当主动删除个人信息。

《中国人民银行业务领域数据安全管理办法》第十六条数据处理者应当根据业务需要，明确业务数据保存期限。除履行法定职责或者法定义务外，高敏感性数据项原则上不在终端设备和移动介质中存储，确需存储的，数据处理者应当统一规范管理相关需求场景。

- 禁止私自搭建数据传输通道

禁止行为	典型场景	后果
 不得违规连接外部网络（如手机热点连办公电脑、私接无线路由器）传输业务数据。	■ 为了方便办公给电脑安装无线网卡，将接入银行内部网络的办公电脑连接互联网。	办公电脑连接互联网遭受病毒木马攻击，数千条客户数据泄露，责任人因“违规外联”被认定为重大安全隐患，终身禁业。

法律依据

《网络数据安全管理条例》第九条：网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用；

《个人信息保护法》第四十七条：处理目的已实现、无法实现或者为实现处理目的不再必要，个人信息处理者应当主动删除个人信息。

《中国人民银行业务领域数据安全管理办法》第十六条数据处理者应当根据业务需要，明确业务数据保存期限。除履行法定职责或者法定义务外，高敏感性数据项原则上不在终端设备和移动介质中存储，确需存储的，数据处理者应当统一规范管理相关需求场景。

案件过程

经法院审理查明，李某在廊坊银行工作期间借调至银监会负责法规部日常文件的处理工作。2017年2月16日下午，法规部法律顾问处保密机上的OA系统收到一份文件，附件是要求他们提出意见的《关于规范金融机构资产管理业务的指导意见》。这份文件长达六七十页，李某经申请将文件打印了出来。2017年2月17日上午9时许，**李某通过微信和原单位（廊坊银行总行）法律合规部总经理郑某聊一些工作时，通过微信将该文件拍照发给了郑某。**这份文件第一页的左上角有机密的字样，李某知道这份文件属于国家秘密，不能随便给别人看，发给郑某的该文件照片就没有拍带有机密标识字样的页面。**最终该文件在多个金融行业微信群及有关人员微博、博客、微信公众号中不断转发，造成涉密信息在互联网上被大范围公开传播。**

处罚结果

判决被告人李某犯故意泄露国家秘密罪，判处有期徒刑一年，缓刑一年。

法律依据

《中华人民共和国宪法》
国家机关工作人员违反保守国家秘密法的规定，故意或者过失泄露国家秘密，情节严重的，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑。

随意丢弃含客户信息的纸质文件

银行员工将记录有客户姓名、账号、交易记录等信息的纸质报表、凭证未粉碎处理，直接丢入普通垃圾桶；或随意放置在办公桌

外包机构超额获取数据

第三方运维人员获取完整客户库

违规删除或篡改数据日志

为掩盖操作失误或违规行为，技术人员删除或修改系统中关于数据操作的日志记录，如删除未经授权访问客户账户的操作日志

在公共网络处理涉密业务数据

员工在咖啡馆、机场候机区等公共Wi-Fi环境下，登录银行内部系统处理客户贷款审批、资金转账等敏感业务。

人员离职后未及时收回权限

员工离职后，其银行系统账号仍保留对客户信息、业务数据的访问权限，导致离职人员可继续查看甚至下载相关数据

APP过度索权

银行手机APP在安装时，要求获取用户通讯录、摄像头、麦克风等与核心金融业务无关的权限，如仅进行账户查询功能时仍强制索要通讯录权限。

超范围使用客户授权数据

客户仅授权银行使用其信息用于贷款审批，但银行将该数据用于精准营销其他金融产品，如向仅申请房贷的客户推送信用卡、理财产品广告

使用弱密码或长期不更换系统登录密码

银行内部系统用户设置“123456”“password”等简单易猜密码，且长期未修改，增加系统被破解风险。

05

章节 PART

总结：安全防线，始于意识，成于行动

例

应急处置前期：事件发现与初步研判

事件发现

1.人工排查与外部反馈：业务部门在日常操作中若发现异常（如客户反馈“未操作却收到账户交易短信”“个人信息被用于非法贷款”），需第一时间上报至数据安全管理部门；或监管机构、合作机构或第三方安全厂商通报相关安全风险。
2.技术监测工具触发预警：通过部署数据防泄漏（DLP）系统、入侵检测/防御系统（IDS/IPS）、SOC平台、数据库审计系统等工具，实时监测异常行为。

初步研判

1.确定事件类型：根据数据安全事件的表现形式，快速归类；常见类型包括：数据泄露、数据篡改、数据损毁、未授权访问等。
2.评估影响范围：结合此前数据分类分级方式，判断受影响的数据级别（重要数据/敏感数据/其他一般数据）、数据量（如泄露100条/10万条客户信息）、涉及对象（个人客户/企业客户/机构内部数据）。
3.判定事件级别：参考《银行保险机构数据安全事件分级》将事件分级。

应急处置中期：控制风险、消除隐患

快速控制

针对不同事件类型采取精准控制措施：
非授权访问/数据泄露：立即冻结异常账号、禁用可疑IP地址的访问权限；若敏感数据正通过邮件、FTP或即时通讯工具向外传输，需阻断对应传输通道（如暂停该时段的外部邮件发送功能、封禁违规传输端口）；
数据篡改：立即暂停相关业务系统（如信贷审批系统、账户交易系统）的写入权限，防止进一步篡改；若已发现篡改数据，需备份当前数据状态（避免篡改痕迹被覆盖）；
数据损毁：若因勒索病毒导致数据加密，需立即隔离受感染的服务器（断开与内网其他设备的连接），防止病毒扩散；若因硬件故障，需停止故障设备运行，避免数据二次损坏。

消除隐患

1.漏洞修复与系统加固：针对事件根源（如系统漏洞、权限配置不当、人员操作失误）采取修复措施；
2.数据恢复（针对数据损毁/篡改事件）：
优先使用备份数据恢复：若存在定期备份（如每日全量备份+增量备份），需选择“未被篡改/损毁的最新备份版本”进行恢复，恢复前需在测试环境验证备份数据的完整性（避免恢复后仍存在问题）；
若备份数据不可用（如备份介质损坏、备份数据也被篡改），可尝试通过技术手段恢复（如使用数据恢复工具找回误删除的文件、通过数据库日志回滚篡改操作）；
恢复后需对比恢复数据与业务记录，确认核心数据（如客户账户余额、交易明细）的准确性，避免因恢复不完整导致业务异常。

应急处置后期：溯源追责、通报上报与复盘优化

事件溯源

结合前期留存的证据链开展深度调查：
1.内部溯源：排查是否为内部人员（员工、外包人员）所为
2.外部溯源：若确认是外部攻击（如黑客入侵、第三方合作机构泄露），需联合公安机关、网络安全厂商开展溯源

通报上报

1.内部通报：向公司管理层、相关业务部门通报事件情况（包括事件类型、影响范围、处置措施、当前状态），确保各部门同步知晓风险，配合后续工作（如业务部门协助联系受影响客户、客服部门准备应对客户咨询）。
2.外部上报：2小时内向属地人行/国家金融监督管理局上报，24小时书面报告；特别重大另需向属地公安机关报告。

复盘优化

事件处置结束后 5个工作日内，需组织复盘会议，形成 “问题清单 - 改进措施 - 责任人 - 完成时限” 的闭环，将事件及其处置的评估、总结和改进报告报送人行、国家金融监督管理总局或者其派出机构。