App隐私合规检测报告

**——安全团队**

**—— 安全人员**

**目 录**

[一、检测依据 4](#_Toc53389165)

[二、应用基本信息 4](#_Toc53389166)

[三、测评结果 5](#_Toc53389167)

[四、评估详情内容 6](#_Toc53389168)

[1. 未公开收集使用规则 6](#_Toc53389169)

[1.1. 是否有隐私政策等收集使用规则 6](#_Toc53389170)

[1.2. 是否提示用户阅读隐私政策等收集使用规则 7](#_Toc53389171)

[1.3. 隐私政策等收集使用规则是否易于访问 7](#_Toc53389172)

[1.4. 隐私政策等收集使用规则是否易于阅读 8](#_Toc53389173)

[1.5. 公开的收集使用规则是否完整 9](#_Toc53389174)

[2. 未明示收集使用个人信息的目的、方式和范围 10](#_Toc53389175)

[2.1. 是否逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等 10](#_Toc53389176)

[2.2. 是否以适当方式通知用户收集使用个人信息的目的、方式、范围发生变化 11](#_Toc53389177)

[2.3. 是否同步告知申请打开权限和要求提供个人敏感信息的目的 11](#_Toc53389178)

[2.4. 收集使用规则是否易于理解 12](#_Toc53389179)

[3. 未经用户同意收集使用个人信息 12](#_Toc53389180)

[3.1. 收集个人信息或打开可收集个人信息的权限前是否征得用户同意 12](#_Toc53389181)

[3.2. 用户明确表示不同意收集后是否仍收集个人信息或打开可收集个人信息的权限 13](#_Toc53389182)

[3.3. 用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用 13](#_Toc53389183)

[3.4. 实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围 14](#_Toc53389184)

[3.5. 是否以默认选择同意隐私政策等非明示方式征求用户同意 15](#_Toc53389185)

[3.6. 是否未经用户同意更改其设置的可收集个人信息权限状态 15](#_Toc53389186)

[3.7. 利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息选项 16](#_Toc53389187)

[3.8. 是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限 16](#_Toc53389188)

[3.9. 是否向用户提供撤回同意收集个人信息的途径、方式 17](#_Toc53389189)

[3.10. 是否违反其所声明的收集使用规则，收集使用个人信息 17](#_Toc53389190)

[4. 违反必要原则，收集与其提供的服务无关的个人信息 18](#_Toc53389191)

[4.1. 是否收集与业务功能无关的个人信息 18](#_Toc53389192)

[4.2. 用户是否可拒绝收集非必要信息或打开非必要权限 18](#_Toc53389193)

[4.3. 是否以非正当方式强迫收集用户个人信息 19](#_Toc53389194)

[4.4. 收集个人信息的频度是否超出业务功能实际需要 20](#_Toc53389195)

[5. 未经同意向他人提供个人信息 20](#_Toc53389196)

[5.1. 向他人提供个人信息前是否征得用户同意 20](#_Toc53389197)

[5.2. 向接入的第三方应用提供个人信息前是否经用户同意 21](#_Toc53389198)

[6. 未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息 22](#_Toc53389199)

[6.1. 是否提供有效的注销用户账号功能 22](#_Toc53389200)

[6.2. 是否提供有效的更正或删除个人信息 22](#_Toc53389201)

[6.3. 是否建立并公布个人信息安全投诉、举报渠道 23](#_Toc53389202)

**[附件一：Android涉及个人信息权限](#_Toc53389203)** [25](#_Toc53389203)

**[附件二：个人信息](#_Toc53389204)** [30](#_Toc53389204)

**[附件三：个人敏感信息](#_Toc53389205)** [32](#_Toc53389205)

# 一、检测依据

* 《网络安全法》
* 《APP违法违规收集使用个人信息行为认定方法》
* 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》
* GB/T 35273《信息安全技术 个人信息安全规范》

# 二、应用基本信息

|  |  |
| --- | --- |
| 应用名称 | xxxxxx |
| 应用包名 | xxxxxxxxx |
| 版本 | x.x.x |
| 应用平台 | Android |
| 评估规范 | 《移动互联网应用程序（App）收集使用个人信息自评估指南（TC260-PG-20202A）》 |

# 三、测评结果

**共计发现该应用存在x处不合规项。相关问题下：**

| **编号** | **问题描述** | **检测结果** | **合规建议** |
| --- | --- | --- | --- |
| 1 | 打开申请的权限未同步告知用户其目的。 | 不合规 |  |
| 2 | 隐私政策同意前收集个人信息。 | 不合规 |  |
| 3 | 用户拒绝位置权限后每次打开App频繁征求用户同意授权位置权限。 | 不合规 |  |
| 4 | 隐私政策同意前App集成的第三方SDK既未经用户同意，也未做匿名化处理向第三方提供个人信息。 | 不合规 |  |
| 5 | 手机信息类型及用途描述中收集个人信息的业务功能使用等方式概括说明所有业务功能。 | 不合规 |  |

