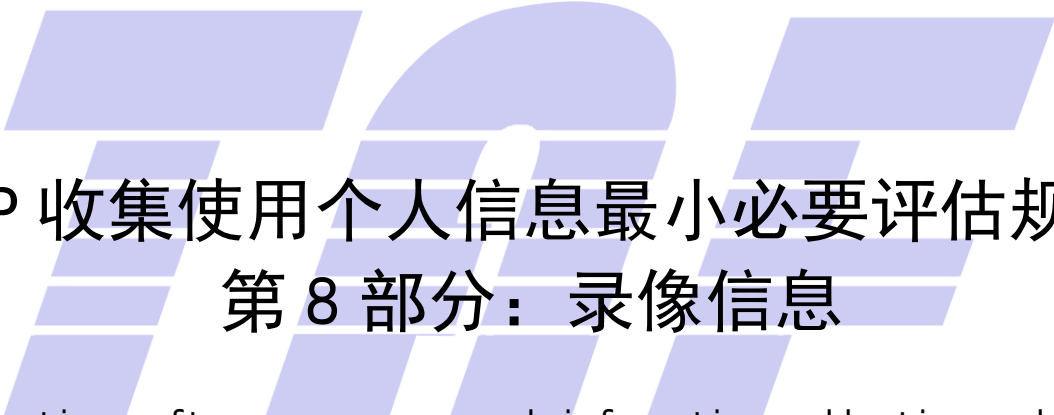


ICS 33.050  
CCS M 30

# 团 体 标 准

T/TAF 077.8—2022  
代替 T/TAF 077.8—2020

---



## APP 收集使用个人信息最小必要评估规范 第 8 部分：录像信息

Application software user personal information collection and usage  
minimization and necessity evaluation specification—  
Part 8: Video information

2022-09-15 发布

2022-09-15 实施

---

电信终端产业协会 发布



# 目 次

前言 .....	II
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	1
5 基本原则 .....	1
5.1 信息最小化原则 .....	2
5.2 权限最小化原则 .....	2
5.3 本地处理原则 .....	2
5.4 其他原则 .....	2
6 录像信息分类 .....	2
7 典型应用场景 .....	2
7.1 概述 .....	2
7.2 典型应用场景分类 .....	2
8 最小必要处理活动 .....	3
8.1 告知同意 .....	3
8.2 收集阶段 .....	4
8.3 存储阶段 .....	5
8.4 使用阶段 .....	6
8.5 加工阶段 .....	6
8.6 传输阶段 .....	7
8.7 提供阶段 .....	7
8.8 公开阶段 .....	7
8.9 删除阶段 .....	8
9 评估方法 .....	8
9.1 概述 .....	8
9.2 告知同意评估 .....	8
9.3 收集阶段评估 .....	9
9.4 存储阶段评估 .....	9
9.5 使用阶段评估 .....	11
9.6 加工阶段评估 .....	12
9.7 传输阶段评估 .....	13
9.8 提供阶段评估 .....	14
9.9 公开阶段评估 .....	14
9.10 删除阶段评估 .....	15

## 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8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。

本文件代替T/TAF 077.8—2020《APP收集使用个人信息最小必要评估规范 录像信息》，与T/TAF 077.8—2020相比，除结构调整和编辑性改动外，主要的技术变化如下：

- a) 增加了“缩略语”一章（见第4章）；
- b) 增加了“基本原则”一章（见第5章）；
- c) 增加了“录像信息分类”一章（见第6章）；
- d) 增加了“概述”（见7.1），并将“服务所必需类场景”细化扩展了四类新的典型应用场景（见7.2，2020年版的4.4）；
- e) 更改了标题，将“授权同意”改为“告知同意”，并增加或修改了一些条款（见8.1，2020年版的5.1）；
- f) 更改了“收集阶段”要求，并细化为“收集信息最小化”、“权限申请最小化”两部分（见8.2，2020年版的5.2）；
- g) 将“存储、删除”拆分并细化成“存储阶段”要求（见8.3，2020年版的5.5）和“删除阶段”要求（见8.9，2020年版的5.5）；
- h) 更改了“使用阶段”要求（见8.4，2020年版的5.3）；
- i) 增加了“加工阶段”要求（见8.5）；
- j) 增加了“传输阶段”要求（见8.6）；

k) 更改了标题，将“对外提供”改为“提供阶段”，并增加或修改了一些条款（见8.7，2020年版的5.4）；

l) 增加了“公开阶段”要求（见8.8）；

m) 增加了“评估方法”一章（见第9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、荣耀终端有限公司、泰尔认证中心有限公司、北京小桔科技有限公司、华为终端有限公司、OPPO广东移动通信有限公司、北京字节跳动科技有限公司、北京奇虎科技有限公司、北京三星通信技术研究有限公司、维沃移动通信有限公司、高通无线通信技术（中国）有限公司、博鼎实华（北京）技术有限公司、北京京东世纪贸易有限公司、郑州信大捷安信息技术股份有限公司、北京快手科技有限公司。

本文件主要起草人：赵晓娜、卜英华、武林娜、宁华、蒲兴、宫展博、衣强、李腾、王宇晓、姚一楠、王艳红、胡越男、杨光、吴越、贾科、宋恺、刘陶、张娜、田明仁、王江胜、董霁、李然、刘献伦、落红卫、王昕、徐曼。

