梆梆安全
BANGCLE

APP个人隐私合规介绍与工信部337专项解读

梆梆安全 | 张廷伦

稳 如 泰 山 · 值 得 托 付

目录

CONTENTS

01 | APP个人信息合规背景介绍

02 | 工信部337号文解读

03 | 个人隐私合规概况

04 | APP合规建议

01 合规背景介绍

事件驱动

2019年1月25日上午，中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，联合发布**《关于开展APP违法违规收集使用个人信息专项治理的公告》。**

2019年12月31日，四部委联合发布**《App违法违规收集使用个人信息行为认定方法》（下称认定方法）**

关于国内个人隐私保护监管的历史背景演化

2018年5月1日

《GB/T 35273 信息安全技术 个人信息安全规范》正式实施。

2019年1月25日

四部委联合发布**《关于开展App违法违规收集使用个人信息专项治理的公告》**。

2019年3月1日

App专项治理工作组发布**《App违法违规收集使用个人信息自评估指南》**。

2019年3月15日

市场监督管理总局、中央网信办关于开展App安全认证的公告。

2019年4月10日

三部门联合发布《互联网个人信息安全保护指南》

2019年5月28日

国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》。

2019年10月2日

国家互联网信息办公室发布《儿童个人信息网络保护规定》。

2019年10月18日

中国人民银行发布**237号文件 金融行业加强移动金融客户端应用软件安全管理**的通知。

2019年10月24日

信安标委发布GB/T 35273-2017《信息安全技术 个人信息安全规范》修订稿，公开征求意见。

2019年11月4日

工业和信息化部 **337号令 关于开展APP侵害用户权益专项整治工作的通知**

2019年12月31日

四部委联合发布**《App违法违规收集使用个人信息行为认定方法》**

2020年1月15日

移动互联网应用程序（App）收集个人信息基本规范，征求意见稿

待续.....

常态化的监管通报

关于侵害用户权益行为的APP（第一批）通报

根据《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》要求，我部按计划、分阶段、稳步推进APP侵害用户权益专项整治行动。专项行动得到了社会的广泛关注和相关企业的高度重视，在加强用户个人信息保护方面取得积极成效。自查自纠阶段共8000多款APP完成整改。在监督检查阶段，我部组织第三方检测机构对各大应用商店APP进行检查，对发现存在问题的百余家企业进行督促整改。

截至目前，尚有41款APP存在违规收集、使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等问题（详见附件），未完成整改。上述APP应在12月31日前完成整改落实工作，逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：存在问题的应用软件名单（第一批）

