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　移动互联网应用程序（App）个人信息安全测评规范

Information security technology — Personal information security measurement and evaluation specification in mobile internet applications

（征求意见稿）

（本稿完成时间：2021 年 4 月 14 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/TC 260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国网络安全审查技术与认证中心、公安部第一研究所、北京信息安全测评中心、中国电子科技集团公司第十五研究所、国家互联网应急中心、中国信息通信研究院、陕西省网络与信息安全测评中心、北京百度网讯科技有限公司、中国移动通信集团有限公司、北京梆梆安全科技有限公司、网神信息技术（北京）股份有限公司、北京指掌易科技有限公司、中国科学院信息工程研究所、国家信息技术安全研究中心、银行卡检测中心、西安交通大学、北京字节跳动科技有限公司、北京小桔科技有限公司、北京智游网安科技有限公司、启明星辰信息技术集团股份有限公司、深圳海云安网络安全技术有限公司、北京汉华飞天信安科技有限公司、OPPO广东移动通信有限公司、深圳市腾讯计算机系统有限公司、阿里巴巴（北京）软件服务有限公司、全知科技（杭州）有限责任公司、江苏通付盾科技有限公司、中国汽车工程研究院股份有限公司、浙江蚂蚁小微金融服务集团有限公司、中科锐眼（天津）科技有限公司、天津融知科技发展有限公司、每日互动股份有限公司、三六零科技集团有限公司、同盾科技有限公司、深信服科技股份有限公司、北京云测信息技术有限公司、北京明略昭辉科技有限公司、联想（北京）有限公司、青岛海尔科技有限公司、北京三快科技有限公司、中通服咨询设计研究院有限公司、中国人民银行数字货币研究所、上海钧正网络科技有限公司。

本文件主要起草人：胡影、刘行、严妍、辛建峰、韩煜、陈淑娟、许静慧、李媛、董晶晶、李海涛、赵会敏、刘海峰、林星辰、李子强、方瑞、陈湉、解伯延、王丹辉、刘健、冀乃杰、杨京、王磊、何永金、邱勤、赵蓓、任航、吕石奎、李彪、巨腾飞、刘玉岭、杜丹、吴冬宇、史大为、李霞、李博文、李宇、张文博、刘烃、范铭、王寅、王海棠、王宇晓、安潇羽、田申、黄如鑫、狄贵宝、张娜、许家乐、阚志刚、魏超、程智力、马志民、史景、赵帅、游南南、陈呈、谢朝海、彭波、雷德诚、彭根、薛涛、李腾、刘洲和、刘俊河、谭礼格、徐永太、惠华、贾雪飞、王勰思、朱通、汪德嘉、张昀球、孟啸龙、李光平、全代勇、唐承玲、李洁、王昕、赵洪宇、袁青霞、赵明、袁小梅、谭耀、方毅、董霖、柯国锋、姚一楠、宁娇、张屹、赵冉冉、姚晟连、陈志标、胡海斌、葛盈利、伊玮珑、奚望、王新泉、李汝鑫、宋探、王淼、祖岩岩、刘笑岑、杨波、刘明君、邓昊、宋玲娓、薛勇。

引　言

本文件依据《App违法违规收集使用个人信息行为认定方法》等文件要求，重点围绕GB/T 35273-2020《信息安全技术 个人信息安全规范》提出的个人信息安全要求，规定了开展App个人信息安全测评的实施过程和测评方法。其中，GB/T 35273-2020第5章至第11章的各项要求，在本文件第6章给出了相应的测评方法，每条要求对应一个测评项。本文件适用于指导第三方测评机构对App的个人信息安全进行测评，也适用于主管监管部门对App个人信息安全进行监督管理，还适用于App提供者开展个人信息安全自评时参考。

信息安全技术　移动互联网应用程序（App）个人信息安全测评规范

1　范围

本文件规定了依据 GB/T 35273—2020《信息安全技术 个人信息安全规范》开展 App 个人信息安全测评的实施过程以及对各项具体安全要求进行测评的方法。

本文件适用于指导第三方测评机构对 App 个人信息安全进行测评，也适用于主管监管部门对 App 个人信息安全进行监督管理，还适用于 App 提供者开展个人信息安全自评时参考。