# 四、评估详情内容

## 未公开收集使用规则

### 是否有隐私政策等收集使用规则

|  |  |
| --- | --- |
| 评估点 | 是否有隐私政策等收集使用规则 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 在App界面中能够找到隐私政策，包括通过弹窗、文本链接、附件、常见问题（FAQs）等形式，且隐私政策可正常显示。  b) 隐私政策中需包含收集使用个人信息规则的相关内容。  c) 隐私政策文本链接有效，且文本可正常显示。  d) 如存在涉及收集使用儿童个人信息相关业务功能的，需制定针对儿童的个人信息保护规则。  注 1：详见 2019 年国家互联网信息办公室令（第 4 号）《儿童个人信息网络保护规定》。  注 2：例如收集不满十四周岁的未成年人个人信息的教育类App，需制定针对儿童的个人信息保护规则。" |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、App使用界面无个人信息保护相关个人信息保护政策条款，或个人信息保护政策条款链接无效，此项视为不符要求；  2、在个人信息保护政策中无包含收集、使用个人信息规则，此项视为不符合要求。 |
| 测试方法 | 1、检查App是否有个人信息保护政策；  2、检测个人信息保护政策中是否将收集个人信息的业务功能罗列； |
| 备注 |  |

### 是否提示用户阅读隐私政策等收集使用规则

|  |  |
| --- | --- |
| 评估点 | 是否提示用户阅读隐私政策等收集使用规则 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) App需在首次运行或用户注册时通过弹窗等明显方式，提示用户阅读隐私政策。  b) 避免使用灰色字体、缩小字号、键盘遮挡、置于边缘等方式未突出显示隐私政策链接。  不合规：例如采用与背景颜色相近的字体、刻意缩小字号、弹出键盘遮挡、置于边缘等为不明显方式展示隐私政策链接。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、首次启动App时，经检查发现无个人信息保护政策，或个人信息保 护政策有遮挡、不突出，此项视为不符合要求； |
| 测试方法 | 1、检查APP是否有个人信息保护政策；  2、检查在首次开启APP时，是否有阅读个人信息保护政策入口； |
| 备注 |  |

### 隐私政策等收集使用规则是否易于访问

|  |  |
| --- | --- |
| 评估点 | 隐私政策等收集使用规则是否易于访问 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 用户进入App主功能界面后，通过 4 次（含）以内的点击，能够访问到隐私政策。  b) 在App常规交互界面展示隐私政策链接，避免仅在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查看隐私政策的情形。  c) 隐私政策以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、进入App主功能界面后，通过5次或5次以上的点击，才能够访问到个人信息保护政策，此项视为不符要求。  2、个人信息保护政策链接位置有遮挡、不突出，或App交互界面未提供链接，此项视为不符要求。  3、隐私政策未独立成文的，此项视为不符要求。 |
| 测试方法 | 1、检查App个人信息保护政策是否独立成文  2、检查在App中个人信息保护政策是否在4次点击之内访问到；  3、查看个人信息保护政策链接位置是否突出、无遮挡点击个人信息保护政策链接，正确进入个人信息保护政策阅读界面。 |
| 备注 |  |

### 隐私政策等收集使用规则是否易于阅读

|  |  |
| --- | --- |
| 评估点 | 隐私政策等收集使用规则是否易于阅读 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 隐私政策文本文字显示方式（字号、颜色、行间距、清晰度等）不会造成阅读困难。  b) 需提供简体中文版隐私政策。  c) 隐私政策的内容需符合通用的语言习惯，使用标准化的数字、图示，避免出现错别字或有歧义的语句。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、文本文字显示方式（字体、大小、颜色、 行间距等），造成阅读困难，此项视为不符要求。  2、无提供简体中文版，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策是否为简体中文版；  2、查看文本文字显示方式（字体、大小、颜色、行间距等）是否易于阅读 |
| 备注 |  |

### 公开的收集使用规则是否完整

|  |  |
| --- | --- |
| 评估点 | 公开的收集使用规则是否完整 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | a) 隐私政策应对App运营者基本情况进行描述，至少包括组织或公司名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。  b) 隐私政策应说明发布、生效或更新日期。  c) 说明收集使用个人信息的目的、方式、范围。  d) 对个人信息存放地域（境内、境外哪个国家或地区）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明。  e) 如果将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。  注：如部分业务功能不涉及用户画像、个性化展示，可在规则中明确说明。  f) 如果存在个人信息出境情形，说明出境个人信息类型并显著标识。  注：例如可采用字体加粗、标星号、下划线、斜体、不同颜色等显著标识方式。  e) 隐私政策中应对App运营者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等。  g) 对个人信息保护方面采取的措施和具备的能力进行说明。  h) 如果存在个人信息对外共享、转让、公开披露的情况，说明以下内容：①对外共享、转让、公开披露个人信息的目的；②涉及的个人信息类型；③接收方类型或身份。  i) 对以下用户权利和相关操作方法进行说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账号注销；⑤撤回已同意的授权。  j) 至少说明以下一种投诉、举报渠道：①电子邮件；②电话；③在线客服；④在线表单；⑤即时通信账号。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、未参照法务提供的《公司-用户个人信息保护政策模板（清洁版）0924》修改的，此项视为不符要求。 |
| 测试方法 | 1、检查隐私政策是否与法务提供格式与内容相符合 |
| 备注 |  |

