



# 国际数字化转型最佳实践管理峰会

— 4月16日·上海 —

## 金融行业隐私保护工作心得

顾然

主办方：



BEST PRACTICE

# 个人简介

- ✓ 专业资格：中国律师执业资格，美国纽约州律师执业资格，EXIN DPO
- ✓ 就职单位：平安国际融资租赁有限公司
- ✓ 行业领域：网络安全和数据保护，飞机租赁、融资租赁
- ✓ 教育背景：美国南加州大学（法学硕士）  
西南政法大学（法学学士）

1/1

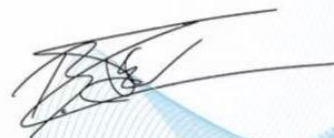


**Role Certificate:**  
**Data Protection Officer**

Presented to:

**Ran Gu**

24 January 2021



drs. Bernd W.E. Taselaar  
Chief Executive Officer

EXIN/2021/01252

EXIN  
The global independent certification institute for ICT Professionals

The validity of all EXIN certificates can be checked on [www.exin.com/certificates/validate](https://www.exin.com/certificates/validate)



# 目录

01 工作难点

02 合规要点

03 应对方法



- ✓立法层面：多、新、快、杂
- ✓监管层面：九龙治水
- ✓执法层面：执法趋严，刑事责任+天价罚单

**合规要求包括法律、行政法规、司法解释等国家法律法规，还包括监管部门发布的政策文件、管理规章、及相关的标准规范等**

- ✓ 法律：《民法典》、《网络安全法》、《刑法修正案（七）》、《刑法修正案（九）》、《个人信息保护法（草案）》、《数据安全法（草案）》、《消费者权益保护法》、《反洗钱法》
- ✓ 行政法规：《征信业管理条例》
- ✓ 司法解释：《两高关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》、《两高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》、《两高关于办理非法利用信息网络、帮助信息网络犯罪等刑事案件适用法律若干问题的解释》
- ✓ 部门规章：《中国人民银行金融消费者权益保护实施办法》、《网络安全审查办法》、《个人金融信息（数据）保护试行办法（初稿）》、《数据安全管理办法》、《金融控股公司监督管理试行办法》、《常见类型移动互联网应用程序必要个人信息范围规定》
- ✓ 规范性文件及标准：《个人信息安全规范》（GB/T35273-2020）、《个人金融信息保护技术规范》（JR/T0170-2020）、《App违法违规收集使用个人信息行为认定方法》、《金融数据安全 数据安全分级指南》（JR/T0197-2020）、《金融数据安全 数据生命周期安全规范》（JR/T0223-2021）

### 安全相关监管部门

- **中央网信办**：中共中央直属机构序列，负责该领域重大工作的顶层设计、总体布局、统筹协调、整体推进、敦促落实，具有统筹协调网络安全与信息化工作的地位
- **工信部**：电信和互联网行业的主管部门，目前主要负责电信业务经营许可、电信设备进网许可、互联网信息服务的登记和备案等工作
- **公安部**：主要从保障网络安全的角度切入，负责防范和打击互联网上的违法犯罪活动
- **其他**：1) 市场监管总局：并非互联网行业的直接主管机关，但近年来一直从“规范市场秩序”的角度出发，在部门规章立法、完善网络监管体系方面积极作为，监管影响力日益增强；2) 国密局：主要职责包括拟订密码工作发展规划，起草相关法规并负责密码法规的解释，组织拟定密码相关标准等

### 金融行业监管机构

- **中国人民银行**：制定和执行货币政策、维护金融稳定、提供金融服务。下属科技司负责人民银行科技管理与建设工作，负责金融标准化组织管理协调工作，指导协调金融业信息安全相关工作，拟定银行卡及电子支付技术标准等。人民银行会经常性发布金融业信息化或信息安全相关的管理和技术要求，是金融行业信息安全合规工作需要重点关注的部门
- **银保监会**：统一监督管理银行业和保险业，维护银行业和保险业合法、稳健运行、防范和化解金融风险，保护金融消费者合法权益，维护金融稳定。银行业和保险业的重要监管机构
- **证监会**：统一监督管理全国证券期货市场，维护证券期货市场秩序，保障其合法运行。证券期货行业的监管机构