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 AAAA—BBBB　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

3　术语和定义

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

3.1

移动互联网应用程序 mobile internet application

通过预装、下载等方式获取并运行在移动智能终端上，向用户提供服务的应用软件，简称 App。

3.2

移动互联网应用程序提供者 mobile internet application provider

移动互联网应用程序所有者或运营者，简称 App 提供者。

3.3

软件开发工具包 software development kit

辅助开发某一类软件的相关二进制文件、文档、范例和工具的集合，简称 SDK。

3.4

个人信息 personal information

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。

[GB/T 35273—2020，术语和定义 3.1]

注：个人信息的范围和类型参见 GB/T 35273—2020 附录 A。

3.5

个人敏感信息 personal sensitive information

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。

[GB/T 35273—2020，术语和定义 3.2]

注：个人敏感信息的范围和类型参见 GB/T 35273—2020 附录 B。

3.6

个人信息保护政策 personal information protection policy

说明 App 收集、使用、传输、存储和删除个人信息的情况，以及用户享有的相关权利等收集使用个人信息规则的文本。

注 1：个人信息保护政策应包含的内容请参见 GB/T 35273—2020 5.5。

注 2：App 提供者习惯性将个人信息保护政策命名为『隐私政策』或其他名称。

3.7

个性化展示 personalized display

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，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

[GB/T 35273—2020，术语和定义 3.16]

3.8

业务功能 business function

满足个人信息主体的具体使用需求的服务类型。

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。

[GB/T 35273—2020，术语和定义 3.17]

3.9

可收集个人信息权限 system permissions to access personal information

移动智能终端操作系统向 App 开放的，具有收集个人信息能力的系统权限，简称系统权限或权限。

[GB/T AAAA—BBBB，术语和定义 3.10]

3.10

权限申请 system permission request

向移动智能终端操作系统声明，并向用户请求授权，以获得对移动智能终端数据或能力的访问许可的过程。

[GB/T AAAA—BBBB，术语和定义 3.15]

3.11

测评对象 target of testing and evaluation

App 个人信息安全测评过程中不同测评方式作用的对象，主要涉及 App、App 服务端、相关文档资料等。

3.12

测评单元 testing and evaluation unit

对测评过程进行划分的最小独立单元，每个测评单元包括指标要求、测评对象、测评方式、测评步骤、单元判定等 5 项内容，可独立验证符合性。

4 缩略语

以下缩略语适用于本文件。

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

MAC：媒体访问控制地址（Media Access Control Address）

IDFA：广告标识符（Identifier For Advertising）

IMSI：国际移动用户识别码（International Mobile Subscriber Identity）

API：应用程序编程接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

5 测评过程

5.1 概述

App 个人信息安全测评主要针对 App、App 服务端和相关文档资料开展，测评过程包含测评准备阶段、测评实施阶段、测评结果判定阶段和测评报告编写阶段，如图 1 所示。