## 未明示收集使用个人信息的目的、方式和范围

### 是否逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等

|  |  |
| --- | --- |
| 评估点 | 是否逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | 在隐私政策中需详细说明App使用的第三方插件及收集使用个人信息的目的、方式、范围。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、检测个人信息保护政策中是否将收集个人信息的业务功能未一一列举，此项视为不符要求。  2、检测个人信息保护政策中第三方SDK收集个人信息未一一列举，此项视为不符要求。  3、未参照法务提供的《公司-用户个人信息保护政策模板（清洁版）0924》修改的，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策是否说明个人信息收集的目的  2、个人信息保护政策是否说明个人信息使用的目的、方式、范围  3、个人信息保护政策中是否说明使用的第三方SDK  4、个人信息保护政策是否说明第三方SDK收集的个人信息 |
| 备注 |  |

### 是否以适当方式通知用户收集使用个人信息的目的、方式、范围发生变化

|  |  |
| --- | --- |
| 评估点 | 是否以适当的方式通知用户收集使用个人信息的目的、方式、范围发生的变化 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 收集使用个人信息的目的、方式和范围发生变化时，应以适当方式通知用户，适当方式包括更新隐私政策并以信息、邮件、弹窗等方式提醒用户阅读发生变化的条款等。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、查看隐私政策中是否说明更新、生效时间，或通过弹窗提醒用户授权同意。 |
| 测试方法 | 1、个人信息保护政策中是否说明更新时间、生效时间  2、实际使用APP，查看个人信息保护政策更新时是否主动提醒用户查看 |
| 备注 |  |

### 是否同步告知申请打开权限和要求提供个人敏感信息的目的

|  |  |
| --- | --- |
| 评估点 | 是否同步告知申请打开权限和要求提供个人敏感信息的目的 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 在申请打开可收集个人信息的权限时，App应通过显著方式（如弹窗提示等）同步告知用户其目的，对目的的描述应明确、易懂。  注：常见可收集个人信息的系统权限有：  iOS系统: 定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康；  Android系统:日历、通话记录、相机、通讯录、位置、麦克风、电话、传感器、短信、存储。  b) 在要求用户提供个人敏感信息（用户身份证号、银行账号、行踪轨迹等）时，App应通过显著方式（如弹窗提示、文字备注、文本链接等）同步告知用户其目的，对目的的描述应明确、易懂。 |
| 测试位置 | 扩展类权限申请交互测试 |
| 测试要点 | 1、使用扩展类权限时未同步告知其目的，此项视为不符要求。  2、目的描述模糊，不明确，此项视为不符要求。 |
| 测试方法 | 1、点击App中所有功能触发扩展类权限申请，查看是否有自定义弹窗告知；  2、检查告知内容目的是否描述清晰。 |
| 备注 |  |

### 收集使用规则是否易于理解

|  |  |
| --- | --- |
| 评估点 | 收集使用规则是否易于理解 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | a) 有关收集使用规则的内容需简练、结构清晰、重点突出。  注：例如使用晦涩难懂的词语、冗长繁琐的篇幅、大量专业术语、逻辑结构混乱等易造成用户难以理解。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、查看隐私政策或告知用户收集个人信息的目的是否包含大量专业术语、冗长繁琐  2、未参照法务提供的《公司-用户个人信息保护政策模板（清洁版）0924》修改的，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策内容是否通俗易懂。  2、个人信息保护政策是否收集个人信息的使用规则简洁、清晰。 |
| 备注 |  |

## 未经用户同意收集使用个人信息

### 收集个人信息或打开可收集个人信息的权限前是否征得用户同意

|  |  |
| --- | --- |
| 评估点 | 收集个人信息或打开可收集个人信息的权限前是否征得用户同意 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改  2、App在用户授权同意隐私政策或权限后，再进行个人信息收集。 |
| 评估标准 | a) App收集个人信息前应提供由用户主动选择同意或不同意（包括退出、上一步、关闭、取消等）的选项。  b) 未征得用户同意时，不应收集个人信息或打开可收集个人信息权限。如App首次打开时，在用户未得知收集个人信息的目的前，App就开始收集个人信息。  注：征得同意，指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。"  c) 不应在征得用户同意前，利用Cookie等同类技术、或私自调用可收集用户个人信息的权限等方式收集个人信息。 |
| 测试位置 | 隐私协议与运行态检查 |
| 测试要点 | 1、App收集个人信息前未提供用户主动选择选项，此项视为不符要求。  2、用户未授权前App或SDK开始收集个人信息，或打开个人信息权限，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策是否提供用户自主选项  2、targetSdkVersion < 23则不合规  3、在同意收集个人信息前，查看APP是否收集个人信息  4、在同意打开收集个人信息权限前，查看APP是否收集个人信息权限 |
| 备注 |  |