本文件及其所代替文件的历次版本发布情况为：

——2020年首次发布为T/TAF 077.8—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，如何保护个人信息，尤其是人脸、通讯录、短信、位置、图片等敏感个人信息受到政府机构和社会公众高度关注。

本文件旨在对移动互联网行业收集使用个人信息主体的录像信息进行规范，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 8 部分：录像信息

## 1 范围

本文件确立了APP处理录像信息的基本原则，结合典型应用场景规定了对录像信息的收集、存储、使用、加工、传输、提供、公开、删除等处理活动中落实最小必要原则的评估要求，并描述了相应的最小必要评估方法。

本文件适用于APP提供者规范用户录像信息的处理活动，也适用于第三方评估机构等组织对APP收集使用录像信息行为进行监督、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—2020 信息安全技术 个人信息安全规范

T/TAF 077.1 APP收集使用个人信息最小必要评估规范 第1部分：总则

## 3 术语和定义

T/TAF 077.1界定的以及下列术语和定义适用于本文件。

### 3.1

**录像信息** video information

通过视频采集设备录制的直接含有自然人个人信息或者能够反映自然人活动情况的视频信息及其衍生数据。

注：衍生数据包括从视频中提取的图像、声音等。

## 4 缩略语

下列缩略语适用于本文件。

APP：移动应用软件（Application）

BDS：北斗卫星定位系统（BeiDou Navigation Satellite System）

GNSS：全球导航卫星定位系统（Global Navigation Satellite System）

GPS：全球定位系统（Global Positioning System）

WLAN：无线局域网（Wireless Local Area Network）

## 5 基本原则

## 5.1 信息最小化原则

APP处理录像信息的类型、数量、频率、范围等，不应超出业务场景的实际需要，法律法规要求的除外。

## 5.2 权限最小化原则

APP如需执行申请、使用录像相关权限，应为实现业务功能所必需，不应过度申请权限，且获得授权后不应过度使用。

## 5.3 本地处理原则

APP优先在本地处理录像信息，能在本地独立完成处理的不应再上传到云端处理。

## 5.4 其他原则

APP处理录像信息以及申请使用录像相关权限的，需满足T/TAF 077.1中的最小必要原则。

## 6 录像信息分类

录像信息可以通过移动智能终端上的摄像头录制功能、屏幕录制功能以及对录像信息的再加工等方式生成，也可以通过移动智能终端上APP绑定的监控摄像头等设备录制生成。

根据录像信息中包含的内容，可将录像信息分为以下三种类型：

- a) 录像基本信息：指录像的基本特征信息，包括录像的内容（视频流）、格式、大小、分辨率、帧率、码率等信息；
- b) 录像附加信息：指录制录像过程中可能同步产生和保存的其他信息，包括录像时间、录像设备型号、录像文件名称等信息；
- c) 录像位置信息：指录制视频图像时可能通过移动智能终端提供的定位能力或个人信息主体主动为录像文件编辑的能真实精准定位到个人信息主体的位置信息。

注1：如无特殊说明，本文件所述的个人信息主体均为APP用户。

注2：移动智能终端提供的定位能力包括通过全球导航卫星定位系统GNSS（如GPS、BDS等）和/或网络位置信息源（如基站、WLAN等）获取到移动智能终端当前的精确位置信息。

## 7 典型应用场景

### 7.1 概述

本文件对涉及处理录像信息的典型应用场景进行梳理和归类，对于未包含在本文件所述典型应用场景范围内的APP，应按T/TAF 077.1规定的最小必要原则进行评估。

对于仅通过移动智能终端上的摄像头提供预览功能的应用场景，如APP根据个人信息主体选择的预览效果等进行相应的本地处理后向用户展示相应的预录制效果，不涉及存储录像信息操作，因此不涉及使用、加工、传输、提供、公开等处理活动，本文件将不针对该应用场景做最小必要规定与评估。

对于通过从互联网下载、从其他移动智能终端或APP接收等方式获取并保存的录像信息，一般不包括录像附加信息和位置信息。因此，APP在本文件7.2所述典型场景下收集和使用此类录像信息时，不涉及对录像附加信息和位置信息的相关收集和使用要求。

### 7.2 典型应用场景分类



APP收集使用录像信息的典型场景包括但不限于：

a) 主动上传类场景，指APP通过主动上传录像为个人信息主体提供向自身或者他人展示或分享等相关服务的场景；

注：例如，在社交类APP内上传已录制好的短视频，并对该APP内一个或多个好友或者APP所有使用者可见；在直播类APP内将实时录像上传进行视频直播。

b) 视频通讯类场景，指APP通过实时录像为个人信息主体提供与一个或多个其他方进行双向通讯服务的场景；

注：例如，使用社交类APP与一个或多个好友进行视频通话；使用视频会议类APP与一个或多个其他方开展视频会议，其中会议主持人还可执行会议录制操作。

c) 录像编辑类场景，指APP为个人信息主体提供对本地录像进行内容编辑服务的场景；

注：例如，使用此类APP对选定的录像进行裁剪、合成、调色、添加文字声音等编辑操作。

d) 身份认证类场景，指APP通过实时录像为个人信息主体提供完成金融开户类所需的实人身份核验、人脸识别类所需的活体检测等相关服务的场景；

e) 云盘备份类场景，指APP通过将本地录像上传到云盘为个人信息主体提供备份服务的场景；

注：为个人信息主体提供备份服务的方式包括但不限于：个人信息主体主动选择一个或多个录像，主动打开APP设置的自动备份开关等。

f) 安防监控类场景，指APP通过事先绑定监控摄像头为个人信息主体提供实时查看、回看、保存、删除该监控摄像头拍摄的周围环境录像等服务的场景；

注：该场景下，录像可通过云端同步下载到移动智能终端的APP客户端进行存储，或者，通过局域网直接从监控摄像头传输到移动智能终端的APP客户端进行存储。

g) 用户体验优化类场景，指APP通过对本地录像进行智慧化处理为个人信息主体提供按位置、内容类型等分类或聚类展示服务的场景。

注：该场景主要是针对录像信息为用户打造更好的展示体验。例如，个人信息主体在APP内可选择基于录像位置信息对录像按位置分类后展示，或者，基于录像时间等附加信息对录像按日期排序后展示，或者，基于录像内容对录像按人物、风景、人脸等聚类后展示。