工业和信息化部信息通信管理局

2019年12月19日

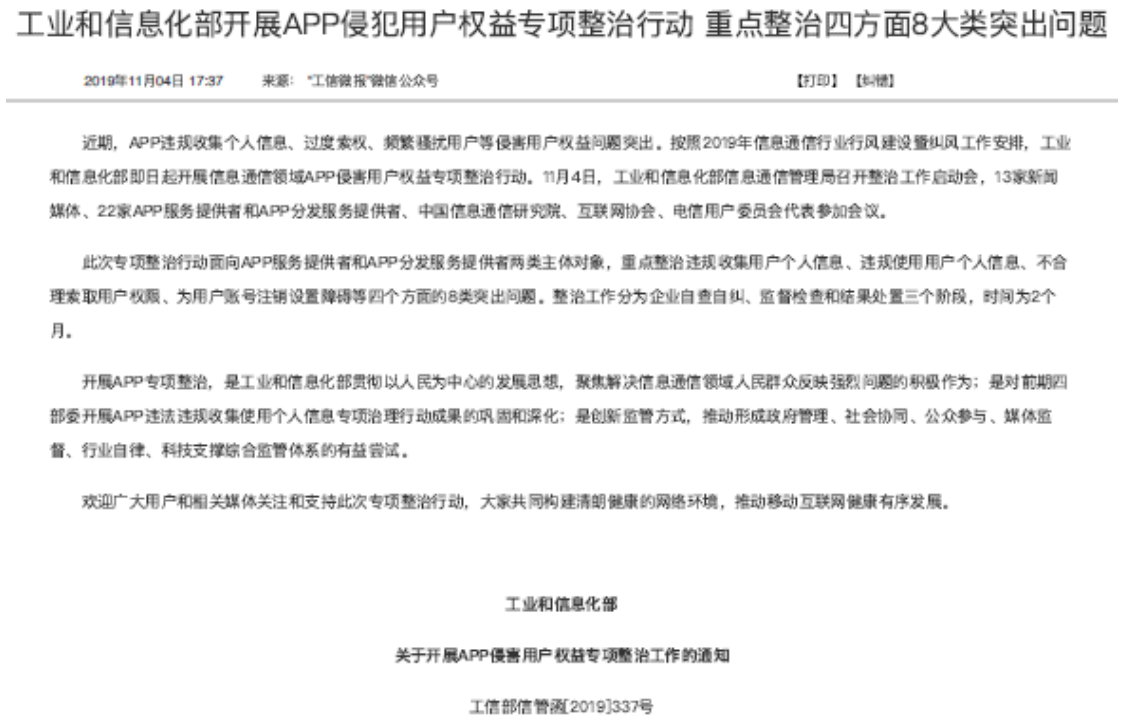
存在问题的应用软件名单（第一批）

序号	软件名称	企业名称	版本	版本来源	所涉问题
1	QQ	深圳市腾讯计算机系统有限公司	8.2.0	官网	强制用户使用定向推送功能 不给权限不让用 账号注销难
2	QQ阅读	上海阅文信息技术有限公司	7.1.1.888	官网	私自收集个人信息 私自共享给第三方 强制用户使用定向推送功能 账号注销难
3	新浪体育	新浪体育有限公司	4.3.3.0	官网	私自收集个人信息
4	小米金融	上海小米金融信息服务有限公司	7.4.4.2689	应用宝	账号注销难
5	搜狐新闻	北京搜狐新媒体信息技术有限公司	6.3.1	官网	私自收集个人信息
6	36氪	北京多氪信息技术有限公司	8.6.7	应用宝	私自共享给第三方

02

工信部337号文解读

工信部337号文内容概况



工业和信息化部开展APP侵犯用户权益专项整治行动 重点整治四方面8大类突出问题

2019年11月04日 17:37　　来源：“工信微报”微信公众号　　【打印】 【纠错】

近期，APP违规收集个人信息、过度索权、频繁骚扰用户等侵害用户权益问题突出。按照2019年信息通信行业行风建设暨纠风工作安排，工业和信息化部即日起开展信息通信领域APP侵害用户权益专项整治行动。11月4日，工业和信息化部信息通信管理局召开整治工作启动会，13家新闻媒体、22家APP服务提供者和APP分发服务提供者、中国信息通信研究院、互联网协会、电信用户委员会代表参加会议。

此次专项整治行动面向APP服务提供者和APP分发服务提供者两类主体对象，重点整治违规收集用户个人信息、违规使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等四个方面的8类突出问题。整治工作分为企业自查自纠、监督检查和结果处置三个阶段，时间为2个月。

开展APP专项整治，是工业和信息化部贯彻以人民为中心的发展思想，聚焦解决信息通信领域人民群众反映强烈问题的积极作为；是对前期四部委开展APP违法违规收集使用个人信息专项治理行动成果的巩固和深化；是创新监管方式，推动形成政府管理、社会协同、公众参与、媒体监督、行业自律、科技支撑综合监管体系的有益尝试。

欢迎广大用户和相关媒体关注和支持此次专项整治行动，大家共同构建清朗健康的网络环境，推动移动互联网健康有序发展。

工业和信息化部

关于开展APP侵害用户权益专项整治工作的通知

工信部信管函[2019]337号

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等法律法规和规范性文件要求，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，重点对以下四个方面开展规范整治工作。

（一）违规**收集**用户个人信息方面

（二）违规**使用**用户个人信息方面

（三）不合理**索取**用户**权限**方面

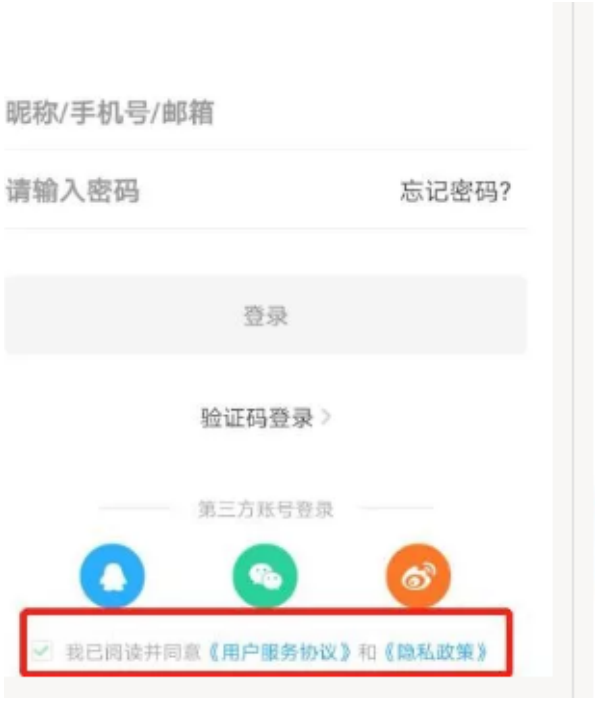
（四）为用户**账号注销**设置障碍方面

一、违规收集用户个人信息方面

(一)“**私自收集个人信息**”。即APP未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前收集用户个人信息。

典型场景1：APP运行时，**缺乏**向用户明示且征求用户同意的环节，收集IMEI、设备MAC地址、软件安装列表、通讯录、短信等个人信息。
典型场景2：APP运行时，虽然有向用户明示并经用户同意环节，但个人信息收集发生在用户**同意前**。

《网络安全法》明确指出，收集、使用个人信息，应明示收集、使用信息的目的、方式和范围，并经被收集者同意。前面提到，隐私政策是收集使用个人信息的规则，其中自然包含了收集、使用信息的目的、方式和范围，App们“两步并一步”，通过让用户同意“隐私政策”的方式，达到明示规则和征得同意两个要求,这种方式已经成为普遍现象和行业惯例。



