# 《银行保险机构数据安全监管办法》

深度解读与实践指南

# 严峻的数据安全形势

## 数字化转型加速

数据量爆炸式增长，数据价值日益凸显，成为企业核心竞争力。

## 风险事件频发

数据泄露、网络攻击、滥用等事件对金融安全和消费者权益构成严重威胁。

## 监管要求趋严

《数据安全法》等法规相继出台，构建了国家数据安全的基本框架。

### 核心挑战总结

- 外部攻击与内部威胁并存
- 数据全生命周期保护难度大
- 合规成本与技术投入持续攀升

# 《办法》的核心目标

## 规范数据处理活动

为银行保险机构的数据处理活动划定红线，确保合法合规。

## 保障数据与金融安全

防范数据安全风险，维护国家金融稳定。

## 促进数据合理利用

鼓励数据要素的合理开发利用，赋能业务创新。

## 保护消费者合法权益

加强个人信息保护，维护金融消费者的知情权、选择权和隐私权。

# 治理体系：组织架构与职责

### 党委/董事会

负主体责任，统筹决策数据安全重大事项。

### 主要负责人

第一责任人，对数据安全工作全面负责。

### 分管高管

直接责任人，领导分管领域数据安全工作。

### 归口管理部门

主责部门，负责统筹协调数据安全工作。

### 业务部门

谁管业务、谁管数据、谁管安全。

### 信息科技部门

技术保护主责部门，提供安全技术支撑。

### 风险/合规/审计

监督、评价、问责，保障体系有效运行。

# 数据安全的“三道防线”

## 第一道防线：业务部门

数据的生产者和使用者，是数据安全的第一道关口，承担着首要的安全责任负，责日常的数据安全管理和风险控制。

## 第二道防线：管理部门

负责制定数据安全政策、制度和标准，进行风险的集中管理和监控。

## 第三道防线：审计部门

对数据安全管理体系的有效性进行独立的监督和评价，提出改进建议。

三道防线层层递进，协同工作，共同构筑企业坚实的数据安全屏障。

# 数据分类：明确数据类型

### 客户数据

如个人身份信息、账户信息、交易记录等。

### 业务数据

如产品信息、营销数据、风控模型数据等。

### 经营管理数据

如财务数据、人力资源数据、战略规划数据等。

