# App个人信息保护团体标准编制说明

1. 背景

随着国家关于个人信息保护配套的法律法规不断颁布实施，各主管部门对于App个人信息保护的监管要求陆续完善，监管态势日趋严格。但由于App个人信息保护合规工作涉及法律法规、技术开发、软件设计，甚至还要排查第三方应用或SDK的合规性，对于大量中小企业而言，存在安全意识不到位、政策理解不准确、问题排查不全面、开发设计不合理、应用整改不到位等诸多问题，面对监管部门的通报，时间紧、任务重，不知如何整改，导致下架和处罚，进而可能面临经济、社会声誉等方面的损失。

云南互联网行业发展较外省发达区域起步晚，缺少深厚的行业经验和实践沉淀，加之App个人信息保护合规管理需要相应的技术、法律和管理专业人才，导致云南省内互联网相关企业，特别是中小微企业面临更高的学习和管理门槛、更大的合规管理压力和法律风险，难以做好App个人信息保护的合规管理。为此，希望该标准的制定能够帮助云南省内企业降低App个人信息保护方面的学习和管理成本，提升企业的个人信息保护能力和合规管理水平，规范企业App个人信息处理活动，落实对个人和组织合法权益的保护，助力营造良好的营商环境，促进企业和行业健康发展。

1. 思路和创新点

针对App个人信息保护监管要求，本标准以《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国反电信网络诈骗法》《关键信息基础设施安全保护条例》等法律法规为基础，结合GB/T 37964-2019、GB/T 25273-2020、GB/T 41391-2022 、GB/T 42460-2023等本领域主要国家标准和相关行业标准、团体标准的要求，充分吸收电信运营商、互联网企业、安全企业等App运营单位在合规治理工作方面的经验，借助网络安全企业、高校、律师事务所专业力量，涵盖App在个人信息的收集、存储、使用、加工、传输、提供、公开、删除的全生命周期的合规规范，梳理一套标准化、体系化、可落地、可扩展的合规标准框架，形成云南省互联网协会团体标准《信息安全技术 移动互联网应用程序(App)个人信息保护合规指南 总则》，以期为中小企业减轻合规成本，为相关部门监管提供参考，切实保障用户合法权益。后续将根据工作需要，在各细分方向作更深入的研究。

1. 主要工作内容
	1. 范围和术语定义

本标准规范的范围覆盖App个人信息处理的全生命周期基本规则、技术规范和管理要求，规范性引用GB/T 37964-2019、GB/T 25273-2020、GB/T 41391-2022 、GB/T 42460-2023，为了便于理解，术语定义从基础的技术概念、个人信息分类、个人信息全生命周期流程等方面进行了列举。

1. 直接引用

术语和定义总共有 36 个，其中直接引用的术语和定义有18个，包括：

* 移动互联网应用程序
* 业务功能
* 基本业务功能
* 扩展业务功能
* 必要个人信息
* 个人信息主体
* 用户
* 删除
* 微数据
* 标识符
* 直接标识符
* 准标识符
* 重标识
* 完全公开共享
* 受控公开共享
* 领地公开共享
* 重标识风险
* 定向推送
* 服务类型
* 个人信息
* 个人敏感信息
* 公开
* 匿名化
* 去标识化
* 第三方应用
1. 新增补充

本团标新增术语补充说明总计 11 个，包括：

* 移动互联网应用程序提供者：根据《中华人民共和国个人信息保护法》统一将运营者改为提供者

|  |  |
| --- | --- |
| **术语：移动互联网应用程序提供者** | 移动互联网应用程序的所有者、开发者或运营者，简称 App 提供者。 |

* 个人信息处理：根据《中华人民共和国个人信息保护法》进行补充

|  |  |
| --- | --- |
| **术语：个人信息处理** | 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等行为。 |

