ICS 33.030
CCS M 21

团　体　标　准

T/TAF 209.8—2024

移动互联网应用程序（APP）合规开发管理测评规范　第8部分：数据使用管理

Evaluation specification for compliance development of mobile Internet application—Part 8: Data use management

2024-02-23 发布　　2024-02-23 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规则起草。

本文件是T/TAF 209《移动互联网应用程序（APP）合规开发管理测评规范》的第8部分。T/TAF 209已经发布了以下部分：

——第1部分：总则；
——第2部分：需求设计；
——第3部分：功能测试；
——第4部分：代码审计；
——第5部分：对外接口管理；
——第6部分：应用编程接口（API）管理；
——第7部分：更新升级管理；
——第8部分：数据使用管理；
——第9部分：算法模型；
——第10部分：人员能力；
——第11部分：能力成熟度评估。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、北京三快科技有限公司、北京快手科技有限公司、维沃移动通信有限公司、阿里巴巴(中国)有限公司、华为终端有限公司、小米通讯技术有限公司。

本文件主要起草人：吴斌、屈蕾蕾、王宇晓、冷杉、宋文娣、王芳、徐辉、落红卫、王昕、赵盈洁、黄天宁、潘洁、李实、顾泽宇。

引　言

当前，我国移动互联网高速发展，APP在架数量和用户规模持续扩大，业务形式、产品形态更新频繁，已成为个人信息保护的关键领域。与此同时，大数据、人工智能、物联网、虚拟现实等技术的蓬勃发展和广泛应用使企业收集使用数据的范围、规模和精度不断提升，个人信息滥用和泄露的风险日益加剧。为了进一步规范企业用户数据使用活动，促进数据依法合理有效利用，维护用户合法权益，推动经济和社会的高质量发展，亟需针对APP合规开发过程中的数据使用情况建立规范，督促指导企业建立健全相关制度、强化技术能力。

T/TAF 209旨在对APP开发流程、功能模块、工程管理等提出合规开发管理要求，拟由11部分构成。

——第1部分：总则。目的在于给出规范移动互联网应用程序（APP）合规开发的总体原则和要求。

——第2部分：需求设计。目的在于提出规范APP需求设计环节的相关合规开发要求。

——第3部分：功能测试。目的在于规范移动互联网应用程序（APP）在合规开发阶段满足功能测试的标准要求。

——第4部分：代码审计。目的在于规范APP代码审计过程，提升代码安全管理能力。

——第5部分：对外接口管理。目的在于规范APP对外接口的合规开发和使用管理，提升合规能力。

——第6部分：应用编程接口（API）管理。目的在于规范APP在开发过程中对于API的使用，提升合规能力。

——第7部分：更新升级管理。目的在于规范APP合规开发在更新升级阶段的要求，提升APP更新升级管理能力。

——第8部分：数据使用管理。目的在于规范APP在合规开发过程中数据使用的合规管理，提升数据使用合规管理能力。

——第9部分：算法模型。目的在于规范APP合规开发在算法模型方面的要求，提升APP算法模型开发的合规管理能力。

——第10部分：人员能力。目的在于规范APP在合规开发过程中的人员能力管理。

——第11部分：能力成熟度评估。目的在于规范APP在合规开发管理过程中的能力成熟度评估。

移动互联网应用程序（APP）合规开发管理测评规范　第8部分：数据使用管理

1　范围

本文件规定了移动互联网应用程序（APP）合规开发过程中数据使用活动的测评规范，主要涉及数据的传输与存储、访问与展示、处理与分析等环节。

本标准适用于APP开发者的设计、生产活动，也适用于主管部门、第三方评估机构等组织对APP开发者的数据使用合规情况进行监督、管理和评估。

注：本文件所指的数据主要包括APP开发过程管理中涉及到的相关数据，其中包括用户个人信息和敏感个人信息。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273　信息安全技术　个人信息安全规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

个人信息　personal information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：《中华人民共和国个人信息保护法》]

3.2

敏感个人信息　sensitive personal information

敏感个人信息是一旦泄露或者非法使用，可能导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：《中华人民共和国个人信息保护法》]