有些App使用了“默认勾选”、灰色字体、遮挡等方式，未能显著提示用户。

有的App输入手机验证码的时候，键盘弹出就将隐私政策遮挡了。

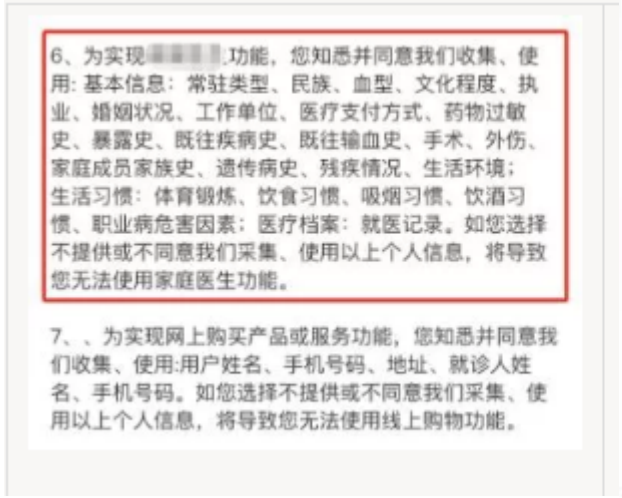
一、违规收集用户个人信息方面

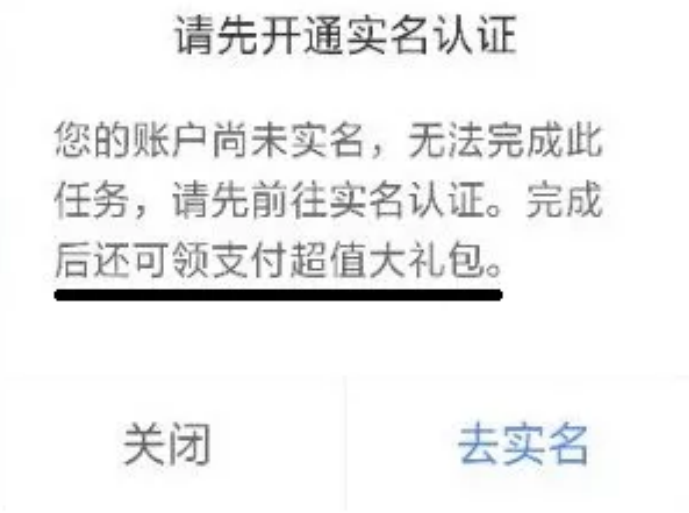
(二)“**超范围收集个人信息**”。即APP收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息。

典型场景1：APP收集个人信息，非服务所必需或无合理应用场景，**超范围**收集个人信息，如过度收集用户通讯录、短信、通话记录等。

典型场景2：APP收集个人信息，非服务所必需或无合理应用场景，**超频次**收集个人信息，如按照一定频次收集位置信息、IMEI或频繁读取通讯录、短信、图片等。

典型场景3：APP收集身份证号、人脸、指纹等个人信息时，**非服务所必需或无合理场景**，如将收集身份证号、人脸、指纹等作为应用开启使用的前提条件，或通过积分、奖励等方式诱导用户，收集身份证号、人脸、指纹等个人信息。





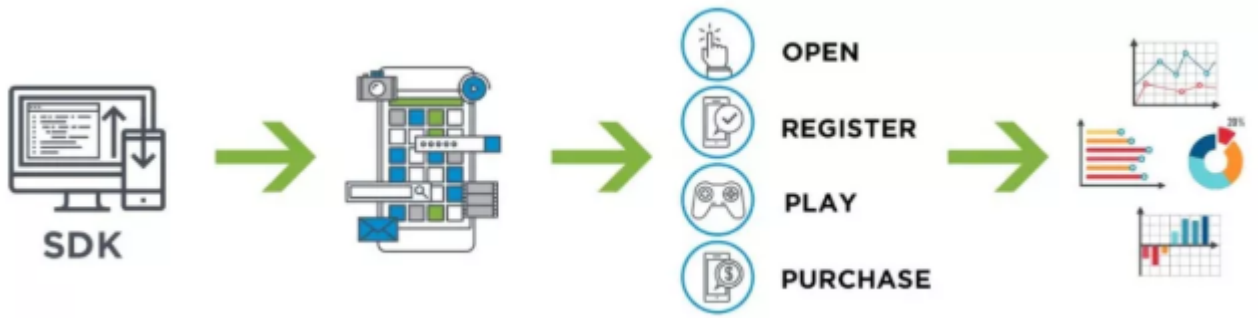
生活服务	休闲娱乐	超频率调用的 App 个数
设备识别码	100 次 / 分钟	59
定位	50 次 / 分钟	44
相机	10 次 / 分钟	3
通讯录	10 次 / 分钟	0
短信	10 次 / 分钟	1
麦克风	10 次 / 分钟	1

二、违规使用用户个人信息方面

(三)“**私自共享给第三方**”即APP未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

典型场景1：APP**未向用户告知且未经用户同意前**，将设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等个人信息直接发送给第三方SDK或第三方服务器。

典型场景2：APP未向用户告知且**未经用户同意**，将设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等共享给第三方，用户的商品浏览记录、搜索使用习惯等出现在第三方APP。



