ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术　网络音视频服务数据安全指南

Information security technology — Data security guidelines for online audio and video services

（征求意见稿）

（本稿完成时间：2021 年 2 月 8 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：北京爱奇艺科技有限公司、中国电子技术标准化研究院、北京百度网讯科技有限公司、阿里巴巴（北京）软件服务有限公司、深圳市腾讯计算机系统有限公司、华为技术有限公司、北京搜狐新媒体信息技术有限公司、湖南快乐阳光互动娱乐传媒有限公司、北京快手科技有限公司、北京字节跳动科技有限公司、上海哔哩哔哩科技有限公司、广州虎牙信息科技有限公司、上海喜马拉雅科技有限公司、上海麦克风文化传媒有限公司、网易（杭州）网络有限公司、北京竞天公诚律师事务所上海分所、海信集团有限公司、北京小米移动软件有限公司、苏宁易购集团股份有限公司、OPPO广东移动通信有限公司、重庆邮电大学、中电长城网际安全技术研究院（北京）有限公司、国家计算机网络应急技术处理协调中心、中国信息通信研究院、陕西省信息化工程研究院、国家工业信息安全发展研究中心、中国网络安全审查技术与认证中心。

本文件主要起草人：朱垒、奚海生、童永祥、刘晓静、胡影、周晨炜、何延哲、洪延青、樊庆君、黄著馨、荣彦平、袁立志、陈梦园、王平、冯帆、林芷晴、刘晓敏、华贤扬、郭卫红、徐雨晴、闵京华、孙宗臣、李明菊、田钊、李俊俊、陈琪曼、武杨、刘振宇、赵芸伟、陈姗姗、李涛、衣强、田申、邵华、费蓓洁、金鑫、吴月升、王小璞、戚琳、徐光侠、柳彩云等。

信息安全技术　网络音视频服务数据安全指南

1　范围

本文件规定了网络音视频服务可以收集、传输、存储、使用、共享、公开披露、删除、出境的数据种类、范围、方式、条件等，以及数据安全保护要求。

本文件适用于网络音视频服务运营者规范数据活动，也适用于主管监管部门、第三方评估机构对网络音视频服务数据活动进行监督、管理、评估时参考。

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

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T AAAAA　信息安全技术　网络数据处理安全规范

GB/T BBBBB　信息安全技术　移动互联网应用（App）收集个人信息基本规范

3　术语和定义

GB/T 25069—2010和GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

网络音视频服务　online audio and video service

通过互联网站、应用程序等网络平台，向用户提供音视频信息制作、发布、传播的服务，也称“网络音视频信息服务”。

注：网络音视频服务主要包括网络音频服务（3.2）、网络视频服务（3.3）以及网络直播服务（3.4），不包括本地音视频播放器服务。

3.2

网络音频服务　online audio service

通过互联网站、应用程序等网络平台，向用户提供音乐、广播、曲艺、有声读物、广播剧、节目赛事直播音频、新闻资讯音频等音频信息制作、发布、传播的服务。

3.3

网络视频服务　online video service

通过互联网站、应用程序等网络平台，向用户提供短视频、在线影音、节目赛事直播视频、新闻资讯视频等视频信息制作、发布、传播的服务。

3.4

网络直播服务 live webcast service

通过互联网站、应用程序等网络平台，向用户提供实时音频信息、视频信息、图文信息等直播信息的发布、传播的服务。

注：本文件中所涉网络直播服务主要包括秀场直播、游戏直播、电商直播等类型，不包括会议直播、在线教育直播等。

3.5

网络音视频服务平台 online audio and video service platform

提供网络音视频服务（3.1）的网络平台。

3.6

网络音视频服务聚合平台 online audio and video service aggregation platform

搭载于智能电视、互联网电视盒等设备中，通过聚合多个网络音视频服务平台（3.5）的音视频信息资源，为用户提供网络音视频服务（3.1）的第三方平台。

3.7

网络音视频服务运营者 online audio and video service operator

向用户提供网络音视频服务（3.1）的组织。本文件中简称“运营者”。

3.8

网络音视频服务数据 online audio and video service data

任何以电子或非电子形式对网络音视频服务（3.1）过程中处理和产生的信息的记录，通常包括用户数据与业务数据。

3.9

网络音视频服务用户 online audio and video service user

使用网络音视频服务（3.1）的个人或组织。本文件中简称“用户”。

注：网络音视频服务用户包括普通用户及网络音视频内容生产用户。

3.10

网络音视频内容生产用户 online audio and video content producer

生产、制作网络音视频内容，并通过网络音视频服务平台（3.5）进行网络音视频内容发布、传播、实时演绎的网络音视频服务用户（3.9）。本文件中简称“内容生产用户”。

注：内容生产用户通常包括普通内容生产用户、专业内容生产用户、网络主播等。

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）

SDK：软件开发工具包（Software Development Kit）

IoT：物联网（Internet of Things）

5 概述

5.1 网络音视频服务组成

网络音视频服务包括网络音频服务、网络视频服务、网络直播服务以及其他网络音视频服务，具体组成要素包括：

a） 参与主体主要包括网络音视频服务用户（包括普通用户与内容生产用户）、网络音视频服务运营者、网络音视频服务第三方（包括第三方技术支持商、内容分发渠道商等）；

b） 服务形式主要包括自建或第三方的网站、App、小程序、SDK 等；

c） 业务功能主要包括网络音视频内容浏览、搜索、播放、下载、收藏、分享、预约、实时发布、实时传播，以及互动交流（发布弹幕、评论等）、会员付费、音视频内容付费、直播打赏、收益分成结算、内容推荐等；