本文件评估的APP可能具备上述a)–g)中的一个或多个服务场景。

## 8 最小必要处理活动

### 8.1 告知同意

对个人信息处理者处理录像信息的告知同意要求包括：

a) APP收集录像信息前，应向使用APP的个人信息主体告知对于录像信息的处理目的、处理方式、保存期限等。宜逐一列出该APP（含委托的第三方或嵌入的第三方SDK、插件等）在不同场景中处理录像信息的目的、方式、范围和频率，以及录像信息存储的地域、期限、超期处理的方式，采取的数据安全保护措施等；

注：相机、相册、视频电话等移动智能终端基本功能软件处理录像信息的例外。

b) 基于个人信息主体同意处理个人信息的，应在8.1 a) 后取得个人信息主体的同意；若录像信息的处理目的、处理方式、保存期限等发生变更，应重新取得个人信息主体同意；

c) 收集录像需要调用移动智能终端系统权限的，宜在录像功能启动前或启动时申请相关权限；

注：本文件中所述系统权限，以安卓操作系统为例时，通常是安卓定义的危险权限，如位置、相机、存储等权限。

d) 个人信息主体拒绝录像相关权限申请后，APP不应拒绝为个人信息主体提供其他服务，录像信息作为服务的最小必要信息的除外；

- e) 个人信息主体拒绝录像相关权限申请后, APP在间隔48小时内重新申请该权限不应超过1次, 不应频繁请求权限干扰个人信息主体正常使用APP其他功能, 个人信息主体主动开启相关功能或主动授予权限的除外;
- f) APP不应擅自更改个人信息主体原有的录像相关权限设置。如需更改, 应重新告知并获得个人信息主体的同意;
- g) 不得欺骗误导个人信息主体同意收集录像信息, 不得在未取得个人信息主体同意的条件下通过隐蔽方式收集录像信息;
- h) 免于同意的情形应按GB/T 35273-2020中5.6规定的要求执行;
- i) APP所处理录像的内容涉及其他信息(如人脸信息)的, 应遵循T/TAF 077中其他相应部分的要求;
- j) APP处理录像信息涉及著作权、肖像权等法律问题的, 本文件不做专门规定。

## 8.2 收集阶段

### 8.2.1 收集信息最小化

对个人信息处理者收集录像信息的要求包括:

- a) 收集目的应与应用场景有关, 不应仅以改善服务质量、提升使用体验、研发新产品等为由强制个人信息主体同意收集跟场景无关的录像信息;
- b) 收集方式可包括通过摄像头摄像或屏幕录制实时生成录像信息、通过读取存储区域(如媒体库)内本地保存的录像信息等方式, 收集录像信息前应获得个人信息主体相应授权。APP通过本地摄像头、绑定的独立监控摄像头或者屏幕录制生成录像信息时, 应为用户呈现显性的摄录界面、屏幕录制界面;
- c) 收集范围应由个人信息主体确定。当个人信息主体仅选取一个或多个已生成的录像时, 宜避免读取其所在存储区域中的其他录像信息; 收集录像信息时, 应结合如下表1中典型应用场景或个人信息主体的选择最小化收集录像附加信息或位置信息;
- d) 收集频率应限定在满足业务目的的最低收集频率。涉及7.2 a)-d)所述场景的APP, 应仅在使用APP的个人信息主体主动提供时才能收集录像信息; 涉及7.2 e)所述场景的APP, 应在个人信息主体主动提供时收集录像信息, 或者在个人信息主体确认使用自动备份功能后自动收集录像信息。

考虑到不同APP可能对于录像附加信息或位置信息具有不同的收集需求或收集能力, APP应按如下表1所述最小必要原则在不同场景下收集录像信息:

表1 APP不同场景下收集录像信息的最小必要原则

场景	录像信息收集方式	录像信息收集范围(是否可收集)			录像信息收集频率
		基本信息	附加信息	位置信息	
主动上传类	摄像或屏幕录制	是	可选1	可选2	用户主动触发的单次收集
	读取本地录像	是		可选3	
视频通讯类	摄像实时生成	是	可选1	可选2	用户主动触发的单次收集
录像编辑类	摄像或屏幕录制	是	可选1	可选2	用户主动触发的单次收集
	读取本地录像	是		可选3	
身份认证类	摄像实时生成	是	否	否	用户主动触发的单次收集
云盘备份类	读取本地录像	是	是	是	用户主动触发的单次收集, 或者, 用户确认使用自动备份功能后的自动(如周期性)收集