### 用户明确表示不同意收集后是否仍收集个人信息或打开可收集个人信息的权限

|  |  |
| --- | --- |
| 评估点 | 用户明确表示不同意收集后是否仍收集个人信息或打开可收集个人信息的权限 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、App在用户授权同意隐私政策或权限后，再进行个人信息收集。 |
| 评估标准 | a) 用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作，明确拒绝App收集某类个人信息后，不应以任何形式收集该类个人信息或打开可收集个人信息的权限。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、用户明确拒绝授权后App或SDK继续收集个人信息，或打开个人信息权限，此项视为不符要求。 |
| 测试方法 | 1、App索取相应授权，点击拒绝，查看App是否收集个人信息与权限 。 |
| 备注 |  |

### 用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用

|  |  |
| --- | --- |
| 评估点 | 用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 用户明确表示不同意收集后，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意收集个人信息。  b) 用户明确表示不同意收集后，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意打开可收集个人信息的权限。  注：为支持App正常运行，或用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰情形。例如用户拒绝授权“相机”权限后的 48 小时内，主动选择使用拍摄、扫码等功能时，App再次申请打开该权限的情形不属于频繁干扰。" |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、验证App在明确拒绝授权后，是否多次频繁弹窗或其他形式地征求用户同意授权，影响用户正常使用，此项视为不符要求。 |
| 测试方法 | 1、拒绝收集个人信息或收集个人信息的权限，查看APP是否超过2次征求用户同意 |
| 备注 |  |

### 实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围

|  |  |
| --- | --- |
| 评估点 | 实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、根据隐私政策中声明的收集个人信息规则进行相应的收集个人信息或打开收集个人信息权限。 |
| 评估标准 | a) 收集使用个人信息的过程需与其所声明的隐私政策等收集使用规则保持一致。实际收集的个人信息类型、申请打开可收集使用个人信息的权限等与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、隐私政策收集个人信息规则或其他声明，与App实际收集个人信息内容进行对比不一致的，此项视为不符要求。 |
| 测试方法 | 1、查看个人信息保护政策中说明的收集个人信息  2、实际使用APP，查看APP运行过程中收集的个人信息或打开的收集个人信息权限。  3、根据1、2进行对比，查看实际运行的信息是否超出个人信息保护政策 中描述的信息 |
| 备注 |  |

### 是否以默认选择同意隐私政策等非明示方式征求用户同意

|  |  |
| --- | --- |
| 评估点 | 是否以默认选择同意隐私政策等非明示方式征求用户同意 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 在首次运行、用户注册等时，可通过弹窗、突出链接等明示方式提醒用户阅读隐私政策后征求用户同意，不采用默认勾选隐私政策等非明示方式。  b) 通过设置“下一步”“注册”“登录即代表同意”等方式征求用户同意的情形，除以显著方式展示隐私政策等收集使用规则外，还需明确执行上述动作与同意隐私政策之间的逻辑关系，以达到主动提醒用户主动阅读隐私政策后征求用户同意的效果。  注：隐私政策等收集使用规则未发生变化时无需反复征求用户同意。如App更新后，隐私政策无变化时，无需再次征求用户同意隐私政策。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、查看App在申请隐私政策授权时，默认选择同意或默认勾选及同意，此项视为不符要求。 |
| 测试方法 | 1、实际使用APP，查看个人信息保护政策在征求用户同意时，是否默认勾选、被遮盖等 |
| 备注 |  |

### 是否未经用户同意更改其设置的可收集个人信息权限状态

|  |  |
| --- | --- |
| 评估点 | 是否未经用户同意更改其设置的可收集个人信息权限状态 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 未经用户同意，不私自更改用户设置的可收集个人信息权限和收集使用个人信息相关功能的状态。  注：例如未经用户同意，在更新升级后，将用户设置的可收集个人信息权限恢复到默认状态，或将用户已关闭的使用通讯录匹配好友等功能重新打开。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App中在用户未进行明示同意授权前，私自更改权限状态，此项视为不符要求。 |
| 测试方法 | 1、实际使用APP，查看APP打开的权限  2、更新APP，查看APP打开的权限  3、将1与2进行对比，查看APP是否对权限状态进行更改 |
| 备注 |  |

### 利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息选项

|  |  |
| --- | --- |
| 评估点 | App利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息的选项 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) 存在利用用户个人信息和算法定向推送信息情形（包括利用个人信息和算法推送新闻和信息、展示商品、推送广告等），应提供拒绝接受定向推送信息，或者停止、退出、关闭相应功能的机制，或者不基于个人信息、用户画像等推送的模式、选项。  注：相关定义和内容可参考GB/T 35273《个人信息安全规范》。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App中提供定向推送，但无关闭定向推送功能，此项视为不符要求。 |
| 测试方法 | 1、实际使用APP，查看APP是否提供可关闭定向推送信息功能 |
| 备注 |  |