d） 数据类型主要包括用户数据与业务数据（媒资数据、业务运营数据）。

网络音视频服务参与主体数据交互示意图如图 1 所示：

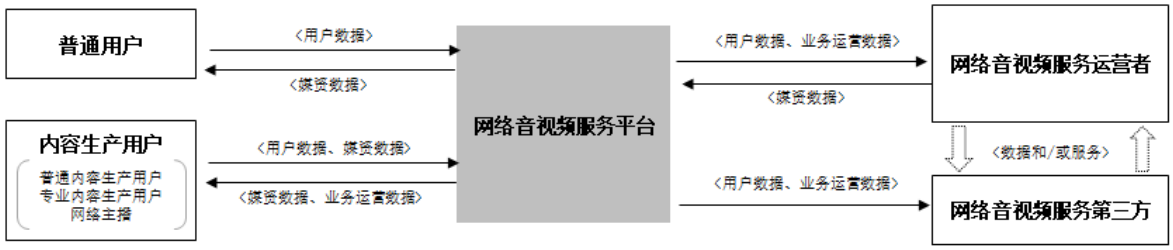

图 1 网络音视频服务参与主体数据交互示意图

5.2 网络音视频服务数据活动与安全风险

5.2.1 网络音视频服务数据活动

网络音视频服务数据活动示意图如图 2 所示：

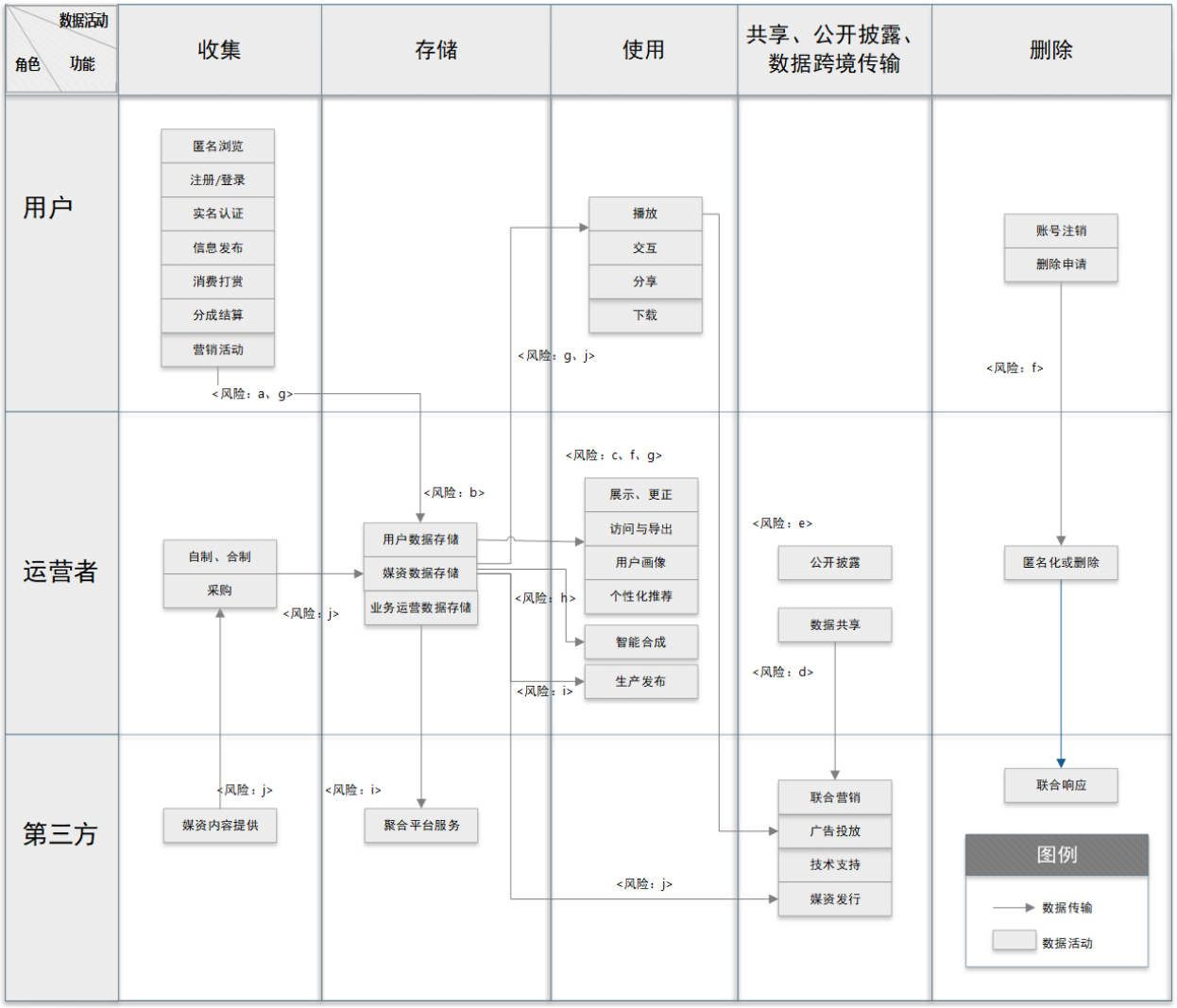

图2 网络音视频服务数据活动示意图

5.2.2 网络音视频服务主要数据安全风险

网络音视频服务中主要数据安全风险包括：

a) 在用户数据收集活动中（如实名认证、IoT 终端音视频服务场景），网络音视频服务运营者存在私自收集、超范围收集用户数据，或过度索取移动终端系统权限导致用户数据被超范围收集的风险；

b) 在用户数据传输、存储活动中，网络音视频服务运营者及相关方（如第三方技术提供商）未采取有效安全措施导致数据泄露或者被窃取、篡改的风险；

c) 在用户数据使用活动中，网络音视频服务运营者未采取脱敏、身份验证或权限控制等安全措施导致用户数据泄露，以及音视频内容与广告推荐等个性化展示场景中用户数据被滥用的风险；

d) 在用户数据共享活动中（如联名会员），用户数据未经授权被共享、超范围共享以及被第三方滥用、第三方无法提供充足安全保障措施等风险；

e) 在用户数据公开披露活动中（如主播黑名单公示），超范围公开披露用户个人敏感信息、未采取数据脱敏等技术导致用户权益受损的风险；

f) 网络音视频服务运营者未能有效响应用户请求导致个人信息权利受损的风险；

g) 未能有效识别未成年用户、未能获得未成年人监护人的有效同意，导致未成年人信息处理不当、未成年人保护措施失效等风险；

h) 智能合成音视频场景下用户数据（如面部识别特征）被滥用、泄露的风险；

i) 网络音视频服务聚合平台场景下用户数据超范围共享、未授权第三方接入等安全风险；

