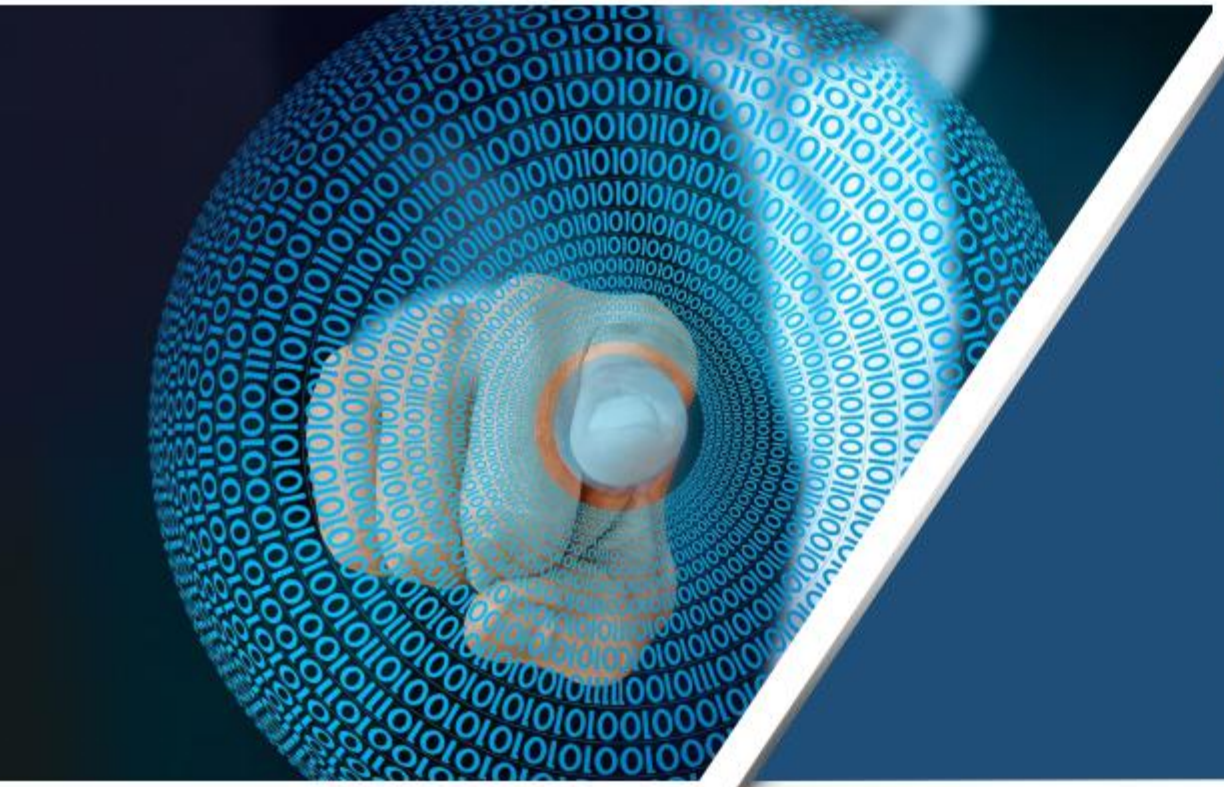


安世加

第 二 十 六 期 沙 龙 之
企 业 安 全 创 新 技 术 （ 线 上 ）

2021. 1. 08

App隐私合规实践

正保远程教育 李晨

00 个人介绍

李晨，在线教育行业，正保远程教育安全负责人

工作：多年甲方安全工作实践，具备金融、车联网、教育行业工作经验

重保：整体负责2018年甲方护网安防工作，成功防守。

撰文：《一个人的安全建设之路》，讲述甲方安全人员不足时方法论与实践

创始人：清流派安全沙龙，目前于北京定期举办线下交流

资质：CISSP（信息系统安全认证专业人员）

目录

01 App隐私合规背景

2017年——《网络安全法》

1、网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息

2、网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。

2020年7月 App违法违规收集使用个人信息治理工作启动会在京召开

1、制定发布SDK、手机操作系统个人信息安全评估要点。

2、针对面部特征等生物特征信息收集使用不规范，App后台自启动、关联启动、私自调用权限上传个人信息，录音、拍照等敏感权限滥用等社会反映强烈的重点问题，开展专题研究和深度检测。