App开发者使用第三方SDK已经成为普遍现象。然而，第三方SDK自身存在的安全漏洞，以及隐瞒收集个人信息等问题

- **推送类SDK**

App开发者可以使用推送类SDK及时地向其用户推送通知或者消息，与用户保持互动，从而有效地提高留存率,提升用户体验。

- **广告类SDK**

广告类SDK对各类广告形式的支持情况成为影响App开发者收入的关键因素之一。

- **数据统计分析类SDK**

数据统计分析类SDK可以帮助App开发商统计和分析流量来源、内容使用、用户属性和行为数据，以便开发商利用数据进行产品、运营、推广策略的决策。

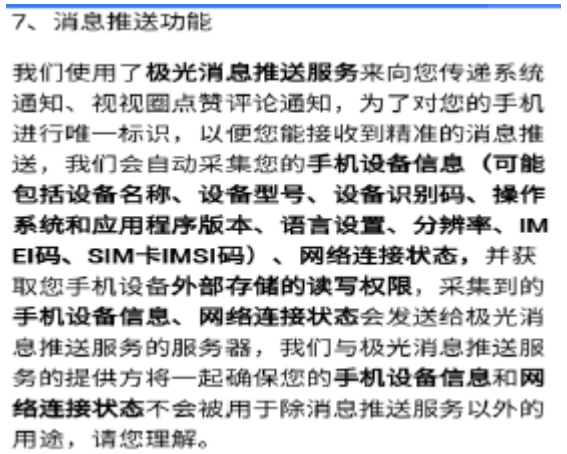
二、违规使用用户个人信息方面

(四)“**强制用户使用定向推送功能**”即APP未向用户告知,或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

典型场景1：APP的定向推送功能未向用户告知，将收集的用户个人信息用于定向推送、精准营销。

典型场景2：APP的定向推送功能未以显著形式标示。

典型场景3：APP的定向推送功能未对用户**提供关闭此功能的选项**。



7、消息推送功能

我们使用了**极光消息推送服务**来向您传递系统通知、视视圈点赞评论通知，为了对您的手机进行唯一标识，以便您能接收到精准的消息推送，我们会自动采集您的**手机设备信息（可能包括设备名称、设备型号、设备识别码、操作系统和应用程序版本、语言设置、分辨率、IMEI码、SIM卡IMSI码）、网络连接状态**，并获取您手机设备**外部存储的读写权限**，采集到的**手机设备信息、网络连接状态**会发送给极光消息推送服务的服务器，我们与极光消息推送服务的提供方将一起确保您的**手机设备信息**和**网络连接状态**不会被用于除消息推送服务以外的用途，请您理解。

隐私政策中对推送功能进行了描述，但未找到关闭推送的途径，且隐私协议中未声明。

三、不合理索取用户权限方面

(五)“**不给权限不让用**”即APP安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

典型场景1：APP首次启动时，向用户索取电话、通讯录、定位、短信、录音、相机、存储、日历等权限，用户拒绝授权后，应用退出或关闭。
典型场景2：APP运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

计算器为什么要获取我的位置权限？果断拒绝。

根据常识判断，计算器和位置权限“八竿子打不着”，而且计算器在申请位置权限时没有告知目的强制索要，显然不合理。

只能允许，没有其它选项，属于典型不给权限不让用。

这个APP是合规的

三、不合理索取用户权限方面

(六)“**频繁申请权限**”即APP在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

典型场景1：APP在运行期间，用户明确拒绝权限申请后，仍向用户频繁弹窗申请开启与当前服务场景无关的通讯录、定位、短信、录音、相机等权限。

(七)“**过度索取权限**”即APP在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

典型场景1：APP在**用户未使用**权限对应的相关功能或服务时，提前向用户弹窗申请开启通讯录、定位、短信、录音、相机等权限。

典型场景2：APP**未提供相关业务**功能或服务，仍申请通讯录、定位、短信、录音、相机等权限。

四、为用户账号注销设置障碍方面

(八)“**账号注销难**”即APP未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

典型场景1：APP未向用户提供账号注销服务。

典型场景2：APP为账号注销服务设置不合理的障碍。

即使提供“注销”功能已经成为App们的规定性动作，但还是有很多App没有提供注销功能。有的App明明在“隐私政策”中写明了可以注销，可要申请注销的时候，客服给出了各种理由，比如“请退出登录或卸载，能够保障安全劝别注销，功能加速研发中”

刻意隐蔽、藏匿注销入口，不让用户轻易找到。翻遍文本协议，终于找到了可以联系到的邮箱，结果邮件发过去后，被退信了。

03

个人隐私合规概览

个人信息保护合规法规体系

法律

1. 《宪法》 “公民的人格尊严不受侵犯，公民享有通信自由和通信秘密的权利，国家尊重和保障人权”
2. 《民法总则》
3. 《网络安全法》
4. 《刑法》“侵犯公民个人信息罪”

国标、行标

1. **GBT 35273《信息安全技术个人信息安全规范》**
2. GBT 22239-2019 《信息安全技术网络安全等级保护基本要求》
3. 《银行业第三方软件开发工具包（SDK）安全准入规范》
4. 《JRT-0092-2019 移动金融客户端应用软件安全》
5. 《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》
6. 《信息安全技术 移动智能终端个人信息保护技术要求》

指南、方法和规范

1. 《互联网个人信息安全保护指南》-公安部
2. 《App违法违规收集使用个人信息自评估指南》-_App专项治理工作组
3. **《App违法违规收集使用个人信息行为认定方法》** 》- App专项治理工作组
4. **《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》** - 信安标委
5. 网络安全实践指南-移动互联应用基本业务功能必要信息规范 - 信安标委
6. 信息安全技术 个人信息安全影响评估指南 - 信安标委