j) 媒资数据收集（自制、合制、采购）、存储、传输、生产、发布、发行等活动中，媒资数据泄露、未授权访问、非法缓存或爬取、盗链等安全风险。

6 基本要求

网络音视频服务运营者应满足以下基本要求：

a) 网络音视频服务的数据活动应符合 GB/T AAAAA 要求；

b) 网络音视频服务的个人信息处理活动应符合 GB/T 35273—2020 要求，网络音视频 App 的个人信息收集活动应符合 GB/T BBBBB 要求；

c) 网络音视频服务运营者应识别数据活动涉及的数据，形成数据保护目录，并对网络音视频服务数据进行分级分类保护。网络音视频服务数据分级分类示例见附录 A。

7 数据收集

7.1 数据收集要求

网络音视频服务运营者在进行数据收集活动时：

a） 应遵循GB/T 35273—2020 第5章、GB/T AAAAA中5.1、GB/T BBBBB第5章的要求；

b） 基本业务功能所需收集的最小必要信息范围，应遵循GB/TBBBBB 附录A中A.9、A.26、A.31的要求；

c） 扩展业务功能收集用户信息的，宜参照GB/T 35273—2020附录C征得用户同意。确定网络音视频服务典型扩展业务功能涉及的可选个人信息收集范围及使用要求时，可参照本文件附录B；

d） 针对普通内容生产用户，应基于手机号码完成实名认证；

e） 针对专业内容生产用户、网络主播，应基于公民身份号码、统一社会信用代码、资质证书等信息完成实名认证；

f） 网络直播服务中，用户使用充值打赏功能的，应事先通过实名认证、人脸识别、人工审核等方式核验身份；

注：实名认证场景下收集用户个人敏感信息时，运营者应通过显著方式告知用户其收集的个人信息类型、使用方式等，并取得用户明示同意。

g） 运营者依托智能电视、智能音箱、车载娱乐系统等IoT智能终端提供网络音视频服务的，应遵循以下要求：

1） 运营者以独立App、网页端等形式实现网络音视频服务，且直接收集用户数据的，应通过弹窗、语音提示、H5页面等方式向用户告知收集、使用个人信息的类型、目的、方式等规则，并取得用户授权同意；