3、对违法违规收集使用个人信息行为加大发现力度、曝光力度、处罚力度。

4、发布免费技术工具，指导中小企业开展个人信息收集使用行为自评估，提升中小企业个人信息收集使用活动的合法合规性。

5、推进App个人信息安全认证工作，有序开展认证证书和标识发放，建立持续动态的认证跟踪机制。

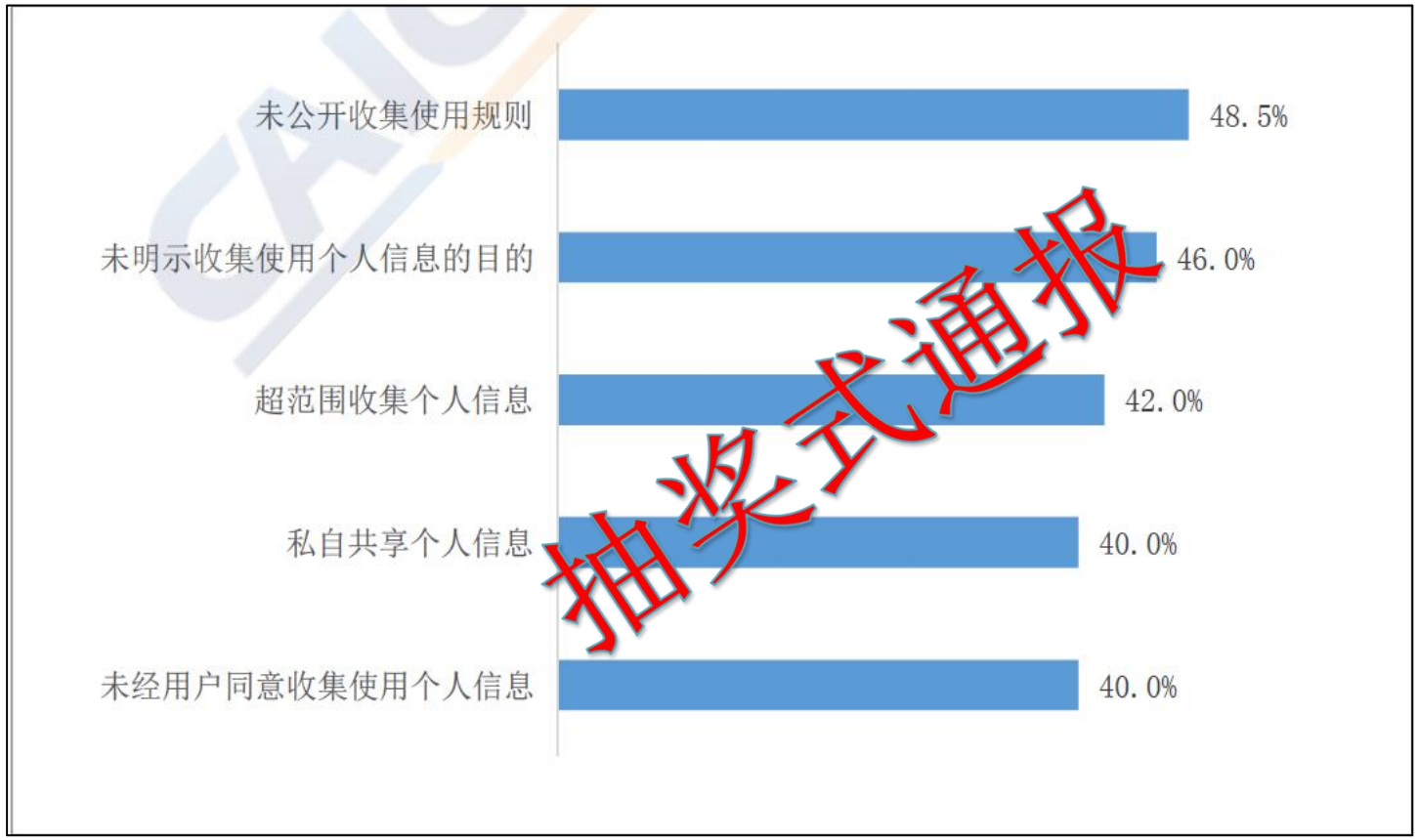
02 App隐私合规监管情况

主管部门	主管司局
工信部	通信管理局
	网络安全管理局
公安部	网络安全保卫局
	广东省公安厅
中央网信办	网络安全协调局
市场监督总局	认证监督局

02 App隐私合规监管情况

关于侵害用户权益行为的APP通报

- 第一批：2020年5月15日　16个
- 第二批：2020年7月3日　15个
- 第三批：2020年7月24日　58个
- 第四批：2020年8月31日　101个
- 第五批：2020年10月26日　131个
- 第六批：2020年12月3日　60个