《信息安全技术 个人信息安全规范》体系结构

《个人信息安全规范》分为五个部分:

- **第一部分** 给出了规范使用的范围、规范性引用文件、相关术语和定义。
- **第二部分**提出了个人信息安全保障七大原则，
- **第三部分**是个人信息收集、保存、使用、委托处理、共享、转让和公开披露全生命周期的具体规范要求。
- **第四部分**是个人信息安全事件处置和组织的管理要求。
- **第五部分**是资料性附录，包括个人信息示例、个人敏感信息判定、保障个人信息主体选择同意权的方法、隐私政策模板。

前　言 III
引　言 IV
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 个人信息安全基本原则 4
5 个人信息的收集 4
5.1 收集个人信息的合法性 4
5.2 收集个人信息的最小必要 4
5.3 不强迫接受多项业务功能 4
5.4 收集个人信息时的授权同意 5
5.5 隐私政策 5
5.6 征得授权同意的例外 6
6 个人信息的保存 7
6.1 个人信息保存时间最小化 7
6.2 去标识化处理 7
6.3 个人敏感信息的传输和存储 7
6.4 个人信息控制者停止运营 7
7 个人信息的使用 7
7.1 个人信息访问控制措施 7
7.2 个人信息的展示限制 8
7.3 个人信息使用的目的限制 8
7.4 用户画像的使用限制 8
7.5 个性化展示的使用 9
7.6 基于不同业务目的所收集的个人信息的汇聚融合 9
7.7 信息系统自动决策机制的使用 9
7.8 个人信息查询 9
7.9 个人信息更正 10
7.10 个人信息删除 10
7.11 个人信息主体撤回授权同意 10
7.12 个人信息主体注销账户 10
7.13 个人信息主体获取个人信息副本 11
7.14 响应个人信息主体的请求 11
7.15 投诉管理 11
8 个人信息的委托处理、共享、转让、公开披露 12
8.1 委托处理 12
8.2 个人信息共享、转让 12
8.3 收购、兼并、重组、破产时的个人信息转让 13
8.4 个人信息公开披露 13
8.5 共享、转让、公开披露个人信息时事先征得授权同意的例外 13
8.6 共同个人信息控制者 14
8.7 第三方接入管理 14
8.8 个人信息跨境传输 14
9 个人信息安全事件处置 14
9.1 个人信息安全事件应急处置和报告 14
9.2 安全事件告知 15
10 组织的管理要求 15
10.1 明确责任部门与人员 15
10.2 个人信息安全工程 16
10.3 个人信息处理活动记录 16
10.4 开展个人信息安全影响评估 16
10.5 数据安全能力 17
10.6 人员管理与培训 17
10.7 安全审计 17
附　录　A　（资料性附录）　个人信息示例 18
附　录　B　（资料性附录）　个人敏感信息判定 19
附　录　C　（资料性附录）　实现个人信息主体自主意愿的方法 20
C.1 区分基本业务功能和扩展业务功能 20
C.2 基本业务功能的告知和明示同意 20
C.3 扩展业务功能的告知和明示同意 20
C.4 交互式功能界面设计 21
附　录　D　（资料性附录）　隐私政策模板 25
参考文献 32

《App违法违规收集使用个人信息行为认定方法》

一、 “未公开收集使用规则”

在App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

隐私政策等收集使用规则难以访问，如进入App主界面后，需多于4次点击等操作才能访问到；

二、 “未明示收集使用个人信息的目的、方式和范围”

有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

三、 “未经用户同意收集使用个人信息”

征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

四、 “违反必要原则，收集与其提供的服务无关的个人信息”

收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、 “未经同意向他人提供个人信息”

既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息

六、 “未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

《APP收集个人信息基本规范》

ICS 35.040
L80

GB

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 移动互联网应用程序（App）收集个人信息基本规范

Information security technology — Basic specification for collecting personal information in mobile internet applications

（征求意见稿）

2020-1-15

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

最小权限要求-2019年草案

序号	服务类型	最小权限范围
1	地图导航	位置权限、存储权限
2	网络约车	位置权限、拨打电话权限
3	即时通信	存储权限
4	博客论坛	存储权限
5	网络支付	存储权限
6	新闻资讯	无
7	网上购物	无
8	短视频	存储权限
9	快递配送	无
10	餐饮外卖	位置权限、拨打电话权限
11	交通票务	无
12	婚恋相亲	存储权限
13	求职招聘	存储权限
14	金融借贷	存储权限
15	房屋租售	存储权限
16	二手车交易	存储权限
17	运动健身	位置权限、传感器权限
18	问诊挂号	存储权限
19	浏览器	无
20	输入法	无
21	安全管理	存储权限、获取应用账户、读取电话状态权限、短信权限