* 个人信息处理者：根据《中华人民共和国个人信息保护法》进行补充

|  |  |
| --- | --- |
| **术语：个人信息处理者** | 在个人信息处理活动中自主决定处理目的、处理方式的组织和个人。 |

* 收集：结合《中华人民共和国个人信息保护法》，对收集进行定义。

|  |  |
| --- | --- |
| **术语：收集** | 直接或间接获取个人信息的行为 |

* 存储：结合《中华人民共和国个人信息保护法》，对存储进行定义。

|  |  |
| --- | --- |
| **术语：存储** | 记录或保存个人信息的行为。 |

* 使用：结合《中华人民共和国个人信息保护法》，对使用进行定义。

|  |  |
| --- | --- |
| **术语：使用** | 利用个人信息实现个人信息处理者或个人信息主体的特定目的的过程。 |

* 加工：结合《中华人民共和国个人信息保护法》，对加工进行定义。

|  |  |
| --- | --- |
| **术语：加工** | 对个人信息进行判别，筛选，分类，排序，分析和再造的过程。 |

* 传输：结合《中华人民共和国个人信息保护法》，对传输进行定义。

|  |  |
| --- | --- |
| **术语：传输** | 个人信息在业务功能系统之间流转的过程。 |

* 提供：结合《中华人民共和国个人信息保护法》，对提供进行定义。

|  |  |
| --- | --- |
| **术语：提供** | 个人信息在个人信息处理者和其他组织或个人之间传递的过程，包括委托处理、共享和转让。 |

* 自启动：结合 GB/T 41391-2022，对自启动进行定义。

|  |  |
| --- | --- |
| **术语：自启动** | 移动互联网应用程序自动启动的行为。 |

* 关联启动：结合 GB/T 41391-2022，对关联启动进行定义。

|  |  |
| --- | --- |
| **术语：关联启动** | 在一个移动互联网应用程序打开时，其他关联的应用程序自动启动的行为。 |

* 1. 个人信息处理基本原则

结合相关法律法规和国标，从个人信息处理的合法、合规、合理、合适几个角度梳理了8条原则，分别是合法正当原则、目的明确原则、告知同意原则、最小必要原则、公开透明原则、安全保障原则、主体参与原则和用户设计原则。相比于GB/T 35273-2020，站在 App 提供者的角度，补充了合法正当、告知同意、安全保障和用户设计4条原则，每条原则都有相应的解释说明，更清晰和直观，便于读者理解。

* 1. 个人信息的收集

相比国标 GB/T 35273-2020 和 GB/T 41391-2022，本标准从 App个人信息收集的整个流程和对应的收集信息进行详细说明。

在明确收集范围和需求中，整合并提炼了GB/T 41391-2022中收集相关的内容。收集个人信息前，需要明确 App 的服务类型，划分基本业务功能和扩展业务功能，并确定必要个人信息范围和使用要求。然后，按照服务类型确定收集的特定信息和系统权限。

在个人信息告知同意中，补充了隐私政策和双清单相关的要求说明，并对其内容要求进行了相应的量化，如字号、字体等要求，让 App 提供者能明白如何构建合规的隐私政策和双清单。

在通用要求中，详细阐述了收集前、收集中的具体事项，并对告知的形式做了举例，同时对频繁收集进行了量化的定义，方便理解。

对于个人敏感信息的说明中，从隐私政策到应用收集时注意的事项进行列出，将“单独同意”的交互形式进行了举例说明，同时将未成年人个人信息作为单独项目进行强调说明。

本标准还为间接获取个人信息、第三方应用收集个人信息的情况进行说明。同时在其他要求处新增了剪切板、更改用户个人信息权限状态、推荐下载 App 时的事项，补充了自启动和关联启动的说明。

* 1. 个人信息的存储

本标准相比国标 GB/T 35273-2020，增加了个人信息存储的类型和数量，引入最小必要原则，同时强调了存储期限和存储地点，列举了不通过法律法规对于存储期限的额外要求，补充了个人信息存储的其他要求，让个人信息存储指引更加完善。