表1 APP不同场景下收集录像信息的最小必要原则（续）

场景	录像信息收集方式	录像信息收集范围（是否可收集）			录像信息收集频率
		基本信息	附加信息	位置信息	
安防监控类	摄像实时生成	是	可选1	否	摄像头正常工作期间的持续收集
用户体验优化类	读取本地录像	是	是	是	用户主动触发的单次收集，或者，用户确认使用相关功能后的自动收集

注1：表格中的“可选1”是指，若APP额外读取录像附加信息，则宜为用户提供选择的能力（例如：向用户提供可设置的开关）。

注2：表格中的“可选2”是指，若APP额外实时收集当前位置信息，则应为用户提供选择的能力（例如：向用户申请位置相关权限）。“可选3”是指，可选2所述情况，或者，若APP额外读取录像位置信息且所选录像中有录像位置信息，则宜为用户提供去除该信息的能力（例如：向用户提供可设置的开关）。

注3：对于7.2 d)所述的身份认证类场景，APP往往无收集录像附加信息、录像位置信息的需求；对于7.2 f)所述的安防监控类场景，APP往往无实时收集当前位置信息的需求或能力。

### 8.2.2 权限申请最小化

APP如8.2.1 b)所述进行收集录像信息的行为时，涉及申请相关权限的，如移动智能终端系统提供的相机权限、位置权限、存储权限等，只有在获得个人信息主体的相应授权后，APP才能收集录像信息。

APP应按如下表2所述最小必要原则在收集录像时申请权限：

表2 APP不同录像信息收集方式下申请权限的最小必要原则

录像信息收集方式	对应权限	用途	是否必需
摄像实时生成	相机	通过摄像头实时拍摄生成录像	是
	麦克风	通过麦克风实时采集声音	是
	位置	通过定位能力实时获取当前地理位置	否
屏幕录制实时生成	屏幕录制（注：如系统无对应权限，应通过打开开关等方式取得个人信息主体同意。用户主动打开该功能的视作已取得同意）	通过屏幕录制功能实时生成录像	是
	麦克风	通过麦克风实时采集声音	是
读取本地录像	存储	读取本地保存的录像	是
	位置	读取时通过定位能力获取当前地理位置	视场景确定

注1：对于移动智能终端提供存储权限的，除了如7.2 g)等因APP的基本功能必需处理本地所有录像信息的场景外，应避免通过申请存储权限方式访问录像信息，宜使用系统自身提供的相关功能，以安卓系统为例时，如通过存储访问框架（SAF，System Access Framework）访问。

注2：上述“视场景确定”表示，因APP的基本功能必需获取位置信息的，如7.2 g)所述基于当前位置匹配展示本地保存的所有在当前位置附近摄制的录像信息等用户体验优化类场景，APP可申请位置权限，其余场景下则为非必需。

### 8.3 存储阶段

对个人信息处理者存储录像信息的要求包括：

- a) 应按APP实现业务功能所需选择在本地还是云端存储录像信息。例如，7.2 a)、b)、d)-f)所述场景可存储在云端，7.2 c)、g)所述场景宜存储在本地；

- b) 应按APP实现业务功能所需最短时限或者按约定的存储时限对录像信息进行存储，法律法规另有规定的除外；
- c) 如个人信息主体在使用服务过程中产生的纠纷尚未解决完毕的，个人信息处理者可以适当延长录像信息的保存期限，在纠纷处理完毕且满足约定存储期限后删除或匿名化处理录像信息；
- d) 应对存储在云端的录像信息提供访问控制机制，避免录像信息被非法访问；
- e) 宜对云端存储的录像信息进行加密，确保录像信息的保密性；
- f) 如有云端自动备份录像信息功能，如7.2 a)所述的主动上传类、7.2 e)所述的云盘备份类等场景，宜提供设置自动备份功能的开关，且默认不打开。

#### 8.4 使用阶段

对个人信息处理者使用录像信息的要求包括：

- a) 使用录像信息时，不应超出与收集时所声称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录像信息的，应按8.1 b)重新取得同意；
- b) 个人信息处理者应对内部人员访问录像信息建立严格的管理机制，合理分配录像信息访问权限，严格控制访问人员和可访问内容。宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权；
- c) APP使用录像信息包括对录像信息的展示操作，个人信息处理者宜对展示的个人信息进行模糊化处理或支持用户自主编辑等措施，降低个人信息泄露风险，对人脸特征进行遮挡导致无法实现使用目的的除外。APP应按如下表3所述的最小必要原则在不同场景下展示录像信息：

表3 APP不同场景下展示录像信息的最小必要原则

场景	展示信息的最小必要
主动上传类	展示时宜提示其中是否含录像附加信息和录像位置信息，并允许选择删除
视频通讯类	不应展示录像附加信息和录像位置信息，基于个人信息主体同意的除外
录像编辑类	展示时宜提示其中是否含录像附加信息和录像位置信息，并允许选择删除
身份认证类	不应展示录像附加信息和录像位置信息，基于个人信息主体同意的除外
云盘备份类	展示时宜提示其中是否含录像附加信息和录像位置信息，并允许选择删除
安防监控类	展示时宜提示其中是否含录像附加信息，并允许选择删除；展示时宜对个人信息（如人脸全部或局部位置）进行模糊化处理；不应展示录像位置信息，基于个人信息主体同意的除外
用户体验优化类	分类或聚类展示录像信息时，可一并展示相应功能维度对应的录像位置信息或录像附加信息