2） 运营者以SDK等形式实现网络音视频服务的，应向IoT智能终端厂商告知有关个人信息收集使用规则及其SDK等的隐私政策链接。

注 1：有屏式 IoT 智能终端应在用户首次开启使用服务时向用户展示个人信息保护政策；无屏式 IoT 智能终端应在用户首次开启时通过语音交互、提示用户扫码查看或阅读文件等方式向用户告知隐私政策核心内容（如最小必要个人信息的收集使用规则），并征得用户授权同意。

注2：网络音视频服务运营者仅作为内容提供商且不涉及用户数据收集、处理的，不适用g)条的要求。

7.2 系统权限要求

网络音视频服务运营者在申请获取用户移动智能终端系统权限时，除应遵循GB/T BBBBB中5.2的要求外，还应：

a) 应在用户使用或触发特定功能时，向用户申请获取与功能实现相关的系统权限；

b) 应在App或小程序内为用户提供便捷的撤回权限授权的功能或路径；

c) 权限申请后，运营者自动访问权限或采集信息的频率应控制在功能所必需的合理最低范围内。

注：网络音视频服务常用系统权限参见本文件附录C。

8 数据使用

8.1 数据展示

网络音视频服务运营者在进行用户数据展示时，应遵循以下要求：

a) 用户在游客模式（未登录账号状态）下使用网络音视频服务时，产生的浏览、播放、下载、收藏、搜索、预约、提醒记录等应仅限当前设备能够查阅；

注1：应为用户提供游客模式或仅浏览模式；

注2：用户在登录账号后，如需将未登录状态产生的使用记录与账号进行绑定的，应取得用户同意。

b) 用户发布评论弹幕、音视频等信息时，网络音视频服务运营者应为用户提供前端匿名发布功能；

c) 用户访问其个人敏感信息时，运营者应采用多因素身份鉴别等安全验证措施；

d) 网络直播打赏排行榜、粉丝榜等运营活动界面涉及展示用户数据时，应对用户数据进行脱敏处理。

8.2 用户画像与个性化展示

网络音视频服务运营者为用户提供个性化内容与广告推荐服务时，除应遵循GB/T 35273—2020中7.5的要求，还应遵循以下要求：

a) 向用户提供新闻类音视频内容个性化展示功能时，应为用户提供设置特定期限或永久退出、关闭个性化展示的功能；

注：新闻类音视频是指有关政治、经济、军事、外交等社会公共事务以及有关社会突发事件的报道、评论类音视频。

b) 宜为用户提供在线关闭个性化广告推送的功能；

注：用户关闭个性化广告不影响运营者进行非个性化广告投放业务。

c) 宜为用户提供自主设置、调整或校正用户画像标签的功能，如针对单项音视频内容或广告设置“不感兴趣”、“屏蔽此类内容”等选项；

d) 以个性化展示为基本业务形态的音视频服务，运营者宜为用户提供设置、校正或重置其画像标签的功能，或单独提供非基于用户画像推送的内容栏目。

8.3 个人信息保护功能

网络音视频服务运营者应根据其所收集的用户数据与产品类型，在产品或服务中融入个人信息保护设计理念，为用户提供多样化个人信息保护功能。运营者宜提供的功能包括：

a) 如提供用户个人主页展示功能，设置选择好友可见范围的功能；

b) 如提供关注、评论和私信功能，设置定向选择互动对象及方式的功能；

注：设置选项可分为“谁可关注我”、“谁可评论我”、“谁可私信我”等。

c) 如提供网络音视频发布功能，设置音视频内容展示范围功能；

注：设置选项可分为“仅自己可见”、“部分公开”、“完全公开”、“仅对好友公开”等。

d) 针对音视频在线社交服务（如添加好友功能），设置社交意向管理功能；

注：设置选项可分为“不把我推荐给通讯录好友”、“不允许通过手机号找到我”等。

e) 针对音视频内容发布等场景，为用户提供“隐藏位置信息”的功能；

f) 针对用户行为与动态展示，设置展示范围控制功能。

注：设置选项可包括：“谁可以看我的动态”、“展示/关闭在线状态”、“不展示我打赏过的主播”等。

9 数据交换

9.1 数据共享

网络音视频服务运营者向第三方共享用户个人信息时，应遵循 GB/T 35273—2020 中 9.2 和 9.5 的要求。在以下典型服务场景下：

a) 电商直播场景下，网络音视频服务运营者向第三方应用导流时，宜使用经技术处理后的账号信息（如 Open ID）与第三方应用进行关联，并在用户点击链接时明示所跳转的第三方应用界面，并提示用户关注第三方应用的个人信息收集使用规则；

b) 游戏直播场景下，为实现游戏内一键开播或直播平台关联游戏账号等功能，运营者与游戏厂商共享用户数据（如用户个人常用设备信息、操作日志）时，宜共建独立的数据库存储前述数据，并采取严格的授权访问机制；