03 隐私合规检测方案

03 合规检测依据

相关标准规范与自评估指南

《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》

描述了多个行业最小权限举例

《App违法违规收集使用个人信息自评估指南》

用于自评估隐私规范的Checklist

《移动互联网应用程序（App）收集使用个 人信息自评估指南-2020》

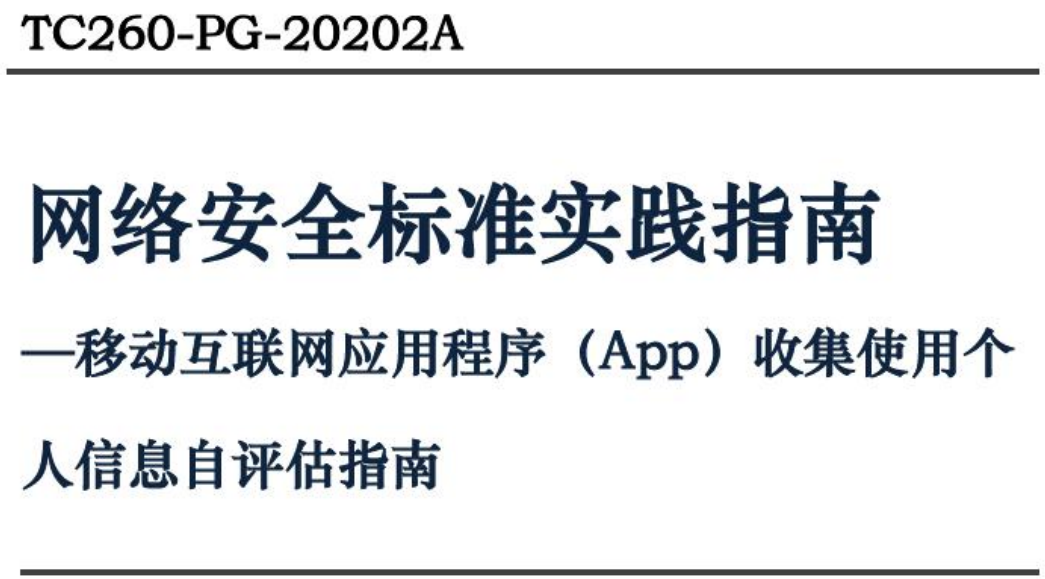
最新版自评估Checklist

