ICS 33.050
CCS M 30

团　体　标　准

T/TAF 077.9-2022
代替 T/TAF 077.9-2021

APP 收集使用个人信息最小必要评估规范 第 9 部分：短信信息

Application software user personal information collection and usage minimization and necessity evaluation specification— Part 9: SMS information

2022-02-23 发布　　2022-02-23 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》的规定起草。

本文件是T/TAF 077《APP收集使用个人信息最小必要评估规范》的第9部分。T/TAF 077已经发布了以下部分：

——第1部分：总则；
——第2部分：位置信息；
——第3部分：图片信息；
——第4部分：通讯录；
——第5部分：设备信息；
——第6部分：软件列表；
——第7部分：人脸信息；
——第8部分：录像信息；
——第10部分：录音信息；
——第11部分：通话记录；
——第12部分：好友列表；
——第13部分：传感器信息；
——第14部分：应用日志信息；
——第15部分：房产信息；
——第16部分：交易记录；
——第17部分：身份信息。

本文件代替T/TAF 077.9-2021 《APP收集使用个人信息最小必要评估规范 短信信息》，与T/TAF 077.9-2021相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“基本原则”一章（见第4章）；
b) 在“典型应用场景”中增加了七类应用场景（见第6章，2021年版的4.2）；
c) 增加了“告知同意要求”一节（见7.1）；
d) 将“本地访问必要性评估”、“收集使用最小必要评估”两章合并为“基本要求”一章，并将2021年版的有关内容更改后纳入（见第7.2、7.3、7.4、7.5、7.6，2021版的第5章和第6章）；
e) 增加了“评估流程和方法”一章（见第8章）。

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、维沃移动通信有限公司、OPPO广东移动通信有限公司、北京奇虎科技有限公司、北京字节跳动科技有限公司、荣耀终端有限公司、华为技术有限公司、北京京东世纪贸易有限公司。

本文件主要起草人：贾科、武林娜、杜云、赵盈洁、李腾、姚一楠、宋恺、宁华、王艳红、卜英华、刘陶、王宇晓、赵晓娜、衣强、冯娜、李然、吴怡、陈鑫爱。

引　　言

本文件根据《中华人民共和国网络安全法》等相关法律要求，依据GB/T 35273 《信息安全技术 个人信息安全规范》的最小必要原则，提出移动应用软件在处理涉及个人短信信息的收集、存储、使用、删除等活动中的最小必要信息规范和评估准则，旨在对移动互联网行业收集使用用户短信信息进行规范，落实最小、必要的原则，进一步促进移动互联网行业的健康稳定发展。

APP收集使用个人信息最小必要评估规范　第9部分：短信信息

1　范围

本文件是APP收集使用个人信息最小必要评估规范系列标准中的短信信息部分，旨在贯彻个人信息收集使用的最小必要的原则，针对移动APP访问、收集、存储、使用、删除用户手机短信信息（含彩信、5G消息等多媒体方式）等各环节提出相应的最小必要性符合度评估项，并结合典型场景，对APP最小必要处理短信信息的进行规定。

本文件适用于规范移动互联网应用软件开发者对用户短信信息的处理，也适用于主管监管部门、第三方评估机构等组织对移动互联网应用程序收集短信信息行为进行监督、管理和评估。

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

T/TAF 077.1-2020　APP收集使用个人信息最小必要评估规范 总则

3　术语、定义和缩略语

3.1　术语和定义

GB/T 35273和T/TAF 077.1-2020界定的术语和定义适用于本文件。

3.2　缩略语

下列缩略语适用于本文件。

APP：应用软件（Application）

SMS：短信（Short Message）

MMS：彩信（Multimedia Message）

4　基本原则

对个人信息处理活动中短信信息收集使用的原则应满足T/TAF 077.1-2020《APP收集使用个人信息最小必要评估规范 总则》中的最小必要原则。

5　短信信息分类

本文件将短信信息包含的信息类型划分为如下类型，如表1：

——本机用户标识：用于识别或区分短信、彩信信息所在移动终端设备用户的的标识信息，可包括发送者的手机号等；依据短信信息的发送方，本机用户标识可以是短信信息的发送者标识，也可以是短信信息的接收者标识。