# 工作难点-执法

## 多部门联合执法

- ✓ 国务院打击治理电信网络新型违法犯罪工作部级联席会议决定在全国范围内开展“断卡”行动
- ✓ 公安部、中央网信办牵头建立跨部委打击危害公民个人信息和数据安全违法犯罪长效机制
- ✓ 2020年App违法违规收集使用个人信息治理工作
- ✓ 中央网信办、工信部、公安部、市场监管总局四部门联合在全国范围组织开展App违法违规收集使用个人信息专项治理
- ✓ **公安部**：“云剑-2020”行动打击电信网络诈骗案件；“净网2020”专项行动严打侵害公民个人信息违法犯罪；专项整治违法违规App
- ✓ **市场监管总局**：开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动
- ✓ **网信办**：“清朗”专项行动
- ✓ **工信部**：通报侵害用户权益行为App
- ✓ **中国人民银行**：对部分金融机构侵害消费者金融信息安全行为立案调查并作出行政处罚；围绕“严监管常态化”对多家支付机构作出行政处罚；下发《关于开展金融科技应用风险专项摸排工作的通知》（银办发【2020】45号）；2019年开展金融消费者权益保护监督检查工作等。截止2020年10月，涉及个人金融信息的，共开出181张罚单，罚款合计超1.8亿元

# 目录

01 工作难点

02 合规要点

03 应对方法



- ✓ **对象：**个人金融信息，指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息
- ✓ 根据《金融数据安全 数据生命周期安全规范》JR/T0223-2021，根据安全性遭到破坏后的影响范围和影响程度，将金融数据安全级别由高到低分为5级、4级、3级、2级和1级
- ✓ **行为：**个人信息处理活动，包括收集、存储、使用、加工、传输、共享、转让、提供、公开、删除等个人信息生命周期内的所有处理行为

✓ **基本原则：**

- 1、合法正当原则
- 2、目的明确原则
- 3、选择同意原则
- 4、最小够用原则

- 5、安全可控原则
- 6、动态控制原则
- 7、权责一致原则

### 采集

#### ✓ 从外部机构采集:

1) 合同明确约定双方在数据安全方面的责任及义务、采集范围、频度、类型、用途等, 确保外部机构数据的合法合规性和真实性, 必要时提供相关主体的授权

2) 事前开展数据安全影响评估

3) 与提供的金融产品或服务直接相关, 不超范围采集

4) 明确知悉范围和安全管控措施, 确保采集数据的合规性、完整性、真实性...

#### ✓ 从个人金融信息主体处采集

1) 与提供的产品或服务直接相关, 不应超范围采集

2) 通过纸质表单采集数据并转化为电子数据时: 对表单的保存、查阅、复制等操作进行严格审批授权...; 在纸质表单电子化的过程中, 应采取技术措施确保数据完整性、保密性...

3) 停止提供金融产品或服务时, 立即停止数据收集活动及数据分析应用活动

### 传输

✓ **传输工具安全:** 应加强软件开发安全管理, 保障数据传输工具的安全性, 工具上线前应开展必要的渗透测试、支持库漏洞查找等工作

✓ **传输网络安全:** 应采用防火墙、入侵检测等安全技术或设备

✓ **安全隔离:** 不同网络区域或者安全域之间进行安全隔离和访问控制

✓ **防止非法接入:** 终端应采取准入控制、终端鉴别等技术措施

✓ **传输双方可信:** 应对通信双方进行身份认证

✓ **数据完整性:** 应采用数字签名、时间戳等方式

✓ **安全的密码算法:** 禁用不安全的算法 (如MD5,SHA1)...

### 存储

#### ✓ 存储安全

1) 不因存储形式或存储时效的改变而降低安全保护强度

2) 应根据安全级别、重要性、量级、使用频率等因素, 将数据分域分级存储

3) 应根据最小够用原则存储数据, 不应以任何形式存储业务非必需的金融数据, 存储时间应为业务必需的最短时间, 法律监管另有规定除外

4) 定期进行风险评估

5) 脱敏后的数据与用于还原数据的恢复文件隔离存储

6) 根据数据风险级别采取相应保护措施, 确保数据的完整性、保密性....