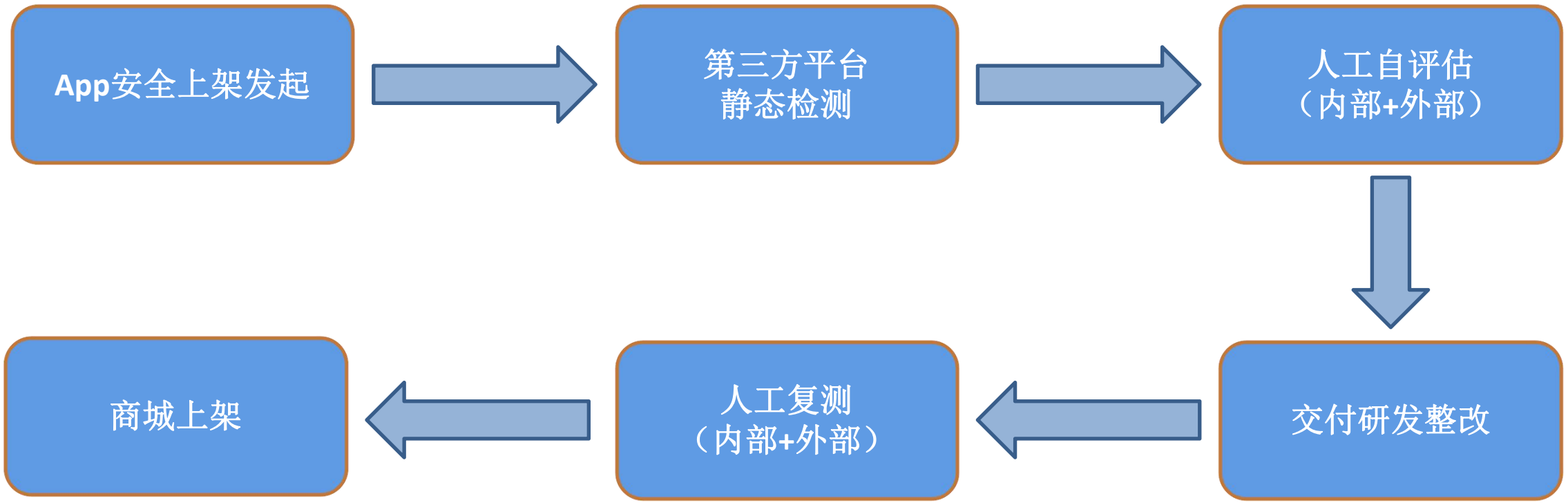
《App违法违规收集使用个人信息行为认定方法》

描述了7类App违规的形式

《GBT35273-2020信息安全技术个人信息安全规范》

解释了各种权限的征集方法以及个人敏感信息列表



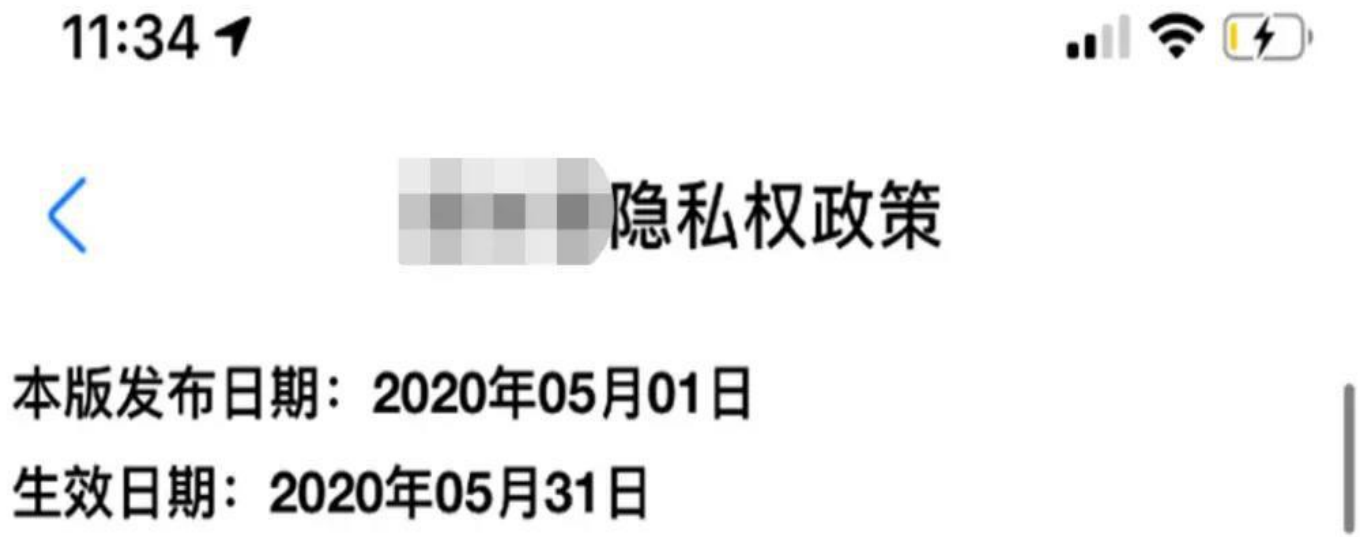

App安全上架发起
第三方平台
静态检测
人工自评估
（内部+外部）
交付研发整改
人工复测
（内部+外部）
商城上架