### 是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限

|  |  |
| --- | --- |
| 评估点 | 是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、将应欺诈，诱导用户同意收集个人信息功能或打开收集 个人信息权限的声明进行删除，并修改对应收集个人信息及权限。 |
| 评估标准 | a) 明示收集使用个人信息的目的需真实、准确。不故意欺瞒、掩饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限。  注：例如App提示用户打开通讯录权限以参与红包、金币、抽奖等活动。事实上，通讯录权限与上述活动之间毫无关联，App诱骗用户打开通讯录权限后，立即上传用户通讯录信息，并将该类信息用于发送商业广告或其它目的。" |
| 测试位置 |  |
| 测试要点 | 1、App中存在欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限的业务功能或声明内容，此项视为不符要求。 |
| 测试方法 | 1、查看APP在运行过程中，是否有以欺诈、诱骗等不正当方式误导用户 同意收集个人信息或授权收集个人信息的权限 |
| 备注 |  |

### 是否向用户提供撤回同意收集个人信息的途径、方式

|  |  |
| --- | --- |
| 评估点 | 是否向用户提供撤回同意收集个人信息的途径、方式 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改 |
| 评估标准 | a) App应向用户提供撤回同意收集个人信息的途径、方式，并在隐私政策等收集使用规则中予以明确。  b) 如用户拒绝或撤回特定业务功能收集个人信息的授权时，App不应暂停提供其他业务功能，或降低其他业务功能的服务质量。  c) 如用户拒绝或撤回可收集个人信息的权限时，不得影响用户正常使用与该权限无关的功能，除非该权限是保证App正常运行所必需。 |
| 测试位置 | 隐私协议与运行态检查 |
| 测试要点 | 1、App中未向用户提供撤回、关闭同意收集个人信息的功能、途径、方式等，此项视为不符要求。 |
| 测试方法 | 1、查看个人信息保护政策中是否说明可撤回同意收集个人信息的途径、方式。  2、实际使用APP，查看APP中是否有撤回同意收集个人信息的途径、方式 |
| 备注 |  |

### 是否违反其所声明的收集使用规则，收集使用个人信息

|  |  |
| --- | --- |
| 评估点 | 是否违反其所声明的收集使用规则，收集使用个人信息 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、增加隐私政策声明描述 |
| 评估标准 | a) 开展个人信息处理活动需严格遵循所公开的隐私政策等收集使用规则，并遵守与用户的约定；如个人信息使用目的、方式、范围等发生变化的，需再次征得用户同意。 |
| 测试位置 | 隐私协议 |
| 测试要点 | 1、App中所有功能业务中收集个人信息内容，与已授权的隐私政策及其他声明的收集个人信息规则不一致，此项视为不符要求。 |
| 测试方法 | 1、查看个人信息保护政策中说明的收集使用个人信息的规则  2、实际使用APP，查看APP实际收集个人信息  3、实际使用APP，查看APP实际的个人信息使用规则  4、将1与2、3对比，判断是否违反个人信息保护政策中说明的规则 |
| 备注 |  |

## 违反必要原则，收集与其提供的服务无关的个人信息

### 是否收集与业务功能无关的个人信息

|  |  |
| --- | --- |
| 评估点 | 是否收集与业务功能无关的个人信息 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、建议删除或关闭与业务功能无关的个人信息或打开申请打开的个人信息权限。 |
| 评估标准 | a) 不应收集与业务功能无关的个人信息。  b) 不申请打开与业务功能无关的可收集个人信息的权限。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App收集的个人信息或申请授权的与个人信息相关权限与当前使用的业务功能无关，此项视为不符要求。 |
| 测试方法 | 1、使用App，判断App的业务功能  2、查看App收集的个人信息，判断收集的个人信息是否与APP的业务功能无关  3、查看APP打开的权限，判断打开的权限是否与APP的业务功能无关 |
| 备注 |  |

### 用户是否可拒绝收集非必要信息或打开非必要权限

|  |  |
| --- | --- |
| 评估点 | 用户是否可拒绝收集非必要信息或打开非必要权限 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、在用户拒绝收集与业务功能无关的个人信息或打开、申请无关的个人信息权限时，保留其他业务功能正常使用。 |
| 评估标准 | a) 收集与业务功能相关但非必要的个人信息或申请打开相关但非必要的可收集个人信息权限时，需由用户自主选择同意，如用户不同意，不影响其使用现有业务功能或相关服务。  b) 不将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需可收集个人信息权限，作为业务功能打开的前提条件。  c) 如提供无需注册即可使用的服务模式（如仅浏览、游客模式），当用户拒绝同意该类服务模式以外的个人信息收集行为时，不影响其使用仅浏览等功能。  注 1：必要信息指与业务功能直接相关的个人信息，缺少该个人信息则无法提供最基本的服务。必要信息范围可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，如果服务类型不在该标准内，则可根据其业务特点，参考该标准相关定义和理念自行分析。  注 2：相关内容和实践案例可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.3 节及其附录C。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App在拒绝功能业务非必要收集的个人信息或权限时，直接拒绝、 关闭业务功能，此项视为不符要求。 |
| 测试方法 | 1、拒绝所有扩展权限申请， 检查应用是否 完全不可用  2、仅通过与功能有关的权限，对无关功能权限进行拒绝，再检查应用是否 完全不可用 |
| 备注 |  |