最小权限要求-2020年征求意见稿

序号	服务类型	最小权限范围
1	地图导航	位置权限
2	网络约车	位置权限
3	即时通讯	存储权限
4	网络社区	无
5	网络支付	读取设备状态权限
6	新闻资讯	无
7	网上购物	无
8	短视频	存储权限
9	快递配送	无
10	餐饮外卖	位置权限
11	交通票务	无
12	婚恋相亲	无
13	求职招聘	无
14	金融借贷	无
15	房屋租售	无
16	二手车交易	无
17	运动健身	位置权限
18	问诊挂号	无
19	网页浏览器	无
20	输入法	无
21	安全管理	通话记录权限、短信权限、存储权限
22	旅游服务	无
23	酒店服务	无
24	网络游戏	无
25	在线影音	无
26	儿童教育	无
27	电子图书	无
28	拍摄美化	相机权限、存储权限
29	应用商店	存储权限
30	网络直播	存储权限

《APP收集个人信息基本规范》

最小必要信息要求

A.7 网上购物

为用户提供网上购买商品或服务的服务类型，包括商品展示、搜索、下单、交付、客服售后等功能。该服务类型的最小必要信息如表 7 所示：

表 7 网上购物类的最小必要信息

类型	个人信息	使用要求/相关法律法规依据
法律法规要求的个人信息	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《网络安全法》 《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
实现服务所需个人信息	账号信息 • 账号 • 口令	仅用于标识网上购物用户和保障账号信息安全。
	收货人信息 • 收货人姓名 • 收货人地址 • 收货人手机号码	仅用于网上购物收货时识别收货人、送达货物和联系收货人，以及完成客服与售后需要。
	第三方支付信息	仅用于用户使用第三方支付方式对网上购物订单付款，通常包括支付时间、支付金额、支付渠道等。
	仅在客服场景下收集： 客服沟通记录和内容 • 通话录音（电话客服） • 聊天消息（在线客服）	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

表 7 所列个人信息主要针对大众用户购物的普通场景，不包括为跨境电商通关、购买手机号等实名购买情景下需提供的用户身份信息，实名购物场景下通常需要收集用户的证件号码。在一些线上到线下（O2O）的购物场景中，由于需要判断用户所在的商场、所属的商圈范围等，可能还会收集用户的位置信息，应告知用户并获得用户授权同意。

“业务所需权限”是指紧密结合业务实际功能所需的权限，比如拍照、扫二维码等需要“相机”权限，查看附近的服务需要“位置”权限等。

不能在实现某种业务功能时，将开启权限作为唯一的实现方式，强迫用户打开权限。

《APP收集个人信息基本规范》要求

收集个人信息要求

App收集个人信息应满足以下要求：

a） App 运营者应履行个人信息安全保护义务，采取必要措施，保障个人信息安全；

b） App 应以制定隐私政策等方式公开收集使用个人信息规则；

c） App 应在首次运行时通过弹窗等明显方式向个人信息主体告知收集最小必要信息规则，如隐私政策的核心内容；

d） App 运营者不应在征得个人信息主体授权同意前，产生个人信息收集行为；

e） App 运营者不应在个人信息主体明确表示不同意后，仍通过技术等其他手段继续收集个人信息；

f） 当个人信息主体同意 App 收集某服务类型的最小必要信息时，App 运营者不应因个人信息主体拒绝提供最小必要信息之外的个人信息而拒绝提供该类型服务；

注：附录 A 列举了 App 常见的服务类型以及服务类型对应的最小必要信息。

g） 除法律法规的强制性要求外，App 运营者不应收集与所提供的服务无关的个人信息；

h） App 运营者不应收集不可变更的设备唯一标识（如 IMEI 号、MAC 地址等），用于保障网络安全或运营安全的除外；

i） 个人信息主体明确拒绝使用某服务类型后，App 运营者不应频繁（如每 48h 超过一次）征求个人信息主体同意使用该类型服务，并保证其他服务的正常使用；

注：个人信息主体主动触发导致的征求同意相关提示除外。

j） 在 App 运营者使用第三方代码或插件满足其特定功能时，如该第三方代码或插件具备个人信息收集功能且个人信息主体无法拒绝的，App 运营者应确保第三方代码或插件履行个人信息安全保护义务，并防止第三方代码或插件收集无关的个人信息；

注：如第三方代码或插件自行向个人信息主体明示其收集、使用个人信息的目的、方式、范围，并征得个人信息主体的授权同意，则第三方代码或插件独立对其个人信息收集行为承担责任。

不可变更的设备唯一标识示例

6类不可变更的设备唯一标识

1. **国际移动设备识别码（IMEI：International Mobile EquipmentIdentity）**，即通常所说的手机序列号、手机“串号”，用于在移动电话网络中识别每一部独立的手机等移动通信设备，相当于移动电话的身份证，IMEI号共有15~17位数字。
2. **移动设备识别码(MEID：Mobile Equipment Identifier)**是支持CDMA手机等移动通信设备唯一的识别码。MEID的数字范围是十六进制的，和IMEI号的格式类似。
3. **Android_ID**是运行安卓系统的手机等设备随机生成一串64位的号码，每一个Android_ID都是独一无二。
4. **设备序列号**（SN：SerialNumber）通常用于验证产品的出厂生产的正规性和合法性，也称作机器码、认证码、注册码，通常可在系统信息中的序列号一栏看到，不可更改。
5. **广告标识符**（IDFA：identifierForIdentifier）是苹果手机iOS 6及以上系统给广告商提供的追踪用户的标识符，广告标识符存储在手机系统中，可被每一个App获取。
6. **应用开发商标识符**（IDFV - Identifier For Vendor）是苹果iOS系统给App开发商生成的唯一性标识符，同一个开发商开发的不同的App获取的IDFV值相同，常用于自开发App及跨App追踪用户行为。