c) 联名会员等营销活动场景下，运营者向联合会员方共享网络身份标识信息前，宜对网络身份标识信息进行加密；

d) 程序化广告场景下，网络音视频服务运营者宜与广告主、广告分发及管理平台等第三方共享经技术措施变换后的设备标识符。

9.2 公开披露

网络音视频服务运营者公开披露个人信息的，除应遵循GB/T 35273—2020中9.4和9.5的要求外，还应遵循以下要求：

a) 对“违法违规用户账号名单”、“网络主播黑名单”等进行公开披露的，应满足法律法规要求或事先取得相关部门批准；

b) 应建立个人信息公开披露评估方法与管理制度，将公开披露信息控制在最小必要范围内；

c) 公开披露个人身份信息时，应采取脱敏等技术措施，如隐去姓名、账号、公民身份号码中的特定字段。

9.3 跨境传输

网络音视频服务运营者将境内运营过程中收集、使用的用户数据向境外提供的，应遵循国家相关规定和相关标准的要求。

10 数据传输与存储

网络音视频服务运营者存储数据时，除应遵循GB/T 35273—2020第6章的要求外，还应遵循以下要求：

a) 通过互联网传输用户数据时，应采用安全通道、数据加密等安全措施；

b) 与第三方通过互联网传输用户数据、媒资数据前，应采用技术手段进行身份鉴别和认证；

c) 对专业内容生产用户、网络主播进行实名认证时采集的个人身份信息等，应加密后单独存储；

d) 因法律法规要求（如监管备查、诉讼时效等原因）需要留存个人信息的，在满足法律法规要求的存储时限后，仍应遵循最小化存储时间要求。

11 个人信息主体权利

网络音视频服务运营者在保障用户个人信息权利实现时，除应遵循 GB/T 35273—2020 第 8 章的要求外，还应遵循以下要求：

a) 用户申请查询、更正、删除个人敏感信息时，应采取技术措施进行账号安全检测，核验用户身份；

注：身份核验的方式通常包括常用设备校验、短信验证码校验等。

b) 应为用户提供便捷的账号注销功能。存在如下情形的，运营者宜设置一定的账号注销前提条件：

1） 普通用户注销账号的，如其账号存在未处理完毕的交易与纠纷、其账号下拥有财产权益（包括零钱、平台虚拟货币、虚拟物品、会员权益等）或法律法规要求限制或禁止注销情形，运营者宜向用户说明注销账号的影响及拒绝的理由。如用户已妥善处理（包括自行提现、结清或自愿放弃等方式）相关财产权益或前述其他待限制情形消除后，运营者应为用户注销账号，并将该账号下的个人信息进行删除或者匿名化处理；

2） 内容生产用户注销账号的，如其账号下存在未处理完毕的交易与纠纷、其与平台签署的线下合同仍在有效期内或法律法规要求限制或禁止注销情形时，运营者宜限制或禁止用户注销账号，并向用户说明理由。前述情形消除后，运营者应为用户注销账号，并将该账号下的个人信息进行删除或者匿名化处理；

3） 除上述限制条件外，运营者可从保障用户权益和履行平台职责角度出发，对账号设置合理的注销限制条件，例如账号近期（不超过十五个工作日）不存在违法违规或被盗风险。针对此类限制条件，应为用户提供专门的申诉渠道。

c) 针对已注销用户已上传的部分用户数据（如弹幕、评论、已上传的音视频内容），运营者依据相关法律法规或与用户的约定仍有权继续展示、使用的，宜采用匿名化的方式继续展示、使用。

12 未成年人个人信息保护

网络音视频服务运营者收集、处理未成年人个人信息的，除应遵循GB/T 35273—2020 5.4 d)的要求，还应遵循以下要求：

a) 宜根据音视频服务类型不同采取差异化技术手段识别未成年人身份；

注1：对于专门或主要面向未成年人提供网络音视频内容或产品（如动漫、动画）的，宜在用户注册时通过弹窗询问、用户主动填写年龄区间信息、出生年月等方式识别未成年人身份；

注2：对于网络直播类服务，宜采取实名认证等方式识别未成年人身份。

b) 宜在技术可行的前提下确认监护人同意的有效性，如采用展示单独的个人信息保护政策、监护人同意书，或通过短信、邮件等方式向监护人发送验证码、验证链接等；

c) 宜提供亲子账号、未成年人虚拟账号等模式，最小化控制对未成年人个人信息的直接收集；

d) 应根据不同的业务功能以及对应收集、使用的信息类型，向用户提供监护人控制功能，如在用户登录账号、充值消费、发布音视频内容、提供/更正/删除个人信息时，通过家长锁、知识验证、短信/邮件验证等方式实现监护人控制，避免未成年人误操作、误提供信息等风险；

e) 在实现语音交互、视频拍摄等功能时，宜默认采用本地保存方式实现功能，经监护人同意后方可上传服务器；

f) 不应收集或分析提取网络音视频内容中的未成年人生物识别信息，不宜向未成年人开放人脸识别、声纹识别等功能；

g) 应在App中设立“青少年模式”，并对该模式下的内容筛选过滤并设置“青少年内容池”，并在该模式下对未成年人使用时长、使用时间、充值打赏、提现、搜索、弹幕评论、内容分享、私信聊天、拍摄发布等功能进行限制；