4　缩略语

下列缩略语适用于本文件。

APP：移动互联网应用程序（Mobile Internet Application）

5　概述

数据使用管理属于移动互联网应用程序（APP）合规开发技术框架的重要组成部分，确保开发过程中涉及到的数据合规使用，主要涉及数据的传输与存储、访问与展示、处理与分析等重点环节。

6 总体原则

APP合规开发过程中，数据合规使用应遵循以下原则：

a） 最小必要——APP合规开发过程中涉及到的个人信息使用管理应遵循最小必要原则。

b） 分类分级——应根据监管要求和业务需求制定明确合理的数据分类分级标准。

c） 安全可用——应采用必要的管理和技术措施保障数据传输和存储、访问与展示、处理与分析等过程中的机密性、完整性和可用性。

d） 可追溯性——应采用日志留存、自动化审计等手段对数据传输和存储、访问与展示、处理与分析等过程中的关键操作进行监测记录。

7 数据传输与存储

数据传输与存储应遵循以下要求，具体包括：

a） 应结合业务需求和业务流程，充分考虑涉及数据传输与存储的各平台系统的设计、部署、运营、和维护，制定系统化的管理体系和具体明确的操作规定，且数据传输与存储活动应严格按照规定开展。

b） 应加强数据传输与存储过程中的安全防护，防范网络攻击和信息泄露，具体技术手段包括但不限于访问控制、数据加密、权限管理等。

c） 应加强对通信密钥、存储密钥、密码算法、传输通道、数据接口等关键安全配置的安全管理，并定期评估相应安全配置的有效性。

d） 应制定全面、明确、合理的数据分类分级管理规定，根据数据的安全风险等级采用差异化的安全防护措施。涉及敏感个人信息时，应采用安全可靠的密码技术来保障传输与存储安全。

e） 应加强对数据传输接口的安全管理，采用白名单机制，通过MAC地址、IP地址、端口号等方式严控非授权的数据传输请求，并对数据传输过程进行日志记录、设置自动化审计规则及告警规则。严格控制数据接口的新增范围与数量，事前做好风险评估，事中配备技术管控措施，事后留存详细日志记录。

f） 应加强对存储介质的安全管理，制定系统化的管理要求并配备相应技术管控措施。对于从移动存储介质中存取数据的情况，应严格审核并留存详细操作日志。

g） 数据传输与存储应在满足业务要求的最小范围、最短时限内进行。若超出期限，应及时删除个人信息或进行匿名化处理。

h） 应全面梳理涉及传输个人信息的数据接口和存储个人信息的系统、介质，建立管理台账，做好数据隔离，配备技术管控措施，对相关数据操作形成日志记录，设置自动化审计规则及告警规则。

i） 有关用户个人信息传输与存储的其他情况，还应遵守GB/T 35273—2020第6章的要求。

8 数据访问与展示

8.1 访问控制

数据访问与与展示应遵循以下访问控制要求，具体包括：

a） 应建立最小授权的访问控制策略，且应在满足业务需求的最小范围内进行数据展示。
b） 应结合数据分类分级管理规定建立数据访问权限管理制度，明确账号权限分配、开通、使用、变更、注销等审批流程和操作要求，重点关注账号权限变更、沉默账号、离职人员账号回收等情况。
c） 应对数据使用人员、数据管理人员、安全审计人员等角色进行分离设置并加强权限管理，为其分配完成职责所需的最少权限。
d） 应确保系统账号的安全性，实现方式包括但不限于设置口令复杂度策略、设置账号锁定策略、对口令遗忘的申请和重置流程实施严格管理等。
e） 应配备实现访问控制所需的技术管控措施，包括但不限于自动化角色分配、角色管理、权限申请、权限审批、权限收回、权限使用等，并对相应操作进行日志记录、设置自动化审计规则及告警规则。
f） 应制定、维护数据访问权限分配表，并定期进行风险评估。
g） 应严格控制系统中的特权账号数量，如超级管理员。
h） 涉及敏感个人信息等高敏感数据时，在访问管理系统过程中应进行二次身份验证，且其访问权限的有效范围和有效期限应受到更加严格的控制，宜在到期后强制回收。应对涉及高敏感数据的所有操作进行详细日志记录，并设置自动化审计规则及告警规则。

