ICS 33.050
CCS M 30

团　体　标　准

T/TAF 077.1—2022
代替 T/TAF 077.1—2020

APP 收集使用个人信息最小必要评估规范 第 1 部分：总则

Application software user personal information collection and usage minimization and necessity evaluation specification—
Part 1: General principle

2022-11-25 发布　　2022-11-25 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1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：终端通讯录；
——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9部分：短信信息；
——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；
——第18部分：剪切板信息。

本文件代替T/TAF 077.1—2020 《APP收集使用个人信息最小必要评估规范 总则》，与T/TAF 077.1—2020相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 题目中增加了“第1部分”；
b) 将“术语、定义和缩略语”更改为“术语和定义”与“缩略语”两章，并增加和更改了部分定义（见第3、4章）；
c) 更改了“告知同意要求、收集要求、使用要求、传输要求”的要求（见6.2、6.3、6.5、6.7）；
d) 增加了“权限要求、存储要求”的要求（见6.1、6.4）；
e) 增加了“加工要求、提供要求、公开要求”（见6.6、6.8、6.9）；
f) 修改了“删除要求”的要求（见6.10）。

请注意本文件中的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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、泰尔认证中心有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、北京奇虎科技有限公司、华为技术有限公司、北京三快在线科技有限公司、小米科技有限责任公司、阿里巴巴(中国)有限公司、北京字节跳动科技有限公司。

本文件主要起草人：陈鑫爱、李可心、周飞、李京典、杜云、王艳红、武林娜、宋恺、宁华、汤立波、常浩伦、李腾、毛欣怡、贾科、姚一楠、衣强、凌大兵、常琳、方强、周圣炎、贾雪飞、杨骁涵、王宇晓、安潇羽。

本文件及其所代替文件的历史版本发布情况为：

——2020年首次发布为T/TAF 077.1—2020；

——本次为第一次修订。

引　　言

随着移动应用种类和数量呈爆发式增长，APP侵害用户权益事件层出不穷，个人信息保护态势愈加严峻，如何保护用户个人信息，尤其是人脸、通讯录、短信、位置、图片等个人敏感信息受到国家和社会公众高度关注。

APP收集使用个人信息最小必要评估旨在对移动互联网行业收集使用用户人脸、通讯录、短信、位置、图片等个人敏感信息进行规范，落实最小、必要的原则。

APP 收集使用个人信息最小必要评估规范　第 1 部分：总则

1　范围

本文件明确APP收集使用个人信息最小必要评估规范系列标准中术语定义，规定了收集使用的最小必要原则及要求，是APP收集使用个人信息最小必要评估规范系列标准的引领部分，或为其他移动终端数据相关标准提供参考。

本文件适用于移动应用软件收集使用个人信息的设计、开发和评估，个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

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 25069-2010 信息安全技术 术语

3　术语和定义

下列术语和定义适用于本文件。

3.1

移动智能终端　smart mobile terminal

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

3.2

移动应用软件 mobile application software

可安装在移动智能终端内，能够利用移动智能终端操作系统提供的公开开发接口，实现某项或某几项特定任务的计算机软件，包含移动智能终端预置应用软件，小程序、快应用以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.3

个人信息　personal information

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。

3.4

敏感个人信息　sensitive personal information

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、财产安全受到严重危害的个人信息,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。

3.5

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

3.6

个人信息处理 personal information processing

对个人信息执行的操作或操作集，主要包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.7

收集 collect

获取个人信息的活动。

3.8

告知同意 inform consent

应用通过弹窗或产品界面等方式提示通知个人信息主体知晓其个人信息处理活动及其有关规则,并获个人信息主体做出自愿、明确授权的行为。

3.9

业务功能 business function

满足个人信息主体具体使用需求的服务能力。

注：如地图导航、网络约车、即时通讯、网络社区、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

3.10

敏感权限 sensitive permissions

涉及用户的个人信息或相关资源，或者可能对用户存储的数据或其他应用的操作产生影响的权限。

3.11

定向推送 directional push

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体推荐或展示信息内容、提供商品或服务的搜索结果以及推送商业广告等活动。

注：业务实践中，定向推送也被称为个性化展示或个性化推荐。本文件中同时使用定向推送、个性化展示和个性化推荐，具有相同含义。

4 缩略语

下列缩略语适用于本文件。

APP：移动应用软件（Application）

SDK：软件工具开发包（Software Development Kit）

5 基本原则

APP个人信息的处理应遵循最小必要原则，即处理个人信息应当具有明确、合理的目的,应与处理目的直接相关，采取对个人权益影响最小的方式。APP提供的业务功能不在《APP收集使用个人信息最小必要评估规范》系列标准内时，也应满足最小必要要求。