——对端标识：用于识别或区分短信、彩信信息所在移动终端设备用户的的短信通信对端标识信息，包括接收者的手机号等。

——短信内容：为短信发送者编辑并发送给接收者的各种格式的内容。单一的短信内容是否包含个人信息、包含的个人信息的类目数量以及包含的具体个人信息类型取决于每个短信内容的本身。

——时间：移动终端设备用户接收或发送该条短信的时间。

表1　短信信息的信息类型

短信信息			
本机用户标识	对端标识	短信内容	时间

6　典型应用场景

短信信息是移动终端用户的个人通信内容，基于多条或单条短信信息可能泄露用户隐私，甚至危害个人的人身安全和财产安全，具有较高敏感性，应在合理的场景下使用。在本文件中列举了以下场景为合理必要收集使用短信信息的场景：

a) 短信云备份：以数据备份为目的，APP将用户终端上的短信信息传输至远端服务器上存储的场景。

b) 验证码便捷获取：以协助用户完成登录或支付操作为目的，APP识别短信中的验证码并提示用户的场景。

c) 便捷短信查询与服务订阅：以便利用户操作为目的，APP帮助用户发送特定短信指令至特定号码，查询相关信息或订阅服务的场景，如流量余额查询。

d) 短信优化编辑与发送：以协助用户编辑并发送短信为目的，APP提供短信编辑功能并发送短信至用户指定号码的场景。

e) 短信功能体验增强：以增强用户短信功能体验为目的，APP为用户提供如短信发送商户识别和图形化展示等增强短信功能的场景。

f) 手机间数据互传：以在用户不同手机间传输数据为目的，将用户一部手机中的短信信息传输至用户另一部手机的场景，如换机。

g) 骚扰拦截：以帮助用户拦截、屏蔽用户不期望接收的短信信息为目的，APP识别并处置相关短信信息的场景。

h) 服务智能化：以改善服务智能化程度或用户体验为目的，APP访问用户短信信息的场景。

i) 已关联设备的配套应用：通过此类应用用户可将移动设备与已关联设备（例如智能手表、汽车、智能家居设备等）连接起来，还能够收发短信。

j) 跨设备同步或转移短信：在多个设备上（例如手机和笔记本电脑之间）同步短信信息。

k) 设备自动化：用户可让设备根据其设置的一个或多个条件（触发条件），在操作系统的多个区域自动执行重复性操作。

l) 企业存档及设备管理：企业存档、客户关系管理CRM和/或设备管理，如运营商通过短信上报设备信息与驻网状态。

m) 车载免提使用和投影显示：与驾驶/出行的核心功能（例如导航）直接相关的APPs，尤其是在用户与设备的物理互动受到限制的情况下。

n) 呼救短信：可在发生人身安全或紧急状况时发送报警短信。

o) 用户数据本地备份与还原：用户的事务性备份和还原以及企业的归档（限时/非连续）。

7 基本要求

7.1 告知同意要求

除终端基本通信功能外的APP，若需收集处理个人信息，应遵循以下要求：

a) 基于用户个人同意收集处理个人信息的：若仅在本地收集处理短信信息，APP应向用户声明收集处理短信信息仅在用户设备上进行，并告知收集处理短信信息的目的，经用户确认后方可开始收集；若存在非本地处理的情形，APP应明确告知用户需传输至远端的短信信息类型及收集处理的目的、方式、范围，并经用户选择同意后方可收集；