### 是否以非正当方式强迫收集用户个人信息

|  |  |
| --- | --- |
| 评估点 | 是否以非正当方式强迫收集用户个人信息 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、 |
| 评估标准 | a) 根据用户主动填写、点击、勾选等自主行为，作为各个业务功能打开或开始收集使用个人信息的前提条件。  b) 新增业务功能申请收集的个人信息超出用户原有同意范围时，不应因用户拒绝新增业务功能收集个人信息的请求，拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外。  c) 不仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集其个人信息并以此作为提供服务的条件。  d) 不以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限。  注：例如将安卓版App的targetSdkVersion值设置低于 23，通过声明机制，在安装App时要求用户一次性同意打开多个可收集个人信息权限属于捆绑方式。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App新增的功能业务需申请收集个人信息授权同意，在拒绝同意 时，关闭原有业务功，此项视为不符要求。  2、App在使用过程中以改善服务质量、提升用户体验、定向推送信 息、研发新产品等为由，强制要求用户同意授权收集个人信息，此项视为不符要求。  3、App的targetSdkVersion是否大于23，在申请用户授权同意时， 进行批量申请，用户拒绝后关闭、退出App，此项视为不符要求。 |
| 测试方法 | 1、拒绝新功能申请的权限，判断原有功能是否仍可使用  2、是否能关闭定向推送等功能，关闭后是否能正常使用其他功能  3、targetSdkVersion< 23  4、是否出现权限组的授权  5、拒绝授权之后，判断App是否可用 |
| 备注 |  |

### 收集个人信息的频度是否超出业务功能实际需要

|  |  |
| --- | --- |
| 评估点 | 收集个人信息的频度是否超出业务功能实际需要 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、降低收集个人信息的频率，并提供合理的目的或解释 |
| 评估标准 | a) 收集个人信息的频度不超出业务功能实际需要，在用户使用某业务功能过程中，仅收集与当前业务功能相关的个人信息。  b) 在App未打开或处于后台运行状态时，不收集用户个人信息，除非业务功能需要后台运行时继续提供服务，如导航功能等。  注：在用户主动关闭App后，未经用户同意不采用自启动、关联启动方式收集个人信息。"  c) 接入第三方应用时，不私自截留第三方应用收集的个人信息。  注：例如信息查询类App，在用户向第三方应用提交相关个人信息时，截留用户个人信息并上传至其后端服务器的行为属于私自截留个人信息。 |
| 测试位置 | 运行态检查 |
| 测试要点 | 1、App在运行时，收集个人信息的频率，并结合功能业务需求判断是否 超出业务功能实际需求。 |
| 测试方法 | 1、判断App是否以合理的频度收集必要的个人信息  2、App未打开或处于后台运行状态时，查看是否收集个人信息 |
| 备注 |  |

## 未经同意向他人提供个人信息

### 向他人提供个人信息前是否征得用户同意

|  |  |
| --- | --- |
| 评估点 | 向他人提供个人信息前是否征得用户同意 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、建议在向第三方插件提供用户个人信息时，对个人信息内容 进行匿名化处理，或征得用户授权同意 |
| 评估标准 | a) 如存在从客户端直接向第三方发送个人信息的情形，包括通过App客户端嵌入第三方代码、插件（如SDK）等方式，应事先征得用户同意，经匿名化处理的除外。  b) 如个人信息传输至服务器后，App运营者向第三方提供其收集的个人信息，应事先征得用户同意，经匿名化处理的除外。  c) 如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。  注：“匿名化”的定义可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》3.14 节。" |
| 测试位置 | 隐私协议&运行态检查 |
| 测试要点 | 1、App在向第三方提供个人信息前，未向用户明示授权同意或进行匿 名化处理，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策中是否说明使用的第三方SDK  2、个人信息保护政策是否说明第三方SDK收集的个人信息  3、个人信息是否明文传输  4、个人信息保护政策中是否说明对外共享、转让、公开披露个人信息的规则 |
| 备注 |  |

### 向接入的第三方应用提供个人信息前是否经用户同意

|  |  |
| --- | --- |
| 评估点 | 向接入的第三方应用提供个人信息前是否经用户同意 |
| 评估结果 | 未评估 |
| 举证信息 |  |
| 整改建议 | 1、建议向接入的第三方应用提供收集使用的个人信息内容前， 征得用户同意。 |
| 评估标准 | a) 如App接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息；当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。  b) App运营者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，明确标识相关业务功能为第三方提供，并提醒用户关注第三方应用收集使用个人信息的规则。  注：第三方接入管理相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》9.7 节。 |
| 测试位置 | 隐私协议&运行态检查 |
| 测试要点 | 1、隐私政策中未明示向第三方提供个人信息，App中第三方收集个人信息是否与隐私政策中描述不一致，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策中是否说明使用的第三方SDK  2、个人信息保护政策是否说明第三方SDK收集的个人信息  3、验证App中第三方收集个人信息范围是否超过隐私政策内容 |
| 备注 |  |