* 1. 个人信息的使用

本标准相比国标 GB/T 35273-2020，个人信息的使用单独作为一个章节，涵盖了个人信息主体的使用和个人信息处理者的使用范围，聚合了个人信息的的展示、查询、更正、撤回、副本、访问控制以及投诉举报建议，在访问控制模块补充了制度建立，在更正模块补充了人工更正和时限，在举报投诉建议模块增加了入口说明和处理时限，同时在其他要求补充了 App 在个人信息使用时的相关事项。

* 1. 个人信息的加工

本标准相比国标 GB/T 35273-2020，对用户画像、个性化展示、自动决策机制补充了要求，新增了人工智能模块，对人工智能处理个人信息进行约束，同时在其他要求补充了个人信息加工的额外要求。

* 1. 个人信息的传输

本标准相比国标 GB/T 35273-2020，增加了个人信息跨境传输的说明，针对 App 中的个人信息传输，详细列举了多种安全传输方式，同时对采用第三方 SDK 传输进行了要求说明。

* 1. 个人信息的提供

本标准相比国标 GB/T 35273-2020，将个人信息的委托处理、共享、转让、共同处理、收合并、充足、解散、破产时的个人信息转让统一归为个人信息的提供，同时在委托处理、共享、转让的模块里补充了 App 提供者在提供个人信息时的义务，如建立提供方名单，建立安全评估和审计机制等。

* 1. 个人信息的公开

本标准相比国标 GB/T 35273-2020，补充了不同公开类型下，对去标识化的要求，同时增加了个人信息涉及跨境公开时的情况说明。

* 1. 个人信息的删除

本标准相比国标 GB/T 35273-2020，将个人信息的删除细分为违规处理用户个人信息、个人信息的注销、用户个人信息保存期限已届满三种情况进行阐述。违规处理用户个人信息分为违规收集使用、违规对外提供和违规公开披露；个人信息注销从注销入口、注销操作、注销时限等方面更加详细说明了注销的要求，补充说明了注销后个人信息删除遵循的原则，比GB/T 35273-2020 更为严格；用户个人信息保存期限已届满的情况为本标准补充阐述。

* 1. 个人信息合规管理要求

个人信息合规管理要求从组织内部管理的角度对个人信息保护进行阐述，汲取了《个人信息保护法》、工信部24号令、164号文、191号文以及部分App运营单位的实际管理经验，更有可行性和落地性。该部分包括组织保障和工作机制，组织保障从组织架构、角色职责两个方面概述，工作机制则建立了六项机制：合规管理机制、合规评估机制、安全保障机制、内部审计机制、外部审计机制、培训演练机制，每项机制都阐明需要做的工作内容，便于企业理解和学习。

* 1. 附录

附录从基础知识、常见技术、监管形势和法规政策标准索引四个层面涵盖了App个人信息合规的相关指导性材料，包括个人信息和个人敏感信息界定、去标识化与匿名化、个人信息的监管与法律责任、个人信息保护相关法律和司法解释、部门规章和标准文件索引。

个人信息和个人敏感信息通过将上述两类个人信息进行合并，并进行举例，通过将个人敏感信息加粗的方式便于区分和理解，同时个人常用设备信息补充“设备传感器信息”字段。

去标识化与匿名化详细对比二者之间的异同，同时引入“标识符”便于更深入理解二者，通过列举直接标识符和准标识符让App 提供者能判断去标识化和匿名化的效果，同时列举相关的技术手段和常见标识符去标识化的参考，让匿名化和去标识化有了实操性。

App个人信息保护的监管与法律责任从护立法概况、主要监管部门、法律责任等方面进行阐述，方便企业了解当前App个人信息保护的法律法规、监管部门、法律责任，加强企业的个人信息保护的意识。

由于目前App个人信息保护相关的法律法规、标准较多，为帮助企业快速查询，于是将App个人信息保护相关法律、司法解释、部门规章和标准文件索引进行罗列，为企业降低资料索引的成本。