h） 向未成年人发布商业广告时，应建立广告内容过滤机制，不得发布医疗、药品、保健食品、医疗器械、化妆品、酒类、美容广告，以及不利于未成年人身心健康的网络游戏广告；

i） 未经监护人单独同意的，不宜将未成年人个人信息用于直接营销、用户画像以及个性化广告推送；

j） 宜建立大额充值或异常消费身份认证和拦截机制。在用户使用充值打赏功能时采用实名认证等方式识别到未成年人用户的，应封禁其充值打赏功能；

k） 受理未成年人充值/打赏退费申请或查明申请事实时，运营者收集、使用未成年人及其监护人的信息应遵循最小必要原则。退费事宜处理完毕后，运营者应将前述信息隔离存储，且至少存储3年，法律法规另有规定的除外。

13 网络音视频服务典型场景数据安全要求

13.1 智能合成音视频场景

网络音视频服务运营者利用大数据、机器学习、人工智能等技术制作、发布、传播合成音视频信息时，应遵循以下要求：

a) 展示智能合成的网络音视频信息时，应与其他音视频信息进行显著区分；
注：区分方式包括：标明“合成”等字样或通过不同的栏目、板块、页面展示等。

b) 合成音视频如具有舆论属性或者社会动员特点的，应按照国家有关规定开展安全评估，同时设置播放量、转发次数等阈值，作为触发再次审核评估的条件；

c) 建立合成音视频内容生产者责任制，明确对虚假内容的处罚机制，包括但不限于封禁账号、永久注销等；

d) 宜采取人工或技术手段加强音视频内容的真伪鉴别能力、风险预警能力。

13.2 网络音视频服务聚合平台场景

网络音视频服务聚合平台应采取适当的管理和技术措施加强对合作方的安全管理，具体包括：

a) 应建立合作方接入管理的安全策略和规程，通过个人信息安全影响评估、合作方安全能力评估、签订数据保护协议等方式督促合作方履行个人信息安全保护义务，并要求合作方配合及时响应个人信息主体的合法请求（如个人信息更正、删除或者撤回同意等）；

b) 未经用户同意，不应私自保留、融合后使用聚合平台中来源于合作方的用户账号信息、浏览或播放记录；

c) 针对引入的第三方代码或插件（如 SDK）时，应采用代码安全扫描等技术进行安全检测，及时识别并修复安全漏洞与隐患；

d) 发现合作方存在安全漏洞、个人信息收集使用问题的，应及时向合作方告知问题进行应急处置，必要时可暂时切断合作方的访问渠道。

13.3 网络音视频媒资数据安全

网络音视频服务运营者应建立媒资数据安全保护机制，可采取的媒资数据安全管理和技术措施有：

a) 建立媒资数据分类分级规范，并对网络音视频服务平台上的媒资数据进行分类分级安全管理；
注：媒资数据分类分级示例参见本文件附录 A。

b) 制定媒资数据安全管理规范，通过员工安全意识培训、业务部门重要岗位人员技能培训等方式，加强组织内部人员的媒资数据安全防护意识和能力；

c) 明确媒资数据存储的安全保障措施，建立媒资数据备份机制，包括备份方式、备份频度、存储介质、保存期限等内容，并定期进行容灾备份演练。针对敏感媒资数据可采用云备份、离线备

份等多种备份方式，保障业务可用性；

d) 针对具备媒资数据编辑、制作、发布等功能的后台应用系统，应采取技术措施加强前述应用系统的安全性，具体包括：
   1） 通过代码安全扫描、渗透测试等方式识别应用系统安全漏洞，并对发现的安全漏洞及时进行修复；
   2） 涉及敏感媒资数据审核的功能模块，实施网络隔离、界面添加明文水印、限制下载等安全策略；
   3） 记录并分析系统操作日志信息，针对授权账户的异常操作（如敏感媒资数据批量下载、浏览、播放等）进行安全监控和告警。
e) 采用数字版权管理（DRM）、码流加密、添加数字水印、限制客户端录制和下载功能等媒资数据保护技术，加强音视频内容版权保护；
f) 涉及与外部共享媒资数据时，如通过移动存储介质传输，宜选用具有身份鉴别、全盘加密、密钥管理功能的产品；如通过互联网传输，宜采用网络专线、接口身份验证等安全措施；
g) 应建立媒资数据泄露事件应急响应机制，明确媒资数据安全事件定级标准、事件报告和处置流程，明确媒资业务部门、安全部门及组织其他相关部门的角色及职责，持续更新媒资安全防护策略，定期进行安全审计和策略更新。