04 合规整改与总结

04 整改与总结

隐私政策发布与生效时间

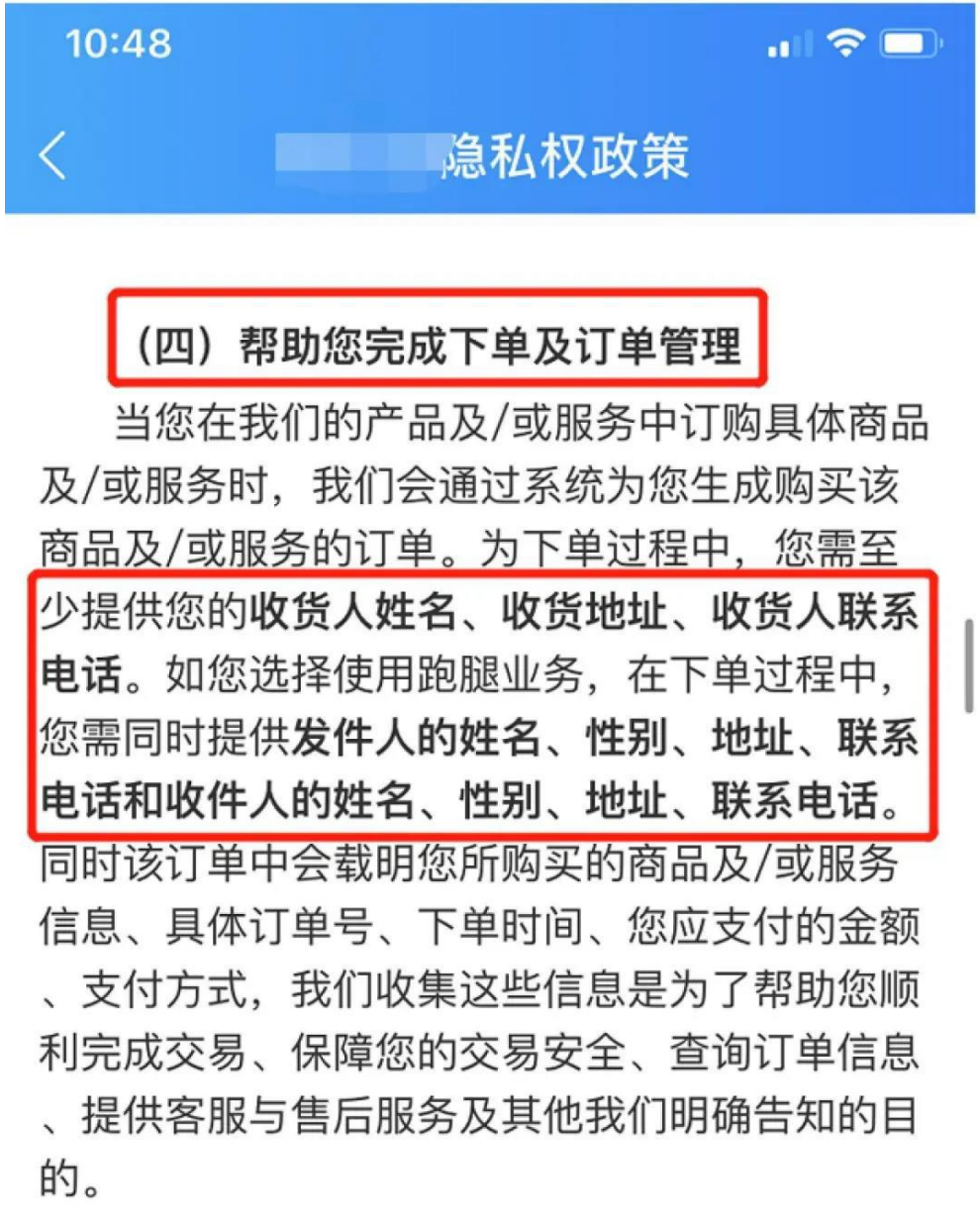
隐私政策注明发布/生效日期是一种规范化的体现，作为公开的规则，如果无法进行透明化的内容变更和有序的版本管理，其公信力恐怕要大打折扣。此外，随着法律法规的不断出台和规则的细化，对隐私政策提出了更多要求，产品也会因为更新换代在个人信息收集使用规则上有所变化，因此，适时、合理更新隐私政策也是一种个人信息保护工作得到重视和常态化的体现违规收集使用个人信息