## 未按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息

### 是否提供有效的注销用户账号功能

|  |  |
| --- | --- |
| 评估点 | 是否提供有效的注销用户账号功能 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改  2、参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | a) 提供有效的注销账号途径，并在用户注销账号后，及时删除其个人信息或进行匿名化处理。  注：例如可提供在线操作、客服电话、电子邮件等注销账号的途径。"  b) 受理注销账号请求后，App运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。  c) 注销账号的过程简单易操作，不设置不必要或不合理的注销条件。  注：不必要或不合理的注销条件相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》8.5 节。 |
| 测试位置 | 隐私协议&运行态检查 |
| 测试要点 | 1、App中未提供更正、删除个人信息及注销账号的功能，此项视为不符要求。  2、在进行更正、删除个人信息及注销账号时，设置不必要、不合理的条件，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策中是否说明个人信息的更正、删除规则  2、个人信息保护政策中是否说明注销用户账号规则  3、在APP实际功能是否提供个人信息更正、删除功能  4、在APP实际功能是否提供注销用户账号的功能  5、在更正、删除、注销账号时，要求提供与此无关的个人信息收集 6、提供无效的账号注销渠道 |
| 备注 |  |

### 是否提供有效的更正或删除个人信息

|  |  |
| --- | --- |
| 评估点 | 是否提供有效的更正或删除个人信息 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改  2、参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | a) 提供有效的查询、更正、删除个人信息的途径。  注：隐私政策中注明的，经证实无法完成相关操作的，视为无效途径。  b) 无法通过在线操作方式及时响应个人信息查询、更正、删除请求的，在承诺时限内（承诺时限不超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。  c) 查询、更正和删除个人信息的过程应简单易操作，不设置不必要或不合理的条件。  d) 用户更正、删除个人信息等操作完成时，App后台应同步执行完成相关操作。 |
| 测试位置 | 隐私协议&运行态检查 |
| 测试要点 | 1、在进行更正、删除个人信息及注销账号后，未在15个工作日内完成 响应用户操作内容，此项视为不符要求。  2、在进行更正、删除个人信息及注销账号后，再次进行自动填充数 据，此项视为不符要求。 |
| 测试方法 | 1、对账号进行更正、删除、注销，检查是否在15个工作日内完成账号的 更正、删除、注销  2、检查个人信息保护政策中是否描述更正、删除、注销等功能  3、对账号进行注销，再次注册，查看账号信息是否自动填充，未进行删除、 匿名化 |
| 备注 |  |

### 是否建立并公布个人信息安全投诉、举报渠道

|  |  |
| --- | --- |
| 评估点 | 是否建立并公布个人信息安全投诉、举报渠道 |
| 评估结果 | 合规/不合规 |
| 举证信息 |  |
| 整改建议 | 1、参考《协议规范\_417（公司隐私合规规范）》修改  2、参考《公司-用户个人信息保护政策模板（清洁版）0924》版本修改 |
| 评估标准 | a) 建立并公布可受理个人信息安全问题相关的投诉、举报渠道。  注：例如可采取电子邮件、电话、在线客服、在线表单、即时通讯账号等受理方式。"  b) 妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理。 |
| 测试位置 | 隐私协议&运行态检查 |
| 测试要点 | 1、App中未提供安全投诉、举报渠道  2、隐私政策中未提供安全投诉、举报方法、途径  3、未在15个工作日内受理并处理，此项视为不符要求。 |
| 测试方法 | 1、个人信息保护政策中是否建立安全投诉、举报渠道  2、实际使用APP，进行投诉、举报，查看APP是否在15个工作日之内 进行反馈处理 |
| 备注 |  |