6 个人信息处理最小必要评估要求

6.1 权限要求

权限申请和使用应遵循最小必要原则，要求如下：

a) 权限的申请和使用的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b) APP应申请与业务功能相关的权限，不应过度申请权限。例如APP的业务功能中，不包含位置相关场景，则不应申请位置权限；

c) APP申请敏感权限时，应同步告知权限使用的目的和用途；

d) 用户拒绝或撤回系统权限授权，不应拒绝提供与该权限使用无关的服务，APP宜优先采用系统自身功能，代替调用相关敏感权限。例如APP需要拨打电话功能时，可优先选择调用系统的电话界面，而不是申请电话权限；

e) 不得以改善服务质量、提升使用体验和实施风险控制等为由，强迫个人信息主体授予权限；

f) APP申请权限时，应在使用对应业务功能时申请，不应提前申请、一揽子申请多个权限，不得默认、捆绑或使用其他手段变相欺骗、误导、强迫个人信息主体授予权限；

g) 对于第三方SDK等外部代码的引用，APP应要求SDK其相关权限的申请同样满足最小必要原则，不得过度申请权限。

6.2 告知同意要求

告知同意应遵循最小必要原则，要求如下：

a) APP所提供产品或服务涉及多项业务功能的，处理个人信息时，应按业务功能单项或分项获得个人信息主体同意,不应采用捆绑方式强迫个人信息主体一次性同意多种业务功能收集的个人信息。个人信息主体拒绝同意时，仅影响与所拒绝个人信息相关的业务功能的正常使用；

b) 告知同意的时机及频率，应在收集使用之前或收集使用之时的适当时机告知，增进个人信息主体对告知与所处理收集的个人信息之间关联性的理解。

6.3 收集要求

收集个人信息应遵循最小必要原则，要求如下：

a) 收集个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b) APP被授予权限后，权限使用应遵循最小必要原则，即应合理使用申请的权限，不应滥用权限，超频次、超范围、超精度收集个人信息。

6.4 存储要求

APP个人信息的存储包含本地存储和服务器远端存储，均应遵循最小必要原则，要求如下：

a) 存储个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b) 存储个人信息的类型及数量不应超出业务功能的实际需要；

c) 存储个人信息的时间应遵循最小必要原则，即存储个人信息的时间，应当为实现处理目的所必要的最短时间，在超出上述期限后，应对个人信息进行删除或匿名化处理；

注：对于保存在端侧的个人信息，只需对业务运行过程中产生的包含个人信息的临时文件，或过程文件指定删除时间，其它个人信息由个人信息主体自己管理和控制；

d) 收集个人信息后，宜立即进行去标识化处理，并将可用于恢复识别个人的信息与去标识化后的信息分开存储；

e) APP 如需在终端本地存储个人信息，则应将个人信息存储在受保护的文件区域，防止其他 APP 非授权访问；

f) 个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息（如样本、图像等）。如确需存储个人生物识别信息的，应在本地进行加密存储。

6.5 使用要求

使用个人信息应遵循最小必要原则，要求如下：

a) 使用个人信息的目的、方式、范围不应超出业务功能的实际需要，法律法规另有规定的除外；

b) 使用个人信息时，除目的所必需外，应消除明确身份指向性，避免精确定位到特定个人；

c) 使用个人信息进行定向推送不应超出业务功能的实际需要；

d) 若APP定向推送功能使用了第三方的个人信息来源，应以个人信息处理规则等形式向个人信息主体明示业务功能使用第三方的个人信息进行定向推送，并向个人信息主体明示第三方的个人信息来源；

e) 使用个人信息进行定向推送应显著区分个性化展示和非个性化展示，显著区分的方式包括但不限于：标明“推荐”、“猜你喜欢”等字样，或通过不同的栏目、版块、页面分别展示等；

f) 使用个人信息进行定向推送应当同时提供关闭个性化展示的选项。此外，APP宜建立个性化展示所依赖的个人信息(如标签、画像维度等)的自主控制机制，保障个人信息主体调控定向推送展示相关性程度的能力。

6.6 加工要求

加工个人信息应遵循最小必要原则，要求如下：

a) 加工个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b) 间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的，需要告知，并重新征得个人信息主体的同意。

6.7 传输要求

传输个人信息应遵循最小必要原则，要求如下：

a) 传输个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b) 个人生物识别信息原则上不应传输，如因业务需要确需传出终端的，应通过不可逆算法对生物

特征识别信息进行处理，例如脱敏或加密传输提取的特征信息。

6.8 提供要求

提供个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。

6.9 公开要求

公开个人信息应遵循最小必要原则，要求如下：

a) 公开个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
b) 公开个人信息前，应单独征得个人信息主体同意。

6.10 删除要求

删除个人信息应遵循最小必要原则，有下列情形之一的，应对个人信息进行删除或匿名化处理；未及时删除的，应在个人信息主体请求删除后及时删除或匿名化处理：

a) 处理目的已实现、无法实现或者为实现处理目的不再必要；
b) 个人信息处理者停止提供产品或者服务，或者保存期限已届满；
c) 个人信息主体撤回同意；
d) 个人信息处理者违反法律、行政法规或违法约定处理个人信息；
e) 法律、行政法规规定的其他情形。