- d) APP基于收集的录像信息进行个性化展示的，应遵循GB/T 35273-2020中7.5规定的要求；
- e) 涉及利用所收集的录像信息进行自动化决策的，应事前进行个人信息保护影响评估，包括处理目的、处理方式等是否合法、正当、必要，对个人权益的影响及安全风险，所采取的保护措施是否合法、有效并与风险程度相适应等；
- f) 涉及将所收集的录像信息与其他个人信息进行汇聚融合的，应满足8.4 a)所述要求。若汇聚融合后个人信息用于其他目的的，应如8.4 e)所述事前进行个人信息保护影响评估，并采取有效的个人信息保护措施。

#### 8.5 加工阶段

对个人信息处理者传输录像信息的要求包括：

- a) 不应非法加工其处理的录像信息；

- b) 对于7.2所述场景，涉及对录像信息进行加工的，例如7.2 c)所述录像编辑类场景，不应超出与收集时所声称的处理目的具有直接或合理关联的范围；
- c) 不应采取隐蔽手段直接从录像信息中提取，或者，通过数据挖掘、分析归纳等方式获得表征个人信息主体身份的个人信息；
- d) 对于录像内容中包含的每个个人信息主体的信息，不宜进行针对个人的分析。法律法规另有规定或获得个人信息主体同意的除外。

注：上述针对个人的分析，不包括7.2 g)所述典型场景下APP提供的按录像内容中人脸信息进行分类或聚类展示功能，可以理解为通过录像信息分析获得与实现业务功能无关的用户画像的活动，例如，APP根据个人信息主体上传到云盘进行备份的录像信息分析其中其他个人信息主体的行为习惯、兴趣爱好、相互之间的关系等。

## 8.6 传输阶段

对个人信息处理者传输录像信息的要求包括：

- a) 不应非法传输其处理的录像信息；
- b) 涉及传输录像信息的，应仅传输实现业务功能所必需的录像信息；
- c) 对于如7.2 a)所述的主动上传类、e)所述的云盘备份类等场景，可设置自动传输控制开关，且默认不打开；
- d) 需要传输录像信息的，应采用满足数据传输安全策略相应的安全控制措施，如采用安全传输通道或加密后传输等；
- e) 应具备对传输的录像信息进行完整性校验的能力。

## 8.7 提供阶段

对个人信息处理者提供录像信息的要求包括：

- a) 除依据法律法规规定、为了维护相关方重大合法权益且对录像信息进行去标识化处理、取得个人信息主体单独同意或者履行用户作为一方当事人的合同所必需外，不应提供录像信息；
- b) 涉及向其他个人信息处理者提供录像信息的，应仅提供实现业务功能所必需的录像信息；
- c) 涉及向其他个人信息处理者提供录像信息的，若录像信息中包含人脸等敏感个人信息，宜按照前面8.4 c)所述技术措施对录像信息进行处理。

## 8.8 公开阶段

对个人信息处理者公开录像信息的要求包括：

- a) 不应公开其处理的录像信息，基于个人信息主体单独同意、履行用户作为一方当事人的合同所必需或者法律法规规定的除外；
- b) APP提供的功能可能导致录像信息被公开的，宜对个人信息主体进行使用提醒，宜为个人信息主体提供自由设置公开范围的能力；

注1：上述使用提醒包括但不限于：提醒个人信息主体谨慎使用该功能或者该功能可能造成录像信息的公开以及公开范围大小等，还可提醒个人信息主体公开录像信息的原因、采取的模糊化等安全措施等。

注2：如针对7.2 a)所述的主动上传类场景，可为个人信息主体提供设置公开范围的选项，允许其在上传录像信息前对上传录像信息的公开范围进行设置，例如，包括仅自己可见、对选择的特定范围可见、对该APP所有好友可见、对该APP的所有用户可见等选项。如针对7.2 b)所述的视频通讯类场景，允许个人信息主体主动选择一个或多个待通讯对象，即可视为提供了自由设置公开范围的能力。

- c) 涉及公开录像信息的，若录像信息中包含个人信息主体的人脸信息等敏感个人信息，宜按照前面8.4 c)所述技术措施对录像信息进行处理。

## 8.9 删除阶段

对个人信息处理者删除录像信息的要求包括：

- a) 有下列情形之一的，应主动删除或匿名化处理录像信息；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：
  - 处理目的已实现、无法实现或者为实现处理目的不再必要；
  - 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；
  - 个人信息主体撤回同意；
  - 个人信息处理者违反法律、行政法规或违法约定处理录像信息；
  - 法律、行政法规规定的其他情形。
- b) 如个人信息主体在使用服务过程中产生的纠纷尚未解决完毕，可以适当延长录像信息的保存期限，在纠纷处理完毕且满足约定存储期限后删除或匿名化处理录像信息。

## 9 评估方法

### 9.1 概述

APP收集使用录像信息的最小必要评估应遵循T/TAF 077.1中的评估流程和方法。

本文件中，评估对象可为APP或APP中某项功能，评估内容为评估对象的告知同意符合性以及评估对象在收集、存储、使用、加工、传输、提供、公开和删除等阶段对录像信息处理的最小必要符合性。