附 录 A
（资料性）
网络音视频服务数据分类分级示例

A.1 网络音视频服务数据分类

网络音视频服务数据通常分为用户数据和业务数据。

a） 用户数据是指网络音视频服务运营者在提供网络音视频服务过程中收集、处理的网络音视频服务用户的数据。

b） 业务数据包括媒资数据和业务运营数据，其中媒资数据是指网络音视频服务运营者所拥有和管理的图文、音视频内容及版权信息等数据；业务运营数据是指网络音视频服务运营者在提供网络音视频服务过程中所产生的，主要用于统计分析业务运营情况、或用于故障排查的数据等相关数据。

A.2 网络音视频服务数据分级

本文件根据数据的敏感程度、重要性、保护要求以及一旦泄露、丢失、破坏或非法使用对国家安全、社会秩序、公共利益、企业利益、用户利益造成的危害程度和影响程度等因素，将网络音视频服务数据从高到低分为S4、S3、S2、S1四个级别，运营者应针对不同级别的数据实施不同程度的安全策略：

a) 对于S4级别数据，原则上禁止对外开放，可在极小范围内且在严格限制条件下供访问或使用，如用户个人生物识别信息。

b) 对于S3级别数据，需经过安全审核且采取必要的安全控制措施后，可在较小范围内可控访问或使用，如用户电话号码、电子邮箱地址、交易记录。

c) 对于S2级别数据，需满足组织信息安全管理制度要求和个人信息保护相关要求的前提下，采取适当安全控制措施后，可供访问、使用以及对外共享，如一般业务运营数据。

d) 对于S1级别数据，可在满足个人信息保护相关要求前提下，一定范围内进行公开，如用户昵称、头像等用户自主公开的数据。

注：不同网络音视频服务运营者根据其实际业务情形与场景，可对其用户数据、媒资数据、业务运营数据的范围定义及具体分类分级采取不同的认定结果。

A.3 网络音视频服务数据分类分级示例表

网络音视频服务数据分类分级示例表如表A.1所示：

表A.1 网络音视频服务数据分类分级示例表

一级类别	子类	级别及示例
用户数据	个人基本资料	S1：用户自主公开上传的昵称、头像等
		S2：性别、年龄、国籍、民族、职业等
		S3：真实姓名、电话号码、电子邮箱地址等
	个人身份信息	S4：公民身份号码、护照、残疾人证书、户籍证明等非公开证件类信息、组织资质证件
	个人生物识别信息	S4：用于鉴别用户身份的指纹、声纹、面部识别特征等原始生物特征数据
	网络身份识别信息	S2：注册账号ID、第三方账号ID、账号创建时间和IP地址等
		S4：鉴别信息（账号密码、动态口令、短信验证码、邮箱验证链接、密码提示或找回密码的问题答案）

表A.1 网络音视频服务数据分类分级示例表（续）

一级类别	子类	级别及示例
用户数据	个人财产信息	S2：支付方式、支付笔数、交易类型等
		S3：提现记录、流水记录、支付金额、交易金额、交易日志，以及未公开的虚拟货币、虚拟交易记录等
		S4：银行卡号/信用卡号，兑换码/优惠码等虚拟财产信息
	个人上网记录	S1：用户自主公开的上网记录(如主动公开上传的照片、音视频、歌单、观影历程报告等)
		S2：基于用户行为统计分析形成的用户间接画像
		S3：用户未公开的浏览记录、搜索记录、收藏记录、下载/缓存记录、预约记录等
	其他个人信息	S2：匿名设备标识符等
		S3：通讯录信息
业务数据	媒资数据	S1：专业内容生产用户上传的公开音视频/图文内容、主播公开的直播内容
		S2：专业内容用户上传的私密音视频/图文内容
		S3：花费一定成本采购或自制/合制的未公开的音视频内容、字幕翻译信息
		S4：花费高成本采购或自制/合制的未公开的音视频内容、字幕翻译信息。
	业务运营数据	S1：公开的业务运营数据，例如平台运营者公开发布的用户量、业务收益等数据
		S2：一般业务运营数据，一般业务后台统计数据等
		S3：重要业务运营数据，如重要业务后台统计数据（包括但不限于弹幕/打赏/流量信息、标签内容、热度值、产品运营报表分析等信息）等
		S4：专业内容生产用户的资质证明材料、会员收益数据（包含虚拟货币收益）、核心后台统计数据（包括但不限于用户间接画像、产品运营报表分析等信息）

附 录 B
（资料性）
网络音视频服务可选个人信息收集范围及使用要求

网络音视频服务运营者可选个人信息收集范围及使用要求如表B.1所示：

表B.1 网络音视频服务可选个人信息收集范围及使用要求

个人信息类型	使用要求
头像、昵称、生日、性别、所在地、个性签名	仅用于用户个人资料展示。
移动电话号码、电子邮件地址、验证码或口令	仅用于账号注册登录、身份认证、保障账号安全、提供客服功能。
内容生产用户的姓名、身份证件信息、面部识别特征	仅用于内容生产用户身份认证及安全风险控制。
浏览记录、搜索记录、收藏/关注/预约列表	仅用于提供用户搜索、收藏、关注、预约的内容以及个性化展示。
用户生产发布的音视频内容、评论弹幕等用户发布信息记录	仅用于为用户提供音视频制作发布功能、用户间交流互动服务。
银行卡信息、第三方支付账号信息、交易记录、支付记录、收货信息	仅用于提供商品与/或服务的购买与交付服务。
内容生产用户收益流水记录、收款信息	仅用于内容生产用户收益结算提现服务。
通讯录信息、好友列表	仅用于添加或关注其他用户、社交分享等服务。
地理位置信息	仅用于网络音视频内容推荐、安全风险控制。
用户与客服的沟通记录	仅用于为用户提供客户服务、处理与用户间争议纠纷。