04 整改与总结

查看业务功能及收集的个人信息

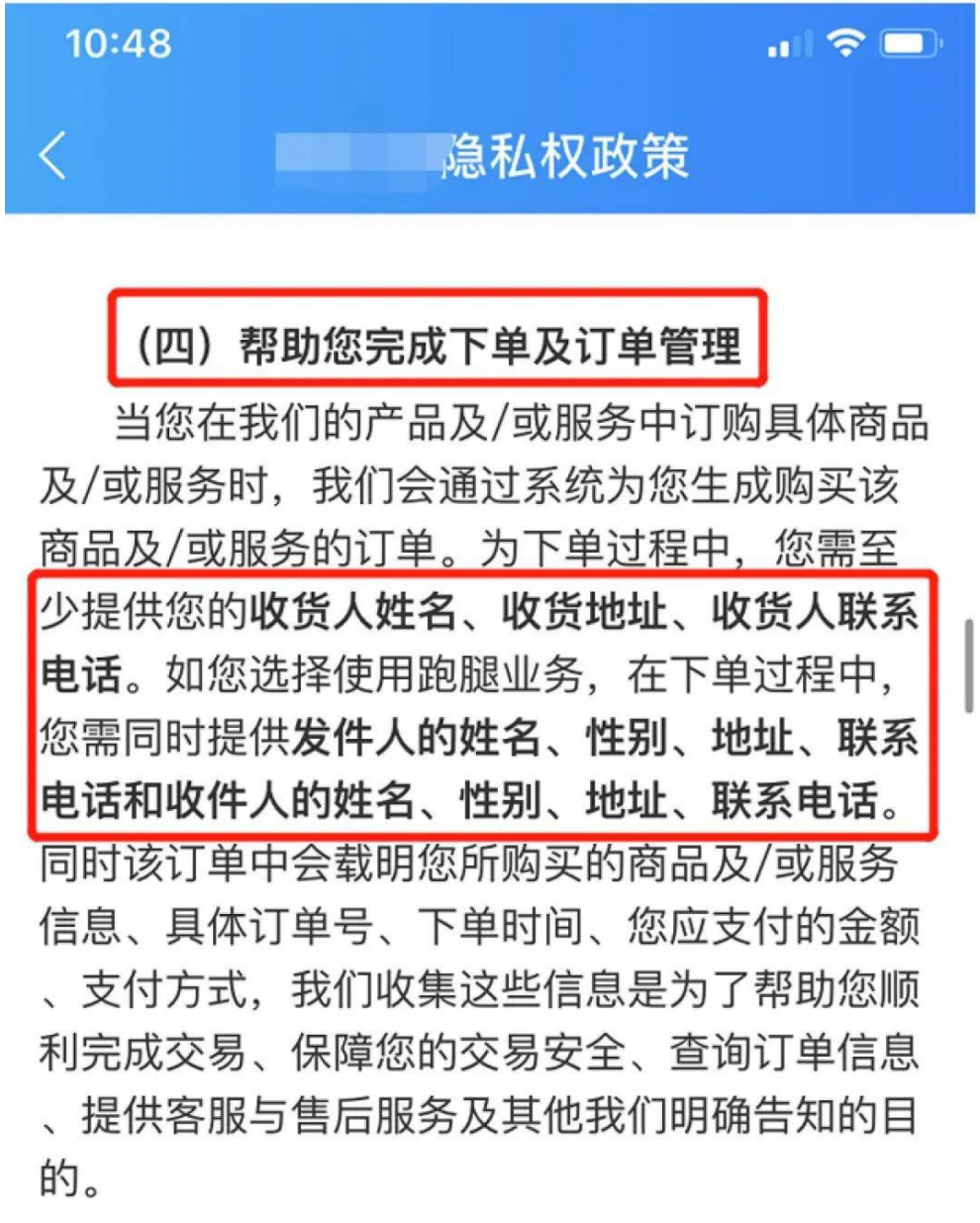
收集规则是用户关心的焦点，也是隐私政策的重点内容。因此，该部分的介绍既要详细也要明了，比如将业务功能根据用户使用App的习惯进行分类，便于用户找到自己所关心的部分了解其收集的个人信息。如果将业务功能混杂在一起，则收集个人信息的目的交代会变得含糊，对用户理解构成干扰。如下图展示了“下单及订单管理”业务所需要收集的个人信息范围，清晰的向用户展示了业务功能与所收集的个人信息的对应关系。