b) 若短信信息的处理目的、处理方式、保存期限等发生变更，应重新告知并取得个人信息主体同意；

c) 免于同意的情形应按GB/T 35273 5.6征得授权同意的例外要求执行；

d) APP处理的短信信息若涉及著作权、肖像权等法律问题的，应遵循国家相关规定的要求，本文件不做专门规定。

7.2 权限要求

7.2.1 权限申请最小化

短信权限作为敏感权限，除终端基本通信功能外的 APP 在申请短信权限时应满足如下要求：

a) 首次启动时，若用户拒绝授权短信权限，应用不应退出或关闭。

b) APP 应基于自身业务功能和场景，以权限申请最小化为为原则，仅在业务功能触发时，向用户申请必要的短信权限；典型场景下的 APP 可申请项如表 2 所示。

c) 当用户拒绝短信权限时，APP 不得以退出、关闭、弹窗循环、频繁申请等方式强迫或诱导用户授权。

表 2 典型场景下的可申请权限

序号	典型场景	可申请权限				
		发送短信	读取短信	接收短信	写/删除短信	接收彩信
1	短信云备份	—	✓	—	✓	—
2	验证码便捷获取	—	✓	✓	—	✓
3	便捷短信查询与服务订阅	✓	—	✓	—	✓
4	短信优化编辑与发送	✓	—	—	—	—
5	短信功能体验增强	—	✓	✓	—	✓
6	手机间数据互传	—	✓	—	✓	—
7	骚扰拦截	—	✓	✓	✓	✓
8	服务智能化	—	✓	✓	✓	✓
9	已连接的设备配套应用	✓	✓	✓	✓	✓

表 2　典型场景下的可申请权限（续）

序号	典型场景	可申请权限				
		发送短信	读取短信	接收短信	写/删除短信	接收彩信
10	跨设备同步或转移短信	✓	✓	✓	✓	✓
11	设备自动化	✓	✓	✓	✓	✓
12	企业存档及设备管理	✓	✓	✓	✓	✓
13	车载免提使用和投影显示	✓	✓	✓	✓	✓
14	呼救短信	✓	—	—	—	—
15	用户数据本地备份与还原	—	✓	✓	✓	—

7.2.2　调用行为最小化

APP在满足业务正常开展的前提下，应以最低频次调用相关短信权限，且仅访问与业务目的相关的短信信息。

本文件将短信权限的APP调用频次和时机划分为3类：

a)　用户主动触发：通过明确的用户知悉影响的动作，如点击APP交互界面上特定的按钮，触发相关行为。

注：触发后，跳转到短信界面由用户进行后续操作的，不需要APP申请相应的短信权限。

b)　固定周期访问：以明示并经用户确认同意的固定周期调用相关权限。

c)　短/彩信到达触发：在App已申请接收短、彩信权限时，当接收到新的短信或彩信时触发。

对于典型场景，建议的调用频次和时机如表 3 所示。

表3　典型场景下的短信权限调用

序号	典型场景	调用频次或时机		
		发送短、彩信	读取短信/彩信	写/删除短、彩信
1	云盘数据备份	—	用户主动触发 固定周期访问	用户主动触发 固定周期访问
2	验证码便捷获取	—	用户主动触发 短、彩信到达触发	—
3	便捷短信查询与服务订阅	用户主动触发	—	—
4	短信优化编辑与发送	用户主动触发	—	—
5	短信功能体验增强	—	用户主动触发 短、彩信到达触发	—
6	手机间数据互传	—	用户主动触发	用户主动触发
7	骚扰拦截	—	用户主动触发 短、彩信到达触发 固定周期访问	用户主动触发 短、彩信到达触发
8	服务智能化	—	用户主动触发 固定周期访问 短、彩信到达触发	—

表3　典型场景下的短信权限调用（续）

序号	典型场景	调用频次或时机		
		发送短、彩信	读取短信/彩信	写/删除短、彩信
9	已连接的设备配套应用	用户主动触发	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发
10	跨设备同步或转移短信	用户主动触发	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发
11	设备自动化	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发
12	企业存档及设备管理	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发
13	车载免提使用和投影显示	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发
14	呼救短信	用户主动触发	—	—
15	用户数据本地备份与还原	—	用户主动触发 固定周期访问 短、彩信到达触发	用户主动触发 固定周期访问 短、彩信到达触发

7.3　本地收集阶段

典型场景下，APP在用户终端本地可收集短信信息类型可参考表4。

表4　典型场景下的可收集信息类型

序号	典型场景	信息类型			
		本机用户标识	对端标识	短信内容	时间
1	云端数据备份	✓	✓	✓	✓
2	验证码便捷获取	✓	✓	✓	✓
3	便捷短信查询与服务订阅	✓	✓	✓	✓
4	短信优化编辑与发送	X	X	X	X
5	短信功能体验增强	✓	✓	✓	✓
6	手机间数据互传	✓	✓	✓	✓
7	骚扰拦截	✓	✓	✓	✓
8	服务智能化	✓	✓	✓	✓
9	已连接的设备配套应用	✓	✓	✓	✓

