

ICS 33.050

M 30

团 体 标 准

T/TAF XXX.X-XXXX

APP 收集使用个人信息最小必要评估规范 应用日志信息

Application software user personal information collection and usage
minimization and necessity evaluation specification: log information

XXXX - XX - XX 发布

XXXX - XX - XX 实施

电信终端产业协会 发布

目 次

目录

目 次	I
前 言	II
引 言	III
APP 收集使用个人信息最小必要评估规范 应用日志信息	1
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 日志中涉及的个人信息及典型场景	2
4.1 日志中涉及个人信息	2
4.2 日志中涉及个人信息的典型场景	2
5 个人信息处理活动中应用日志信息收集使用原则	2
5.1 收集	2
5.2 存储	2
5.3 使用	3
5.4 传输	错误!未定义书签。
5.5 删除	3

前 言

本文件按照GB/T1.1-2020的规定起草。

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、每日互动股份有限公司。

本文件主要起草人：方毅、董霖、高可、李颖莹、苗玉雷、常曦微、宁华、武林娜、王艳红、金岩、郟世杰。



引 言

随着移动互联网的迅速发展, 各行各业的APP应运而生, APP已经和我们的生活息息相关。然而在使用APP的过程中, 由于缺少必要的规范作为依据, 导致一部分APP为了自身业务或其他服务可能会采集大量的应用日志信息, 而这些应用日志信息中可能包含了用户的隐私信息数据, 进而造成了用户数据泄露的风险。

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/T35273-2020《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相关应用日志信息的收集、存储、使用、传输、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应用日志信息进行规范, 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 应用日志信息

1 范围

本文件规定了在移动应用软件在处理涉及用户个人信息相关应用日志信息的收集、存储、使用、传输、删除等活动中的最小必要信息规范和评估方法，并通过对在个人信息处理活动中的典型应用场景来说明如何落实最小必要原则。

本文件适用于移动互联网应用软件提供者规范用户个人信息（应用日志信息）的处理活动，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应用日志信息的行为进行监督、管理和评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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》

GB/T 35273-2020 《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

系列标准《APP收集使用个人信息最小必要评估规范 总则》中术语和定义适用于本文件。

下列术语和定义适用于本文件。

3.1.1 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开放操作系统，具有安装、加载和运行应用软件能力的终端。

3.1.2 移动应用软件 mobile application

针对移动智能终端所开发的应用程序，包括移动智能终端预置应用软件以及互联网信息服务提供者提供的可以通过智能终端下载、安装、升级、卸载的应用软件。

3.1.3 应用日志信息 application log information

用于具体描述移动应用软件在运行过程中产生的记录文件。

3.1.4 个人信息处理者 Personal Information Processor

能够自主决定处理目的、处理方式等个人信息处理事项的组织、个人，包括但不限于APP或SDK开发者。

3.2 缩略语

下列缩略语适用于本文件。

APP 移动应用软件 Mobile Application

4 包含个人信息的日志及典型场景

4.1 包含个人信息的日志

部分日志中可能包含个人信息，如系统功能产生的敏感应用日志信息；应用内商品浏览或浏览器访问所产生的临时文件；APP使用过程中产生的日志记录；APP 安装运行后生成的各种与个人信息相关的日志等。

4.2 典型场景

可能包含个人信息的日志所产生的典型场景，如：聊天场景、电商场景、系统场景、支付场景等。

5 个人信息处理活动中应用日志信息收集使用最小必要规范

个人信息处理者仅应处理与其提供服务相关的最小、必要的应用日志信息。

5.1 收集

5.1.1 收集前须满足的必要条件

收集应用日志信息必须具有合理必要的理由，并且应当通过隐私条款或其他方式获得用户的授权。

5.1.2 日志生成阶段

个人信息处理者经法律授权或具备合理事由确需在日志中体现个人信息时，除应当对个人敏感信息采用加密等安全措施外，还应符合《APP 收集使用个人信息最小必要评估规范》系列规范的其他规范要求。

5.1.3 日志收集阶段

5.1.3.1 日志检索、读取、上传

APP 只可检索、读取、上传本 APP 生成的日志文件。

5.1.3.2 除外情形

个人信息处理者经法律授权或具备合理事由的情形除外。

5.2 存储

- a) 个人信息处理者存储日志应保证日志的安全，例如可采用可靠的数据加密、合理的访问控制权等方式。
- b) 个人信息处理者存储日志应保证存储周期最小化，若法律法规或行业监管对存储期限另有规定的，从其规定。
- c) 个人信息处理者存储日志超过存储期限后，应当对其所持有的应用日志信息进行删除或匿名化处理。

5.3 使用

- a) 个人信息处理者使用应用日志信息时，不应超出与收集个人信息时所告知用户的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。
- b) 个人信息处理者对被授权访问用户应用日志信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的应用日志信息，且仅具备完成职责所需的最少的数据操作权限。

5.4 删除

- a) 个人信息处理者应定期检查其所存储的用户应用日志信息，并根据移动应用的必要功能删除不必要的相关数据。
- b) 超出应用日志信息的存储期限后，个人信息处理者应对应用日志信息进行删除或匿名化处理。
- c) 在对于应用日志信息的删除，个人信息处理者应提供途径并保证实现用户删除权。
- d) 个人信息处理者需要证明其如何满足在法律规定的时限内及时答复用户行使删除权请求。如果必须延长答复用户的时间，个人信息处理者需提供合理理由。
- e) 个人信息处理者经法律授权或具备合理事由需要保留日志文件的情形除外。



版权所有 侵权必究

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