#### ✓ 备份和恢复

1) 根据数据的安全级别和数据对系统运行的影响, 制定数据备份策略和恢复策略

2) 生产数据应采取实时备份与异步备份、增量备份与完全备份的方式, 提供本地数据备份与恢复功能...

### 数据使用

- ◆ **数据访问**：应综合考虑主体角色、信用等级、业务需要、时效性等因素，按最小化原则确定2级以上数据的访问权限规则...
- ◆ **特权访问安全要求**：特权账户应明确安全责任人，严格限定使用地点，并配套多因素认证措施对使用者进行实名认证
- ◆ **数据导出**：根据最小够用原则，确定数据导出场景、范围和相应的权限规则...
- ◆ **数据加工**：明确数据获取方式、访问接口、授权机制、逻辑安全...
- ◆ **数据展示**：事前评估，展示时增加水印，禁用可将展示数据导出的功能等
- ◆ **开发测试**：采用技术措施实现测试环境数据与生产环境数据的有效隔离...
- ◆ **汇聚融合**：不应超出采集时声明的使用范围；开展安全影响评估；合同约定...

### 委托处理

- ◆ 对第三方开展数据安全管理工作
  - 1) 建立第三方机构管理制度
  - 2) 对接入和涉及的第三方产品和服务进行专门的数据安全管理
- ◆ 开展事前尽职调查
- ◆ 委托行为不应超出事前已获授权范围
- ◆ 对委托处理行为进行数据安全影响评估
- ◆ 对被委托方数据安全防护能力进行数据安全评估，确保被委托方的数据安全防护能力
- ◆ 不应对4级数据进行委托
- ◆ 对委托处理的金融数据，应事先采用数据脱敏
- ◆ 对委托处理的数据进行安全审计

### 共享

#### ◆ 内部共享

- 1) 应梳理数据共享的各类场景，明确各类场景的安全要求和责任部门，并建立相应的审核批准机制...
- 2) 共享前，开展数据安全影响评估
- 3) 应对2级以上的数据共享过程留存日志记录
- 4) 应对3级以上的数据进行脱敏
- 5) 不应共享4级数据
- 6) 利用自动化工具（如代码、脚本）进行共享时，应通过身份认证、数据加密、反爬虫机制等手段防范网络攻击
- 7) 共享前，约定使用期限...

#### ◆ 外部共享

- 1) 满足上述7点要求
- 2) 通过合同，明确双方在数据安全方面的责任及义务，约定共享数据的内容、用途、使用范围
- 3) 定期对数据接收方的安全保护能力进行评估
- 4) 向个人信息主体等告知共享目的、数据接收方类型，并事先征得相应授权...



# 目录

01 工作难点

02 合规要求

03 应对方法

个人信息收集的底线要求  
遵循合法、正当、必要原则  
明示规则；授权同意；按规收集、使用、存储等

## 具体要求1：明示个人信息收集处理规则

- 形式：简洁、显著、易懂的方式提醒用户阅读；涉及个人敏感信息，以显著方式强调
- 必要内容：产品/服务的基本业务功能/扩展业务功能下对应的各功能目的涉及个人信息类型及范围、收集、使用方式、涉及的系统权限功能；委托处理及共享的基本情况（包括目的、信息类型及范围、接收方的类型、数据保护能力等）；用户权利