8.2 个人信息的脱敏处理

涉及用户个人信息时，数据展示应遵循以下脱敏、去标识化处理要求，具体包括：
a） 应结合数据分类分级管理规定建立数据脱敏处理管理制度，明确适用场景、工作方法、工作流程等。
b） 涉及敏感个人信息时，如果数据脱敏后能够满足业务功能，应使用脱敏后的数据（包括页面、页面源代码、日志信息等）进行用户交互层面的展示，数据底层脱敏工作宜在后端服务器完成。
c） 应定期对所使用脱敏方法的安全性和可逆性进行重新评估，若不符合业务需求和安全要求，应及时进行替换。
d） 开发测试环境中，不应使用未脱敏的个人信息。

9 数据处理与分析

数据处理与分析应遵循以下要求，具体包括：
a） 应确保数据处理与分析遵循法律法规、社会公德伦理，不损害国家、社会、公众及他人的合法权益，不以垄断经营和不正当竞争为目的，不发生误导、欺诈、胁迫或者干扰等限制个人或者组织正当选择与决策的行为。
b） 数据处理与分析的目的、方式、范围应始终与进行数据采集时的约定保持一致，不应超出与其具有直接或合理关联的范围。若因业务需求确需改变数据处理与分析的目的、方式、范围，基于个人同意处理个人信息的应在重新进行风险评估后再次征得用户明示同意。
c） 应结合业务需求和业务流程，充分考虑涉及数据处理与分析的各平台系统的设计、部署、运营、和维护，制定系统化的管理体系和具体明确的操作规定，且数据处理与分析活动应严格按照规定开展。
d） 应加强数据处理与分析过程中的安全防护，防范网络攻击和信息泄露。
e） 应当实施必要的技术防护措施降低涉及敏感个人信息的恶意截屏、图片盗用、恶意下载、恶意打印等风险。
f） 应综合运用管理和技术措施确保数据处理与分析的方法得当、结果客观准确。

g） 基于个人信息处理与分析面向个人提供自动化决策服务时，应当以适当方式说明分析目的、依赖数据基本情况和分析算法基本逻辑，提升决策的透明度。

h） 除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。

i） 应对数据处理与分析过程中的关键操作进行日志记录，以备对分析结果的准确性、可信性进行溯源。同时，应设置自动化审计规则及告警规则，及时定位违规使用数据的行为。

j） 有关用户个人信息分析使用的其他情况，还应遵守GB/T 35273—2020第7章的要求。

10 评估方法

数据使用管理的测试方法主要采用资料审查、技术验证和人员访谈对各项要求进行符合性评估。具体见表1。

表 1 数据使用管理与测评方式对应关系表

要求条款	测评方式		
	资料审查	技术验证	人员访谈
7 a)	√	–	√
7 b)	√	–	√
7 c)	√	√	√
7 b)	√	√	√
7 e)	√	√	√
7 f)	√	√	√
7 g)	√	√	√
7 h)	√	√	√
7 i)	√	√	√
7 j)	√	√	√
7 k)	√	–	–
8.1 a)	√	–	√
8.1 b)	√	–	√
8.1 c)	√	√	√
8.1 d)	√	√	–
8.1 e)	–	√	√
8.1 f)	√	–	√
8.1 g)	√	–	√
8.1 h)	–	√	–
8.2 a)	√	–	√
8.2 b)	√	√	√
8.2 c)	√	√	–
8.2 d)	√	√	√
9 a)	√	–	–
9 b)	√	–	–
9 c)	√	–	–

表 1　数据使用管理与测评方式对应关系表（续）

要求条款	测评方式		
	资料审查	技术验证	人员访谈
9 d)	√	–	–
9 e)	√	√	√
9 f)	√	–	√
9 g)	√	–	√
9 h)	√	√	√
9 i)	√	–	√
9 j)	√	–	–
注：“√”表示可采用的测评方式；“-”表示不适用。			

参 考 文 献

[1] 《中华人民共和国个人信息保护法》

电信终端产业协会团体标准

移动互联网应用程序（APP）合规开发管理测评规范 第8部分：数据使用管理

T/TAF 209.8—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街28号
电话：010-82052809
电子版发行网址：www.taf.org.cn