### 系统与安全数据

如日志数据、网络流量数据、安全告警数据等。

# 数据分级：确定保护强度

**核心数据**

影响国家安全、经济命脉、重大公共利益

**重要数据**

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**

对经济运行、社会稳定、公共利益或个人造成重要影响

**其他一般数据**

除上述之外的其他数据

# 数据全生命周期安全管理

**收集**

合法、正当、必要

**使用**

最小权限、防止滥用


**存储**

加密存储、异地备份、容灾

**传输**

加密传输、通道安全

**销毁**

安全擦除、不可恢复

# 关键环节：存储与备份

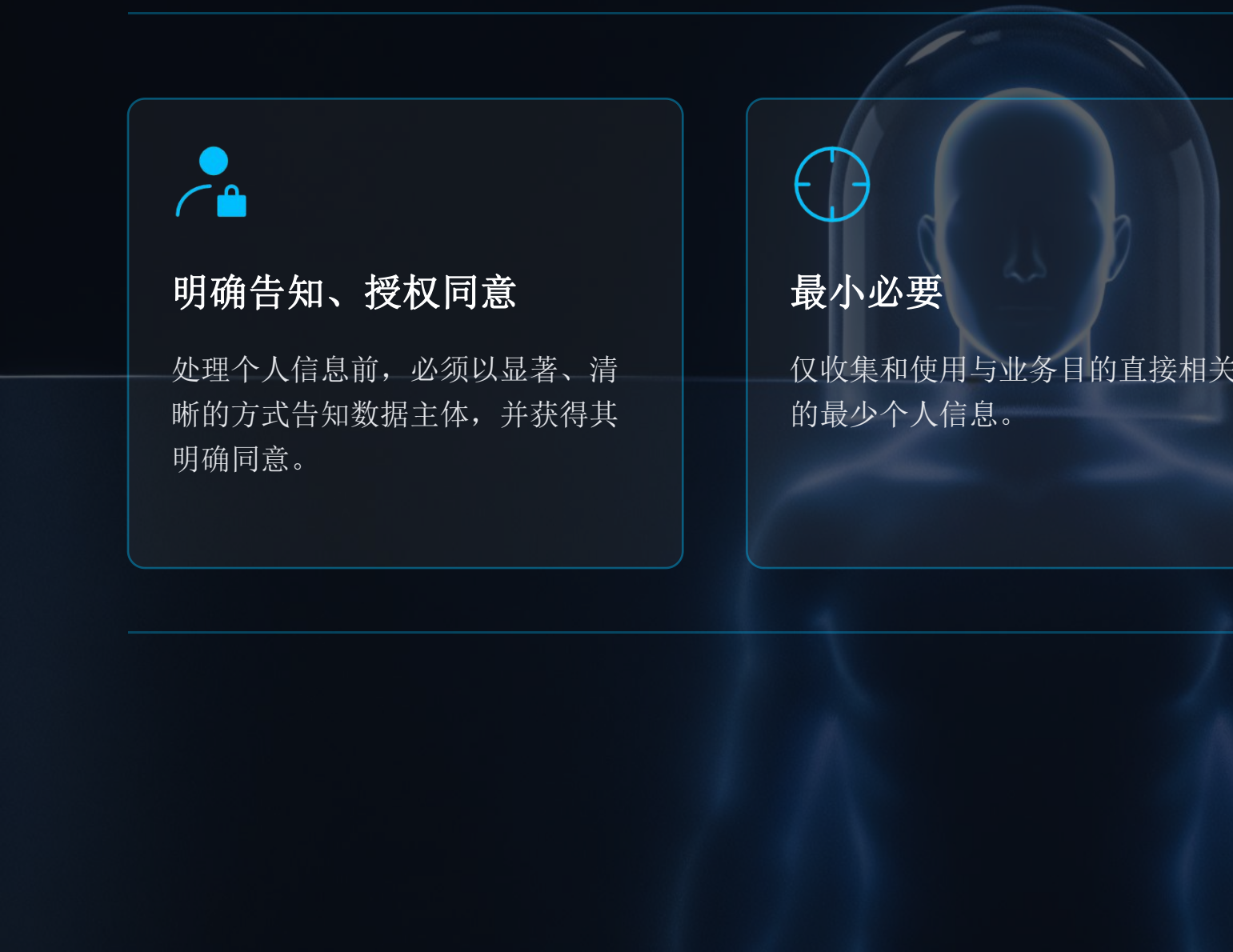
## 安全存储

- 敏感及以上数据必须加密存储。
- 个人身份鉴别数据不得明文存储。
- 防止勒索病毒等恶意攻击。

## 数据备份与容灾

- 制定备份策略，定期执行备份。
- 备份数据与生产数据隔离存放。
- 定期进行数据恢复演练，确保有效性。
- 实施数据容灾备份，保障业务连续性。

# 个人信息保护的核心原则



### 明确告知、授权同意

处理个人信息前，必须以显著、清晰的方式告知数据主体，并获得其明确同意。

### 最小必要

仅收集和使用与业务目的直接相关的最少个人信息。

### 确保安全

采取必要措施保护个人信息不被泄露、篡改、丢失。

# 建立数据安全风险监测体系

### 监测对象

数据处理活动、网络流量、系统日志、异常行为

### 监测内容

未授权访问、数据泄露、异常使用、攻击行为

### 监测技术

大数据分析、用户行为分析(UBA)、SIEM

### 核心目标

实现对数据安全风险的“可见、可感、可控”


构建主动防御体系，全面提升数据安全水位

# 数据安全事件应急处置

### 事件发现与报告

立即启动应急预案，2小时内上报监管。

### 应急响应与控制

采取技术和业务措施，控制事态发展。

### 事件调查与评估

分析事件原因、影响范围和损失。

### 处置与恢复

清除威胁，恢复系统，总结改进。

闭环管理，持续优化：从发现到恢复，形成完整处置流程，不断提升安全防护能力。