附 录 C
（资料性）
网络音视频服务 App 相关系统权限申请范围及使用要求

C.1 Android权限范围

表C.1 Android App相关系统权限申请范围及使用要求

权限名称	使用要求
CAMERA 拍摄	仅用于拍摄照片/视频、直播、扫码、实名认证、头像上传/修改等场景。
RECORD_AUDIO 录音	仅用于语音搜索、语音聊天、音视频录制、直播等语音输入场景。
WRITE_CALENDAR 编辑日历	仅用于网络音视频服务预约、提醒等场景。
ACCESS_COARSE_LOCATION 访问粗略位置	仅用于基于城市或地域进行个性化展示。
ACCESS_FINE_LOCATION 访问精准定位	仅用于用户内容发布、直播时展示所在位置。
READ_EXTERNAL_STORAGE 读取外置存储器	仅用于上传用户选择的设备中的照片、音频、视频等。
WRITE_EXTERNAL_STORAGE 写入外置存储器	仅用于将网络音视频内容、图片等缓存/下载到设备中。
READ_PHONE_STATE 读取设备信息	仅用于安全风控等网络安全保障，对用户常用设备进行标识、监测账户异常登录、关联用户行为等。
READ_CONTACTS 读取通讯录	仅用于添加或关注其他用户、社交分享等服务。

C.2 iOS权限范围

表C.2 iOS App相关系统权限申请范围及使用要求

权限名称	使用要求
Camera 拍摄	仅用于拍摄照片/视频、直播、扫码、实名认证、头像上传/修改等场景。
Photos 照片	仅用于上传用户选择的设备中的照片、视频等。
Microphone 麦克风	仅用于语音搜索、语音聊天、音视频录制、直播等语音输入场景。
Contacts 通讯录	仅用于添加或关注其他用户、社交分享等服务。
Calendar 日历	仅用于网络音视频服务预约、提醒等场景。
Location 位置	仅用于基于城市或地域进行个性化展示以及用户内容发布、直播时展示所在位置。

参 考 文 献

[1] 中华人民共和国网络安全法（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

[2] 中华人民共和国消费者权益保护法（1993 年 10 月 31 日第八届全国人民代表大会常务委员会第四次会议通过，2013 年 10 月 25 日第十二届全国人民代表大会常务委员会第五次会议第二次修正）

[3] 中华人民共和国电子商务法（2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过）

[4] 电信和互联网用户个人信息保护规定（2013 年 7 月 16 日工业和信息化部令第 24 号公布）

[5] 儿童个人信息网络保护规定（2019 年 8 月 22 日国家互联网信息办公室令第 4 号公布）

[6] 网络音视频信息服务管理规定（2019 年 11 月 18 日国家互联网信息办公室、文化和旅游部、国家广播电视总局国信办通字〔2019〕3 号公布）

[7] 互联网信息服务管理办法（2000 年 9 月 25 日国务院令第二百九十二号公布，2011 年 1 月 8 日国务院修订）

[8] 互联网直播服务管理规定（2016 年 11 月 4 日国家互联网信息办公室公布）

[9] 互联网视听节目服务管理规定（2007 年 12 月 20 日国家广播电影电视总局、信息产业部令第 56 号公布，2015 年 8 月 28 日国家新闻出版广电总局令第 3 号修订）

[10] 互联网用户公众账号信息服务管理规定（2017 年 9 月 7 日国家互联网信息办公室公布）

[11] 移动互联网应用程序信息服务管理规定（2016 年 6 月 28 日国家互联网信息办公室公布）

[12] 网络表演经营活动管理办法（2016 年 12 月 2 日文化部文市发〔2016〕33 号公布）

[13] 具有舆论属性或社会动员能力的互联网信息服务安全评估规定（2018 年 11 月 15 日国家互联网信息办公室、公安部公布）

[14] App 违法违规收集使用个人信息行为认定方法（2019 年 11 月 28 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局国信办秘字〔2019〕191 号公布）

[15] 互联网个人信息安全保护指南（2019 年 4 月 10 日公安部、北京市网络行业协会公布）

[16] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[17] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

[18] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[19] TC260-PG-20202A 网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南

[20] TC260-PG-20191A 网络安全实践指南—移动互联网应用基本业务功能必要信息规范