**附件一：Android涉及个人信息权限**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **权限分组** | **权限名** | **功能描述** | **涉及个人信息** | **备注** |
| 1 | CALENDAR 日历 | READ\_CALENDAR 读取日历 | 允许 App 读取用户日历数据 | 用户在日历中录入的个人日程安排等信息 | 如学习计划、旅行日程、车票预订、生日、会议安排等 |
| 2 | WRITE\_CALENDAR 编辑日历 | 允许 App 编辑用户日历数据 |
| 3 | CALL\_LOG 通话记录 | READ\_CALL\_LOG 读取通话记录 | 允许 App 读取用户的  通话记录 | 用户通话记录 | 如通话记录管理、备份与恢复，骚扰拦截、呼出电话监控等 |
| 4 | WRITE\_CALL\_LOG 编辑通话记录 | 允许 App 写入用户的  通话记录 |
| 5 | PROCESS\_OUTGOING\_CALLS 修改或查看拨号 | 允许 App 查看正在拨打的号码，或终止通  话 |
| 6 | CAMERA相机 | CAMERA 拍摄 | 允许 App 使用摄像头 | 照片或视频信息 | 如拍照、扫描二维码、条形码；录像、人脸识别、智能识图等 |
| 7 | CONTACTS 通讯录 | READ\_CONTACTS 读取通讯录 | 允许 App 读取用户通  讯录 | 通讯录 | 通过通讯录添加好友、通讯录备份与恢复、获取各类 App 注册在手机中的账户等 |
| 8 | WRITE\_CONTACTS 编辑通讯录 | 允许 App 写入用户通  讯录 |
| 9 | GET\_ACCOUNTS 获取应用账户 | 允许 App 从账户服务中获取应用账户列表 | 网络身份标识 |
| 10 | LOCATION 位置 | ACCESS\_FINE\_LOCATION 访问精准定位 | 允许 App 获取基于GPS 等的精准地理位置 | 精准地理位置信息 | 如地图导航、活动轨迹、位置记录与共享、查看附近的服务、基于位置的智能推荐等 |
| 11 | ACCESS\_COARSE\_LOCATION 访问粗略位置 | 允许 App 获取基于基站、IP 等粗略的地理位置 | 粗略地理位置信息 |
| 12 | MICROPHONE 麦克风 | RECORD\_AUDIO 录音 | 允许 App 使用麦克风录音 | 录音内容 | 如录制音视频、语音助手功能、语音通话、聊 天、语音录入文字、语音搜索等 |
| 13 | PHONE  电话 | READ\_PHONE\_STATE读取电话状态（获取设备 IMSI、IMEI号） | 授权应用可以获取设备 IMSI（国际移动用户识别码）、IMEI  （国际移动设备识别码）等设备唯一标识信息。还可以通过此权限，获取手机通话状态，如来电、响铃中、通话中等 | 设备唯一标识信息 | 进行用户常用设备的标识，可用户监测应用账户异常登录、关联用户行为 |
| 14 | READ\_PHONE\_NUMBERS 读取本机电话号码 | 允许 App 读取用户的本机电话号码 | 电话号码 |  |
| 15 | CALL\_PHONE 拨打电话 | 允许 App 直接拨打电话 | 实时通话行为 | 如在 App 内直接拨打外卖、快递、客服等电话 |
| 16 | ANSWER\_PHONE\_CALLS 接听电话 | 允许 App 接听拨打进来的电话 | 如在用户驾驶模式下直接接听来电 |
| 17 | ADD\_VOICEMAIL 添加语音邮件 | 允许 App 向系统中添  加语音邮件 | 语音邮件内容 |  |
| 18 | USE\_SIP 使用网络电话 | 允许 App 拨打/接听网络电话 | 实时网络通话  行为 | 如接听/拨打网络电话 |
| 19 | SENSORS 传感器 | BODY\_SENSORS 获取身体传感器（心率等）信息 | 允许 App 访问身体健康相关的传感器数 据，比如心率传感器数据。 | 个人健康生理信息 | 如运动/健康类App 显示心率等健康状况 |
| 20 | SMS 短信 | SEND\_SMS 发送短信 | 允许 App 发送短信 | 短信内容 | 如短信管理、备份与恢复、验证码自动填写、短信支付、垃圾短信过滤、电话号  码等特征字提取 |
| 21 | RECEIVE\_SMS 接收短信 | 允许 App 接收短信 |
| 22 | READ\_SMS 读取短信 | 允许 App 读取短信 |
| 23 | RECEIVE\_WAP\_PUSH接收 WAP 推送 | 允许 App 接收 WAP  （无线应用协议）推送信息 | WAP 推送内容 |  |
| 24 | RECEIVE\_MMS 接收彩信 | 允许 App 接收彩信 | 彩信内容 |  |
| 25 | STORAGE 存储 | READ\_EXTERNAL\_STORAGE 读取外置存储器 | 允许 App 读取外置存储器 | 存储的个人文件 | 如存储拍摄的照片和视频、下载文件、打开本地的上传文件等 |
| 26 | WRITE\_EXTERNAL\_STORAGE 写入外置存储器 | 允许 App 写入外置存储器 |
| 27 | 工信部 | GET\_TASKS，允许程序获取当前或最近运行的应用 | 允许APP获取当前或最近运行的应用 | 当前或最近运行的应用 |  |
| 28 | 工信部 | PackageManager.getInstalledPackages() | 允许APP获取当前已安装应用软件列表 | 已安装应用软件列表 |  |

**附件二：个人信息**

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表A.1给出了个人信息举例。

表A.1 个人信息举例

|  |  |
| --- | --- |
| **个人基本资料** | 个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等 |
| **个人身份信息** | 身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等 |
| **个人生物识别信息** | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| **网络身份标识信息** | 个人信息主体账号、IP 地址、个人数字证书等 |
| **个人健康生理信息** | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等 |
| **个人教育工作信息** | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等 |
| **个人财产信息** | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| **个人通信信息** | 通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等 |
| **联系人信息** | 通讯录、好友列表、群列表、电子邮件地址列表等 |
| **个人上网记录** | 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等 |
| **个人常用设备信息** | 指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM卡/IMSI信息等）等在内的描述个人常用设备基本情况的信息 |
| **个人位置信息** | 包括行踪轨迹、精准定位信息、住宿信息、经纬度等 |
| **其他信息** | 婚史、宗教信仰、性取向、未公开的违法犯罪记录等 |

**附件三：个人敏感信息**

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14岁以下（含）儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表B.1给出了个人敏感信息举例。

表B.1 个人敏感信息举例

|  |  |
| --- | --- |
| **个人财产信息** | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| **个人健康生理信息** | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等 |
| **个人生物识别信息** | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| **个人身份信息** | 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等 |
| **其他信息** | 性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等 |