04 整改与总结

查看阅读加黑、加粗等内容

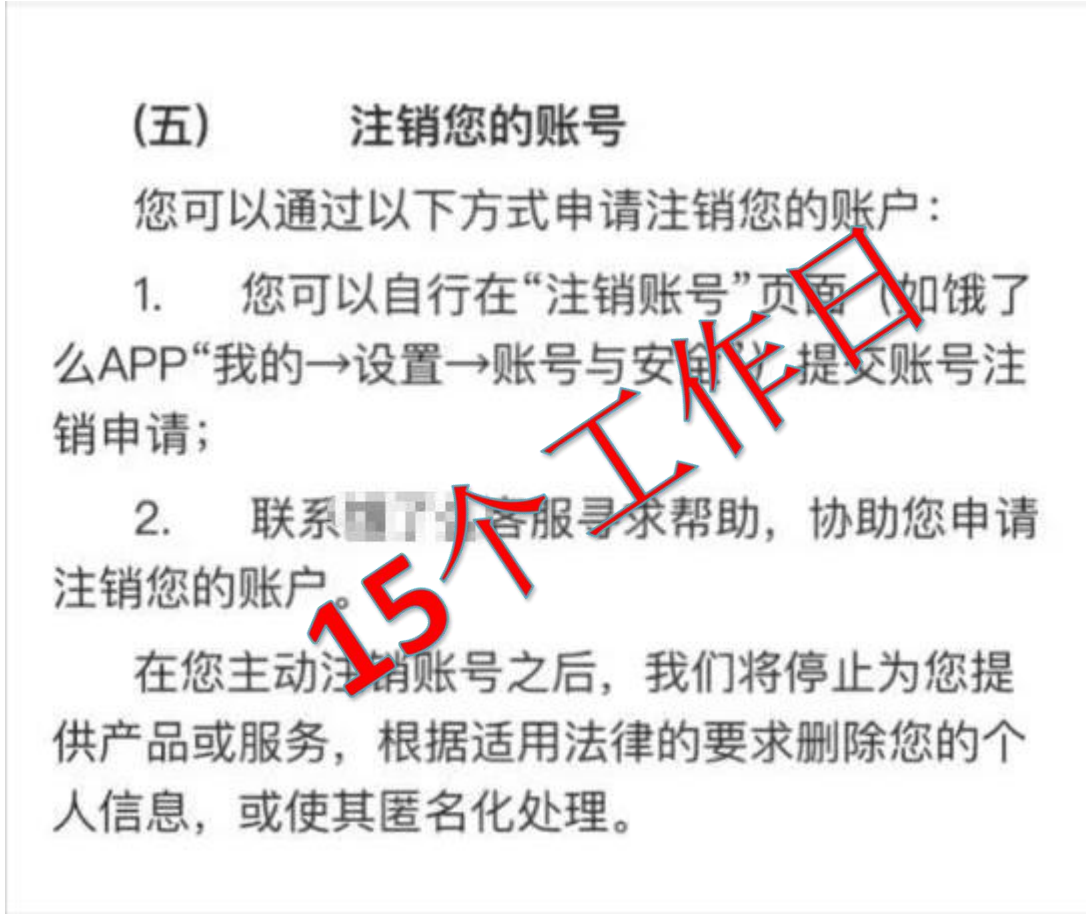
隐私政策通常会对提及的个人敏感信息通过加黑、加粗、下划线等显著方式进行标识，以强调内容的重要性，提醒用户着重关注。如下图可以看出“收件人的姓名，性别、地址”等个人敏感信息已经加黑。用户可以通过查看该部分内容迅速判断个人敏感信息是否可能被强制、过度收集。



04 整改与总结

用户注销账户的权利

当用户决定账号不再使用时，如不注销，则绑定的姓名、手机号、身份证号、地址等个人敏感信息会长期保留，是否会被滥用或泄露将是个未知数。通常，用户可以查看隐私政策中关于用户注销账号的步骤等内容，如下图所示。如果隐私政策未提及注销账号，则大概率该App未提供该功能，注册使用该App则可能面临无法注销账户的境地。



04 整改与总结

查看投诉举报渠道

App建立有效的投诉举报渠道，及时处理用户的投诉建议，是对用户负责任的一种重要体现。如下图中App既有个人信息保护专职部门邮箱地址，也有儿童个人信息保护客服。如果App未能提供投诉举报渠道，一旦个人信息方面出现问题很难得到响应和解决。