本文件中，评估方可采用功能验证、技术检测、文档审查、人员访谈等方式实施评估过程。

### 9.2 告知同意评估

测试编号：9.2.1
测试项目：处理录像信息的告知同意
测试要求：见本文件8.1 a)、b)、g)
预置条件：被评估APP处于正常状态
测试步骤： <ol style="list-style-type: none"> <li>a) 运行APP，通过功能验证方式检查APP在收集录像信息前是否以弹框等形式向用户告知其对录像信息的处理规则，包括处理目的、处理方式、保存期限等；</li> <li>b) 通过人员访谈等方式确认是基于个人信息主体同意处理个人信息的情形，检查在功能验证中是否有针对步骤1)的确认要求；并检查APP在对录像信息的处理目的、处理方式、保存期限等发生变更时是否要求重新取得同意；</li> <li>c) 通过功能验证方式检查APP在告知用户并征求同意过程中是否不存在欺骗或误导用户同意的行为，通过技术检测、功能验证方式检查APP收集的录像信息是否均为经过用户同意后才进行的。</li> </ol>
预期结果：若以上步骤a)-c)测试结果均为肯定，则该项评估结论为符合要求，否则为不符合。

测试编号：9.2.2
测试项目：收集录像信息时涉及权限的告知同意
测试要求：见本文件8.1 c)-f)
预置条件： <ol style="list-style-type: none"> <li>a) 被评估APP处于正常状态；</li> <li>b) 被评估APP所在移动智能终端支持收集录像信息相关权限（如相机、麦克风、位置、存</li> </ol>

储等权限)，且被评估APP需要向用户申请权限。
<p>测试步骤：</p> <ul style="list-style-type: none"> <li>a) 运行APP，通过功能验证方式检查APP在收集录像信息前是否向用户申请相关权限；</li> <li>b) 通过功能验证检查用户确认拒绝授予相应权限后，APP是否能够正常提供其他服务，录像信息作为服务的最小必要信息的除外；</li> <li>c) 通过功能验证检查用户确认拒绝授予相应权限后，APP是否在48小时以内重新申请该权限不超过1次，用户主动开启相关功能或主动授予权限的除外；</li> <li>d) 通过功能验证或人员访谈检查用户确认拒绝授予相应权限后，APP是否不存在擅自修改为同意授予的行为；若因实现业务功能（如用户拒绝授权后，在48小时以内再次主动打开相关功能）需要重新获取权限的，检查APP是否按步骤a)重新向用户申请。</li> </ul>
预期结果：若以上步骤a)-d)测试结果均为肯定，则该项评估结论为符合要求，否则为不符合。

### 9.3 收集阶段评估

测试编号：9.3.1
测试项目：收集录像信息的最小化
测试要求：见本文件8.2.1
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <ul style="list-style-type: none"> <li>a) 运行APP，通过文档审查方式检查APP的个人信息处理规则声明的收集目的是否不是仅以改善服务质量、提升使用体验、研发新产品等为由要求用户同意其收集行为，并结合功能验证方式检查所声明的收集目的与其实际功能对应的应用场景是否一致；</li> <li>b) 针对7.2所述每种典型场景的APP，通过功能验证、技术检测方式检查APP收集录像信息的方式、范围和频率是否符合表1所述要求。</li> </ul>
预期结果：若以上步骤a)、b)测试结果均为肯定，则该项评估结论为符合要求，否则为不符合。

测试编号：9.3.2
测试项目：收集录像信息的权限申请最小化
测试要求：见本文件8.2.2
<p>预置条件：</p> <ul style="list-style-type: none"> <li>a) 被评估APP处于正常状态；</li> <li>b) 被评估APP所在移动智能终端支持收集录像信息相关权限（如相机、麦克风、位置、存储等权限），且被评估APP需要向用户申请权限。</li> </ul>
<p>测试步骤：</p> <p>针对7.2所述每种典型场景的APP，通过技术检测、功能验证方式检查APP在收集录像信息之前，是否已经按表2所述原则向用户申请相关权限并获得用户授权。</p>
预期结果：若以上步骤的测试结果为肯定，则该项评估结论为符合要求，否则不符合。

### 9.4 存储阶段评估

测试编号：9.4.1
测试项目：录像信息的存储位置最小化

测试要求：见本文件8.3 a)、f)
预置条件：被评估APP处于正常状态
测试步骤： <ul style="list-style-type: none"> <li>a) 针对7.2所述每种典型场景的APP，通过功能验证检查APP在完成业务功能后是否按匹配其场景类型的最小化原则将录像信息存储在云端还是本地，例如，在移动智能终端联网开关打开或关闭时，检查APP内是否存在或能否打开录像信息。对于7.2 a)、b)、d)-f)所述场景下的APP应在未联网时不存在或无法打开录像信息，在联网时则存在且能打开录像信息；对于7.2 c)、g)所述场景下的APP，未联网时的验证效果应相反，并检查未联网时其相应功能能否正常使用；</li> <li>b) 通过功能验证方式确认涉及云端自动备份录像信息功能的APP，如7.2 a)所述的主动上传类、7.2 e)所述的云盘备份类，再检查APP是否提供自动备份功能开关；对于提供该开关的，再检查开关是否为默认关闭。</li> </ul>
预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.4.2
测试项目：录像信息的存储时间最小化
测试要求：见本文件8.3 b)、c)
预置条件：被评估APP处于正常状态
测试步骤： <ul style="list-style-type: none"> <li>a) 通过文档审查、人员访谈方式检查个人信息处理者是否设立有个人信息保存期限相关管理制度，是否明确要求保存期限为实现业务功能所需最短时限或约定的固定时限，法律法规另有规定的除外；</li> <li>b) 通过文档审查、人员访谈方式检查APP服务器是否存在针对超期数据的甄别机制；</li> <li>c) 通过文档审查、人员访谈方式检查对于超期未处理（如删除或匿名化）的录像信息，是否能提供法律法规的另行规定或者涉及纠纷的处理记录等证明材料。</li> </ul>
预期结果：若以上步骤a)-c)测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.4.3
测试项目：录像信息的访问最小化
测试要求：见本文件8.3 d)
预置条件：被评估APP处于正常状态
测试步骤： <p>通过功能验证方式检查APP是否存在针对存储在云端的录像信息的访问控制机制，例如，是否要求用户进行身份验证（如输入登录账号和密码等）。</p>
预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.4.4
测试项目：录像信息的访问最小化（保密性）
测试要求：见本文件8.3 e)
预置条件：被评估APP处于正常状态
测试步骤： <ul style="list-style-type: none"> <li>a) 通过文档审查、人员访谈方式确认APP在云端存储录像信息的，再检查个人信息处理者</li> </ul>