表4　典型场景下的可收集信息类型（续）

序号	典型场景	信息类型			
		本机用户标识	对端标识	短信内容	时间
10	跨设备同步或转移短信	✓	✓	✓	✓
11	设备自动化	✓	✓	✓	✓
12	企业存档及设备管理	✓	✓	✓	✓
13	车载免提使用和投影显示	✓	✓	✓	✓
14	呼救短信	X	X	X	X
15	用户数据本地备份与还原	✓	✓	✓	✓

7.4　远程传输阶段

APP需传输用户短信信息至APP远端服务器时，应严格限定远程传输的短信信息类型。典型场景下，可由APP服务器端收集的短信信息类型可参考表5。

表5　典型场景下的可收集信息类型

序号	典型场景	信息类型			
		本机用户标识	对端标识	短信内容	时间
1	云端数据备份	✓	✓	✓	✓
2	验证码便捷获取	X	X	X	X
3	便捷短信查询与服务订阅	X	X	X	X
4	短信优化编辑与发送	X	X	X	X
5	短信功能体验增强	✓	X	X	✓
6	手机间数据互传	X	X	X	X
7	骚扰拦截（垃圾短信上报）	✓	✓	✓	✓
8	服务智能化	✓	✓	✓	✓
9	已连接设备的配套应用	X	✓	✓	✓
10	跨设备同步或转移短信	X	✓	X	X
11	设备自动化	X	X	X	X
12	企业存档及设备管理	✓	✓	✓	✓
13	车载免提使用和投影显示	X	X	X	X
14	呼救短信	✓	✓	✓	✓
15	用户数据本地备份与还原	X	X	X	X

7.5　存储阶段

APP服务器端存储短信信息应满足以下要求：

a)　短信信息的存储期限应为实现个人信息主体授权使用的目的所必需的最短时间。

b)　除用户主动上报的垃圾短信外，其余场景下，应加密存储用户短信信息。

c)　在APP服务端上存储的移动终端用户的短信信息应不超过按7.4节要求评估后允许远程传输的

短信信息的信息类型和收集范围。

7.6 使用阶段

APP服务器端使用短信信息应严格按照收集目的使用短信信息，若需扩大使用目的，则应在使用前再次告知并经个人信息主体同意后才能使用。

8 评估流程和方法

8.1 评估方法

评估方实施APP收集使用短信信息最小必要评估的流程和方法应遵循T/TAF 077.1-2020《APP收集使用个人信息最小必要评估规范 总则》中的评估流程和方法。

8.2 评估步骤

评估方在实施短信信息收集使用最小必要评估时，宜遵循以下步骤和方法：

a） 确定被评估对象及评估范围；

注：被评估对象可为单个 APP 或者 APP 中某项或某类功能。

b） 评估方根据被评估方提交的说明材料的业务场景初步判断被评估对象是否有必要收集使用短信信息：

1） 若被评估对象的业务场景为本文件第6章所述的典型应用场景；

2） 若被评估对象的业务场景并非典型应用场景，则评估方应基于T/TAF 077.1-2020《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第1部分：总则》中的最小必要原则，重点评估自述材料中对短信信息的收集使用的目的、方式和范围是否最小必要。