九、 如何联系我们

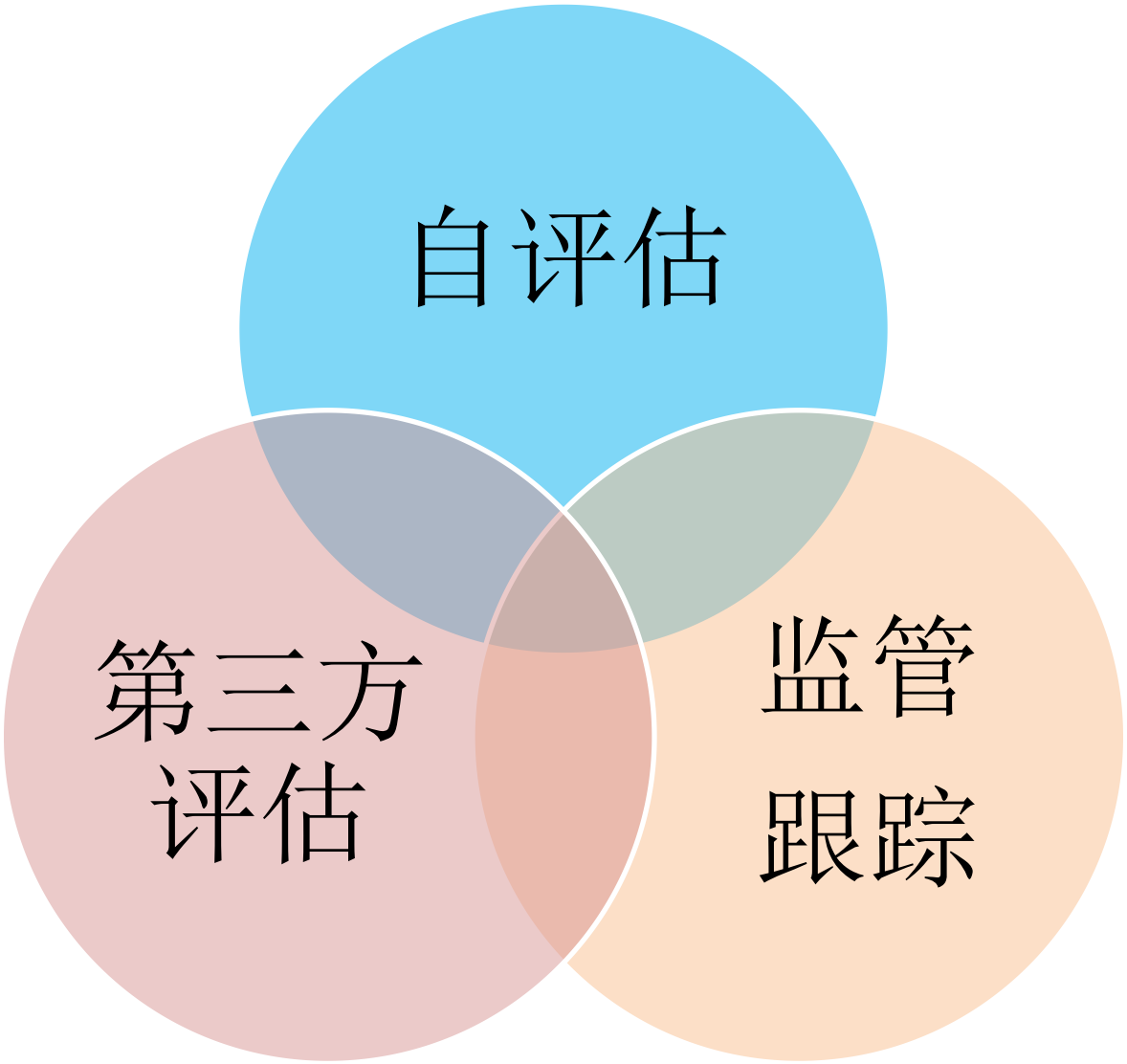
您可以通过以下方式与我们联系，我们将在15天内回复您的请求：

1. 如对本政策内容、儿童个人信息保护有任何疑问、意见或建议，您可通过[redacted]客服与我们联系；

2. 如发现个人信息可能被泄露，您可以通过[redacted]客服（[redacted]）投诉举报；

3. 我们还设立了个人信息保护专职部门，您可以通过[redacted]其联系，我方收件地址：[redacted]

4. 如果您对我们的回复不满意，特别是您认为我们的个人信息处理行为损害了您的合法权益，**您还可以通过向被告住所地有管辖权的法院提起诉讼来寻求解决方案。**


自评估
第三方
评估
监管
跟踪

尽力而为

安世力口专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、 人才招聘等多种形式，
致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：https://www.anshijia.net.cn

微信公众号：asjeiss