<p>是否设立有加密机制；</p> <p>b) 对于设立有加密机制的情况，通过技术检测等方式检查云端是否以密文形式存储录像信息。</p>
<p>预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

## 9.5 使用阶段评估

测试编号：9.5.1
测试项目：录像信息的使用目的范围最小化
测试要求：见本文件8.4 a)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 通过文档审查、人员访谈方式检查个人信息处理者的个人信息相关管理制度中是否明确要求超出征求同意范围使用录像信息的，应按9.2.1测试步骤b)方式重新取得同意；</p> <p>b) 通过文档审查、人员访谈方式检查APP服务器是否存在针对超出征求同意范围使用个人信息的重新取得同意机制；</p> <p>c) 通过文档审查方式检查个人信息处理者存在超出征求同意范围使用录像信息的历史行为的，检查是否存在重新取得同意的记录。</p>
<p>预期结果：若以上步骤a)-c)测试结果均为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.5.2
测试项目：录像信息的访问最小化
测试要求：见本文件8.4 b)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 通过文档审核、人员访谈方式检查个人信息处理者设立的相关管理制度中是否包含访问控制策略及相应的审批流程，且该策略是否按最小授权原则对各职责角色仅能访问的数据类型进行规定；</p> <p>b) 通过文档审查、人员访谈方式检查个人信息处理者是否对每次访问进行有效记录，如访问时间、访问数据范围、访问操作类型、访问人员或所使用账号等。</p>
<p>预期结果：若以上步骤a)-b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.5.3
测试项目：录像信息的展示最小化
测试要求：见本文件8.4 c)、d)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 针对7.2所述每种场景下的APP，通过功能验证方式检查APP是否按8.4表2所述原则进行相应展示；</p> <p>b) APP涉及基于录像信息进行个性化展示的，通过功能验证方式检查APP是否遵循GB/T 35273-2020 7.5章节所述要求，例如：能显著区分个性化展示和非个性化展示的内容；向用户提供不针对其个人特征的选项，以及在用户选择退出或关闭个性化展示功能后提</p>

供删除或匿名化该个性化展示功能所基于的录像信息的选项。
预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.5.4
测试项目：录像信息的再利用限制
测试要求：见本文件8.4 e)、f)
预置条件：被评估APP处于正常状态
测试步骤： <ul style="list-style-type: none"> <li>a) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求利用所收集的录像信息进行自动化决策的，应事前进行个人信息保护影响评估，包括处理目的、处理方式等是否合法、正当、必要，对个人权益的影响及安全风险，所采取的保护措施是否合法、有效并与风险程度相适应等；</li> <li>b) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求将所收集的录像信息与其他个人信息进行汇聚融合后用于其他目的的，应按步骤a)方式在事前进行个人信息保护影响评估，并采取有效的个人信息保护措施。</li> </ul>
预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。

## 9.6 加工阶段评估

测试编号：9.6.1
测试项目：录像信息的加工最小化（目的范围限制）
测试要求：见本文件8.5 a)、b)
预置条件：被评估APP处于正常状态
测试步骤： <p>通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求不能非法加工其处理的录像信息，是否明确要求不能超出征求同意范围的加工录像信息。</p>
预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.6.2
测试项目：录像信息的加工最小化（再利用限制）
测试要求：见本文件8.5 c)、b)
预置条件：被评估APP处于正常状态
测试步骤： <p>通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求不能采取隐蔽手段直接从录像信息中提取，或者，通过数据挖掘、分析归纳等方式获得表征个人信息主体身份的个人信息。</p>
预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.6.3
测试项目：录像信息的加工最小化（再利用限制）
测试要求：见本文件8.5 d)
预置条件：被评估APP处于正常状态

<p>测试步骤：</p> <p>通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求不能对录像内容中包含的每个个人信息主体的信息进行针对个人的分析，法律法规另有规定或获得个人信息主体同意的除外。</p>
<p>预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

## 9.7 传输阶段评估

测试编号：9.7.1
测试项目：录像信息的传输最小化
测试要求：见本文件8.6 a)、b)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求不能非法传输其处理的录像信息；</p> <p>b) 通过功能验证、技术检测方式检查APP是否仅传输实现业务功能所必需的录像信息，例如，结合7.2所述每种场景下的APP，涉及用户主动选择录像信息的，检查APP是否仅上传或处理了用户所选择的录像信息。</p>
<p>预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.7.2
测试项目：录像信息的自动传输控制
测试要求：见本文件8.6 c)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>通过功能验证方式确认APP提供自动传输控制开关的，如7.2 a)所述的主动上传类、e)所述的云盘备份类等场景下的APP，再检查该开关是否默认关闭。</p>
<p>预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.7.3
测试项目：录像信息的传输保密性和完整性
测试要求：见本文件8.6 d)、e)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 通过文档审查、人员访谈方式检查APP是否存在加密传输等安全控制措施；</p> <p>b) 通过技术检测检查APP是否以密文方式传输录像信息，例如，通过抓包方式获取APP传输的数据包并检查其内容是明文还是密文；</p> <p>c) 通过文档审查、人员访谈方式检查APP服务器或客户端是否存在对所接收录像信息的完整性校验机制。</p>
<p>预期结果：若以上步骤a)-c)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