c） 确定评估基准。基于本文件第7章基本要求确定针对被评估对象的评估基准；

d） APP终端侧评估：

1） 告知同意符合性评估：基于7.1节要求，检查被评估对象对短信信息的收集使用是否有在隐私政策中详细说明；

2） 权限申请最小化评估：检查被评估对象申请的短信权限是否遵循7.2.1节要求；

3） 调用行为最小化评估：检查被评估对象申请的短信权限是否遵循7.2.2节要求；

4） 本地收集最小化评估：检查被评估对象通过系统API收集处理的短信信息类型是否符合7.3节要求；

5） 远程传输最小化评估：检查被评估对象传输出终端侧的信息类型是否遵循7.4节要求。

e） APP服务器端侧评估：

1） 存储安全措施评估：被评估方应提供举证材料证明短信信息的在APP服务端的存储安全措施符合7.5节的要求；必要时，评估方可采用现场核查的方式；

2） 使用目的一致性评估：被评估方应提供举证材料证明短信信息的在APP服务端的使用符合7.6节要求。

8.3 评估项目

8.3.1 告知同意符合性测评

测试编号：8.3.1.1
测试项目：短信信息的告知同意
测试要求：见本文件 7.1
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 在本地收集处理短信信息前，是否声明收集处理短信信息仅在用户设备上进行，并告知收集处理短信信息的目的； b) 检查 APP 在非本地收集处理短信信息前，是否明确告知用户需传输至远端的短信信息类型及收集处理的目的、方式、范围； c) 检查若短信信息的处理目的、处理方式、保存期限等发生变更，APP 是否重新告知并取得个人信息主体同意； d) 检查 APP 是否在个人同意后才进行信息收集。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.2 权限申请最小化评估

测试编号：8.3.2.1
测试项目：短信信息的权限申请
测试要求：见本文件 7.2.1a）
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 在首次启动时，当用户拒绝授权短信权限，应用是否没有退出或关闭。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

测试编号：8.3.2.2
测试项目：短信信息的权限申请
测试要求：见本文件 7.2.1b）
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 是否基于自身业务功能和场景，以权限申请最小化为原则，仅在业务功能触发时，向用户申请必要的短信权限； b) 检查典型场景下的 APP 的申请权限项目是否符合表 2。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

测试编号：8.3.2.3
测试项目：短信信息的权限申请
测试要求：见本文件 7.2.1c）
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查当用户拒绝短信权限时，APP 是否没有以退出、关闭、弹窗循环、频繁申请等方式强迫或诱导用户授权。

预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.3 调用行为最小化评估

测试编号：8.3.3.1
测试项目：短信信息的权限申请
测试要求：见本文件 7.2.2
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 在满足业务正常开展的前提下，是否以最低频次调用相关短信权限，且仅访问与业务目的相关的短信信息； b) 检查典型场景下的 APP 的短信权限调用频次或时机是否符合表 3。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.4 本地收集最小化评估

测试编号：8.3.4.1
测试项目：短信信息的本地收集
测试要求：见本文件 7.3
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 在用户终端本地收集短信信息类型是否符合表 4。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.5 远程传输最小化评估

测试编号：8.3.5.1
测试项目：短信信息的权限申请
测试要求：见本文件 7.4
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 在传输用户短信信息至 APP 远端服务器时，是否严格限定远程传输的短信信息类型； b) 检查在典型场景下，由 APP 服务器端收集的短信信息类型是否符合表 5。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.6 存储最小化评估

测试编号：8.3.6.1
测试项目：短信信息的权限申请
测试要求：见本文件 7.5a）
预置条件：被评估 APP 处于正常状态
测试步骤： a) 运行 APP，检查 APP 服务器端的短信信息存储期限是否为是实现个人信息主体授权使用的目的所必需的最短时间。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

测试编号：8.3.6.2
测试项目：短信信息的权限申请
测试要求：见本文件 7.5b）
预置条件：被评估 APP 处于正常状态
测试步骤： a） 运行 APP，检查 APP 服务器端的短信信息，除用户主动上报的垃圾短信时，其余场景下，是否加密存储用户短信信息。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

测试编号：8.3.6.3
测试项目：短信信息的权限申请
测试要求：见本文件 7.5c）
预置条件：被评估 APP 处于正常状态
测试步骤： a） 运行 APP，检查 APP 服务器端上存储的移动终端用户的短信信息是否不超过按 7.4 节要求评估后允许远程传输的短信信息的信息类型和收集范围。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

8.3.7 使用最小化评估

测试编号：8.3.7.1
测试项目：短信信息的权限申请
测试要求：见本文件 7.6
预置条件：被评估 APP 处于正常状态
测试步骤： a） 运行 APP，检查 APP 服务器端使用短信信息是否严格按照收集目的使用短信信息； b） 若需扩大使用目的，APP 是否在使用前再次告知并经个人信息主体同意后才使用短信信息。
预期结果：若以上测试步骤结果为肯定，则测试项判定为符合，否则判定为不符合。

电信终端产业协会团体标准

APP 收集使用个人信息最小必要评估规范　第 9 部分：短信信息

T/TAF 077.9-2022

*

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