注：法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

7 评估流程

7.1 总体要求

APP收集使用个人信息最小必要评估流程如图1所示。包括确定评估目标、选择评估指标、制定评估计划、实施评估及得出评估结论这四个活动。

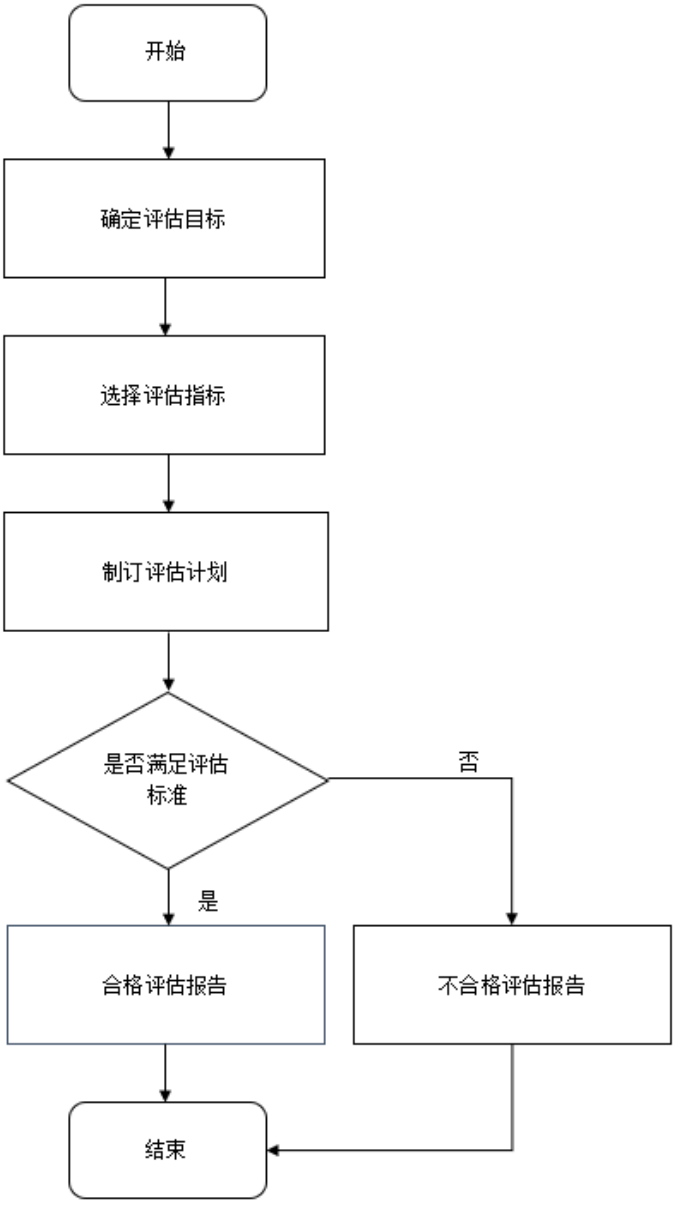

图1　APP收集使用个人信息最小必要评估流程图

7.2　评估方与被评估方

应考虑以下方面，确定评估方和被评估方：

a)　被评估方可为 APP 或者 APP 中某项某类功能；

b)　评估方可为 APP 提供者、开发者和运营者，也可为第三方实验室。

7.3　选择评估指标

应考虑以下方面，确定评估指标：

a)　评估方根据被评估方提供的技术说明文档、被评估 APP 样品等材料，确定初步的方案审核，发现涉及的个人信息类型，选择对应的评估规范标准，并由此定义后续的评估的计划和评估项例。

7.4　制定评估计划

应考虑以下方面，制定评估准则：

a) 评估方应根据评估目标，本着公平、公正、公开原则开展评估工作；
b) 评估准则内容应至少包括评估对象和范围、评估依据、评估环境、评估工具；
c) 评估准则中应明确评估通过/不通过准则。

7.5 实施评估

应考虑以下方面，实施评估工作：

a) 依据对应的评估规范标准开展实施评估活动；
b) 通过各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系；
c) 各部分最小必要评估结果均应以评估报告的形式进行输出，其内容至少应包括开展最小必要信息类型、评估所选择的评估指标及针对评估指标的评估结果。

7.6 评估结论

应考虑以下方面，给出评估结论：

a) 针对开展评估的个人信息类别进行评估，APP 收集使用最小必要通过评估并达到目标要求，否则未通过评估。
b) 在最小必要评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还要具体地描述评估过程中的步骤，如包含未通过项则评估报告中应包含未通过原因的具体描述。

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 1 部分：总则

T/TAF 077.1—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