## 9.8 提供阶段评估

测试编号：9.8.1
测试项目：录像信息的提供最小化
测试要求：见本文件8.7 a)、b)
预置条件：被评估APP处于正常状态
测试步骤： a) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求除依据法律法规规定、为了维护相关方重大合法权益且对录像信息进行去标识化处理、取得个人信息主体单独同意或者履行用户作为一方当事人的合同所必需外，APP不应提供录像信息； b) 通过文档审查、人员访谈方式确认涉及向其他个人信息处理者提供录像信息的，再检查个人信息处理者是否仅提供实现业务功能所必需的录像信息，例如，审查个人信息处理者与其他个人信息处理者签署的合同中是否明确所提供的个人信息类型、数量等。
预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.8.2
测试项目：录像信息的提供最小化
测试要求：见本文件8.7 c)
预置条件：被评估APP处于正常状态
测试步骤： 通过文档审查、人员访谈方式确认涉及向其他个人信息处理者提供录像信息的，再检查个人信息处理者是否对包含人脸等敏感个人信息的录像信息按8.4 c)所述模糊化处理技术措施进行局部模糊处理，例如，审查个人信息处理者与其他个人信息处理者签署的合同中是否明确对录像信息中包含的敏感个人信息的处理措施等。
预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。

## 9.9 公开阶段评估

测试编号：9.9.1
测试项目：录像信息的公开限制
测试要求：见本文件8.8 a)
预置条件：被评估APP处于正常状态
测试步骤： 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求除依据法律法规规定、基于个人信息主体单独同意或者履行用户作为一方当事人的合同所必需外，APP不应公开其处理的录像信息。
预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。

测试编号：9.9.2
测试项目：公开录像信息的可知可控
测试要求：见本文件8.8 b)
预置条件：被评估APP处于正常状态

<p>测试步骤：</p> <p>a) 通过功能验证方式确认APP在用户所用功能涉及公开录像信息的，例如7.2 a)所述主动上传类场景下的APP，再检查APP是否进行使用提醒，以使用户理解该功能可能造成录像信息的公开及公开范围大小、公开原因、采取的模糊化等安全措施等；</p> <p>b) 通过功能验证方式检查APP是否提供方便用户自由设置公开范围的能力，例如，用户在APP内选择上传录像信息时可选择仅自己可见、对选择的特定范围或好友可见或其他选项；用户在使用APP实时录像功能时选择一个或多个特定对象即可视为同时做了自由设置。</p>
<p>预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.9.3
测试项目：录像信息的公开最小化
测试要求：见本文件8.8 c)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>通过功能验证方式检查APP是否对公开展示的包含人脸等敏感个人信息的录像信息进行特殊处理；或者，通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求在公开前对包含人脸等敏感个人信息的录像信息进行特殊处理。例如，按8.4 c)所述模糊化处理技术措施进行局部模糊处理。</p>
<p>预期结果：若以上步骤测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

## 9.10 删除阶段评估

测试编号：9.10.1
测试项目：录像信息的删除期限最小化
测试要求：见本文件8.9 a)、b)
预置条件：被评估APP处于正常状态
<p>测试步骤：</p> <p>a) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求存在8.9 a)所述的五种情形之一的应主动删除或匿名化处理录像信息。对于其中前四种情形，继续检查涉及个人信息处理者存在删除历史行为的，是否APP服务器存在相应处理机制（如删除或匿名化）以及相关处理记录；对于第五种情形，继续检查是否能提供法律法规规定的其他情形要求删除或匿名化处理的证明材料；</p> <p>b) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求对于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，并明确删除流程及响应时间等内容。针对7.2所述典型场景下涉及存储录像信息的APP，通过功能验证方式检查APP是否提供删除功能，以使用户方便地删除录像信息。</p>
<p>预期结果：若以上步骤a)、b)测试结果为肯定，则该项评估结论为符合要求，否则不符合。</p>

测试编号：9.10.2
测试项目：录像信息的删除期限特殊处理
测试要求：见本文件8.9 c)

预置条件：被评估APP处于正常状态
测试步骤： <ul style="list-style-type: none"><li>a) 通过文档审查、人员访谈方式检查个人信息处理者设立的相关管理制度中是否明确要求涉及所产生纠纷未解决完毕的，可以适当延长录像信息的保存期限，在纠纷处理完毕且满足约定存储期限后删除录像信息；</li><li>b) 通过文档审查、人员访谈方式检查APP服务器是否存在针对超期数据的甄别机制；</li><li>c) 通过文档审查、人员访谈方式检查对于超期未处理（如删除或匿名化）的录像信息，是否能提供纠纷处理记录等证明材料。</li></ul>
预期结果：若以上步骤a)-c)测试结果为肯定，则该项评估结论为符合要求，否则不符合。



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 8 部分：录像信息

T/TAF 077.8—2022

\*

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](http://www.taf.org.cn)