违规案例二则

一、金融行业237号文违规案例

评估结果	不符合，一般。 1、[redacted]未对 TalkingData SDK 开展技术检测； 2、[redacted]未对 TalkingData SDK 收集个人信息的行为进行审计
整改建议	1、对 TalkingData SDK 开展技术检测，并形成安全检测报告； 2、对 TalkingData SDK 收集个人信息的行为进行审计，并形成行为审计报告；

评估结果	**不符合，严重。** 当前会与北京 CA、短信网关传输个人敏感信息，但是未获得用户的明示同意。
整改建议	1、在高端理财专区内签署协议前，向用户告知会将其信息用于申请个人数字证书，并获得同意（可以是单选框，但默认不选中）； 2、在注册时向用户告知会将其信息共享至短信网关，并经得用户明示同意后再发送短信（可以是单选框或按钮）

二、APP侵害用户权益专项整治工作案例

附件：

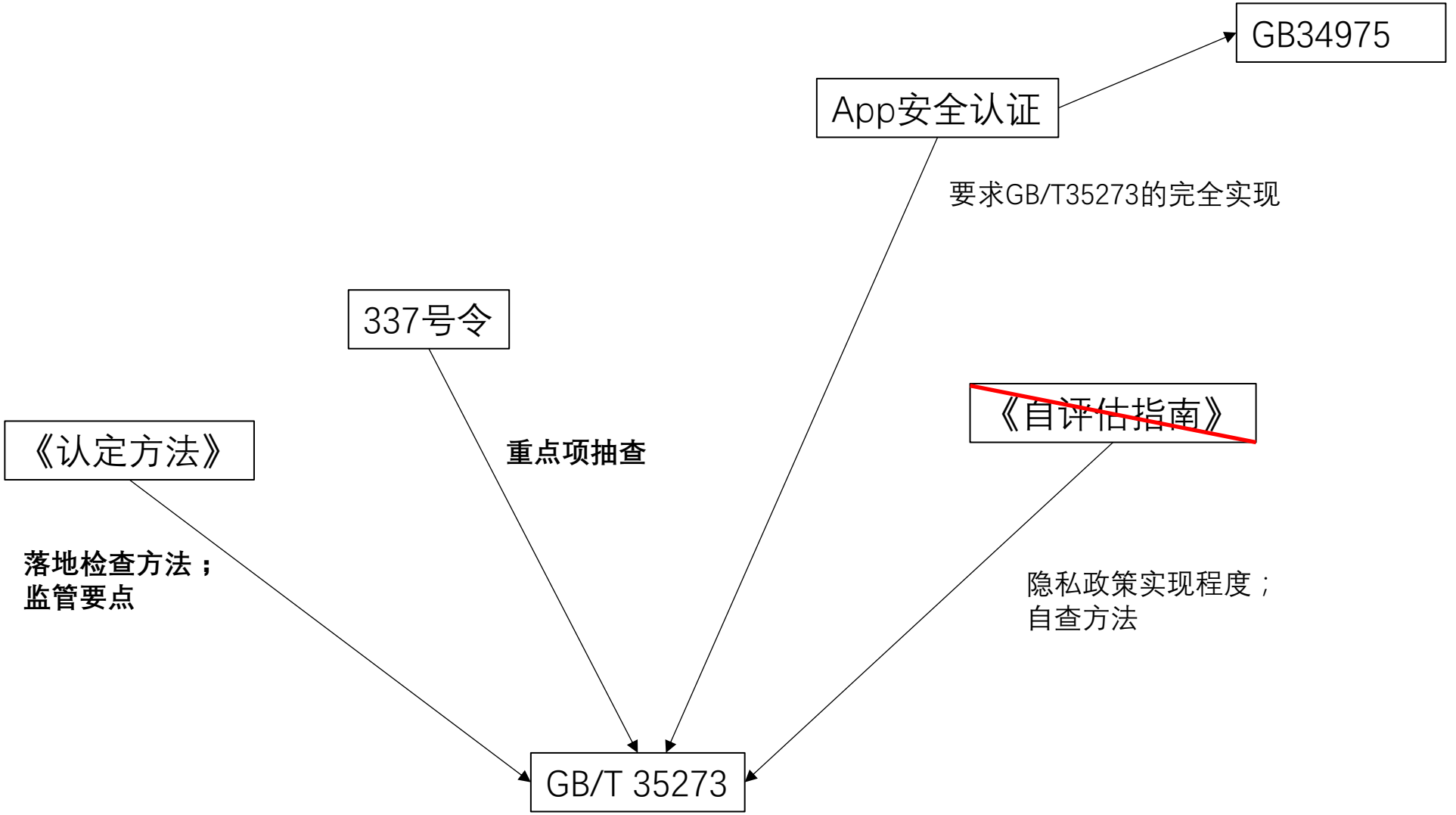
APP 侵犯用户权益专项行动检测企业问题列表

企业名称	APP 名称	版本号	应用问题	问题描述
[redacted]			（一）私自收集个人信息	APP 首次开启时，在向用户明示个人信息收集使用规则且用户同意前，存在收集 MAC 地址、应用软件列表、IMEI、定位信息等个人信息的行为。
			（三）私自共享给第三方	APP 未向用户告知且未经用户同意前，存在将个人信息直接发送给魅族等第三方服务器的行为。
			（五）不给权限不让用	APP 首次启动时，向用户索取电话权限，用户拒绝授权后，应用陷入弹窗循环，无法正常使用。