## 具体要求2：根据业务场景确定获取个人信息主体同意的方式

### 授权同意：

- ❑ 明示同意（主动点击、主动勾选等方式）
- ❑ 默示同意

依据目前法律，需要获取明示同意的场景包括但不限于：

- ✓ 定向市场营销
- ✓ 收集个人敏感信息等

执法机关严厉打击“一揽子授权”的方式

## 具体要求3：获取个人信息的手段及方式合法合规

### 个人信息来源：

- ◆ 运营者主动收集
- ◆ 信息主体主动提供
- ◆ 第三方共享
- ◆ 通过爬虫等技术从公开渠道及第三方平台获取

保证个人信息来源合法合规性，具体要求：

- ✓ 是否充分告知，并依据具体情境获取授权同意
- ✓ 不涉及非法获取，购买
- ✓ 采用爬虫等技术符合相关合规性要求

收集手段应在隐私政策中清晰说明

## 公司场景

- ✓ 对全公司收集、使用、对外提供个人信息的场景进行调研、汇总
- ✓ 结合公司产品全周期和业务流程，确定收集、使用的目的
- ✓ 区分业务类型
- ✓ 区分签署方式

## 参考范本

- ✓ 国标：《个人信息安全规范》附录 D 个人信息保护政策
- ✓ 标杆企业隐私政策：支付宝、淘宝、微信、京东
- ✓ 集团兄弟公司：平安银行、平安普惠

## 合规要求

- ✓ 《移动金融客户端应用软件安全管理规范》：要求金融机构按照规范对App进行整改，并向中国互联网金融协会进行备案
- ✓ 《民法典》：根据《民法典》对格式条款的要求，设置平台协议、注册协议及隐私协议
- ✓ 《常见类型移动互联网应用程序必要个人信息范围规定》评估收集信息是否符合最小必要原则
- ✓ 注册协议、隐私政策等呈现时间延长，确保用户实际清楚了解各条款内容
- ✓ 注册协议、隐私政策尽量用通俗的语言，保证文本的易读性
- ✓ 在收集、使用个人金融信息时，各金融机构不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供金融服务无关的个人金融信息...



- ✓ **组织架构：**明确个人金融信息保护责任部门和责任人，明确安全岗位
- ✓ **内控制度：**集团制度 + 公司制度（个人金融信息保护、分类分级管理、脱敏管理、外包服务与外包合作机构管理、信息泄露安全事件应急处置、投诉与申诉处理）
- ✓ **人员管理：**员工上岗、离岗前的保密责任确认和访问权限配置、定期培训考核
- ✓ **外部监测：**对新出台的法律法规、监管要求、经典、热点案例进行实时监测；并进行解读；梳理汇总法律法规基线要求
- ✓ **合规检视：**根据法律法规监测，检视内部安全合规工作，或开展专项检查或整改工作
- ✓ **文本工具：**《隐私政策》；根据业务场景，制定个人信息安全相关的合同模板
- ✓ **合规审查：**针对制度制定、重要事项、合同签订等，进行评估并出具意见
- ✓ **管理评估：**对上述工作的落实情况和有效性进行定期评估，不断复盘检视，提升信息安全管理能力

# 应对方法-心得

## 主动学习

专业培训认证课程，  
如EXIN DPO，书籍，  
公众号

## 沟通交流

对内：加强与公司其他部门的  
沟通合作，有利于了解公司的  
真实情况，同时可以提升相关  
部门的意识

对外：多参加同业会议，多与  
同业沟通交流，避免闭门造车

## 专业机构

如条件许可，聘请  
外部专业机构，借  
助外力做好隐私保  
护工作

## 及时总结

定期梳理总结、  
复盘检视

## 国际数字化转型最佳实践管理峰会



珠海山竹科技是国内知名的专注于数据安全及隐私合规的培训机构和咨询机构，致力于培养国内DPO专家和讲师、打造国内首家跨律所、跨企业的集法律+IT+安全人员的综合性数据合规咨询平台，推动国内隐私和数据保护的相关立法和合规实践。目前培养了几百名DPO学员，授权讲师10名。

山竹科技数据合规团队为企业提供咨询评估和法律风险规避、体系落地建设、数据安全技术解决方案等综合性服务，资深项目团队均具有十多年世界500强或咨询公司的项目管理和实施经验。我们直接或间接辅导了多家企业的GDPR出海合规、ISO27001信息安全管理体系和ISO27701隐私保护管理体系的咨询及实施。

<http://www.mangosteen-zh.com>

联系我们：向老师 13823096461



# Thanks

## 感谢聆听