04

APP合规建议

认定方法、337、安全认证、自评估指南的关系



企业合规步骤建议

优先认定方法（已包含337），建议拿认证

建立合规专项项目组

- 建立包含研发，测试，安全，商务及法务在内地虚拟项目组
- 确定合规App范围

现状调研及差距分析

- 管理类要求调研
- 技术类要求调研及测试
- 商务类要求调研
- 法务类要求调研

基于认定方法和GB35273要求，明确：

1. 符合项目，不符合项及不适用项
2. 问题严重等级

定义目标及整改方案

基于企业规模，预算及人力资源，在满足合规要起的前提下，定义目标及整改方案。

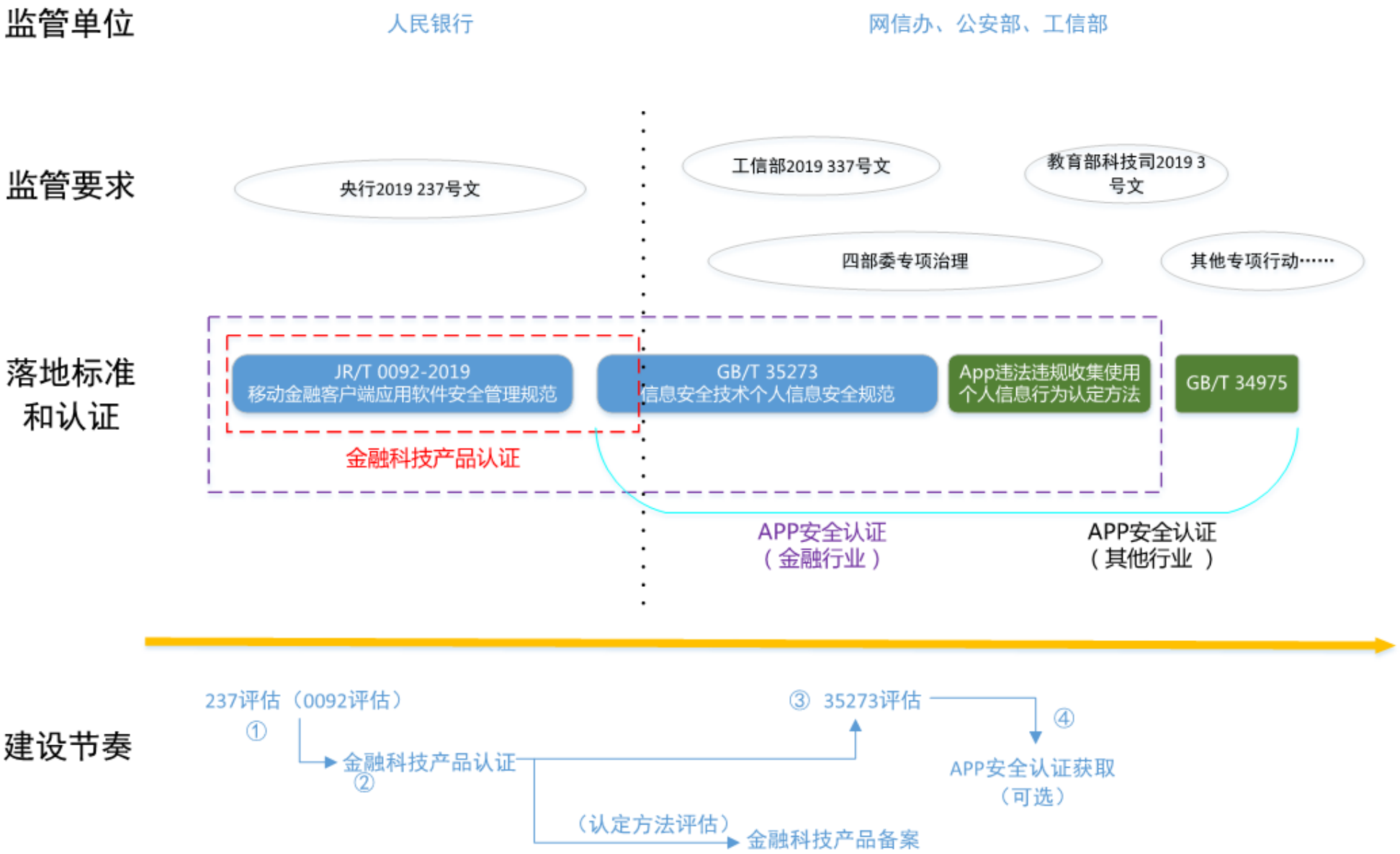
- 自行整改
- 外部服务
- 外部产品
- 问题存留不处置

持续合规应对

企业建立应对合规的工作机制及技术能力，持续性满足合规要求：

- 安全认证
- 工具及平台
- 内生安全能力及人才培养
- 管理制度及安全流程的落地

不同行业的推荐合规路径



扫一扫上面的二维码图案，加我微信

THANK YOU