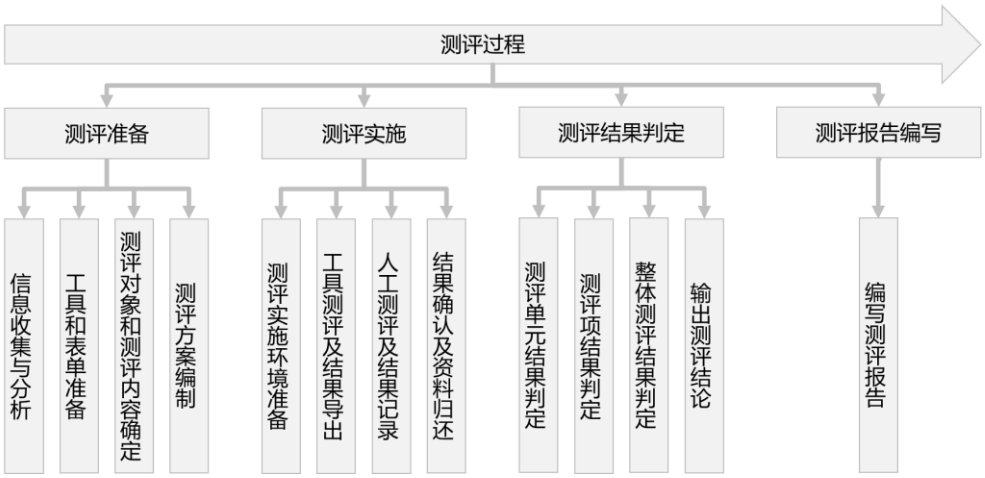

图 1 App 个人信息安全测评实施过程图

5.2 实施过程

5.2.1 测评准备

在测评准备阶段，测评人员需完成的工作主要包括：

a) App 提供者基本信息的收集与分析。测评人员应要求被测评 App 提供者提供被测 App 样本、App 功能说明、App 收集使用个人信息情况说明等材料（提交材料内容可参考附录 A）。为提高测评结果的准确性，对于有特殊登录需求的 App，测评人员宜要求被测 App 提供者提供对应登录账号；

b) 测评工具和测评表单准备。测评人员应根据 App 提供者基本信息的收集与分析，初步确定测

评工作中所使用的测评工具和测评记录表；

c) 测评对象和测评内容确定。测评人员应根据 App 提供者基本信息的收集与分析，确定测评工作的具体测评对象，例如需验证的 App 功能范围、需查看的制度文档、需核查的服务端系统、需访谈的人员岗位等；

d) 测评方案编制。测评人员应编制 App 个人信息安全测评方案，方案内容应涵盖测评对象、测评依据、测评内容、测评方法、测评工具、测评计划等。方案编制过程中，根据具体情况，测评人员可能还需要 App 提供者提供额外的信息材料或需要进行现场调研。

5.2.2 测评实施

在测评实施阶段，测评人员需完成的工作主要包括：

a) 测评实施环境准备。开始实施测评时，测评人员应进行技术检测工具的部署和调试，保障技术检测工具输出结果的可靠性；

b) 工具和人工测评及结果导出和记录。测评人员按照本文件第 6 章规定的测评方法实施测评，并将测评过程中获取的证据进行详细、准确的导出、记录；

c) 结果确认及资料归还。测评实施阶段完成时，测评人员应与被测 App 提供者确认测评实施阶段全部完成且形成了对应的测评记录，并确认测评实施阶段记录的证据的准确性。确认测评实施动作完成后，测评人员应归还被测评 App 的相关资料、移交相关权限。

5.2.3 测评结果判定

在测评结果判定阶段，测评人员对测评实施阶段所形成的证据进行分析，需完成的工作主要包括：

a) 测评单元结果判定。测评人员首先应通过证据分析，给出每一个测评单元的判定结果；

b) 测评项结果判定。测评人员根据测评单元的判定结果确定每一个测评项的判定结果；

c) 整体测评结果判定。测评人员根据测评项的判定结果确定 App 个人信息安全测评的整体结果；

d) 输出测评结论。测评人员根据整体测评结果给出 App 个人信息安全测评的结论。

5.2.4 测评报告编写

在测评报告编写阶段，测评人员根据App个人信息安全测评记录和结果判定，编制测评报告。测评报告应包括但不限于以下内容：

a) 被测评对象信息，包括 App 名称、版本号、操作系统平台、运营机构信息等；

b) 测评机构和测评人员信息，包括测评机构名称、测评人员名称等；

c) 测评环境信息，包括测评地点、测评时间、测评工具等；

d) 测评总体结论，包括测评范围、测评项总体符合情况、测评项符合率、测评是否通过等；

e) 测评项符合情况，包括每个测评项的测评过程简述、符合情况判定等。

5.3 测评方式

测评人员宜综合采用文档审查、服务端核查、功能验证、技术检测、人员访谈等测评方式，以测评App个人信息安全性。

a) 文档审查。为了分析 App 现有的或计划采取的个人信息安全保护措施，需要查看各类文档资料，包括策略文档（例如政策法规、指导性文档、组织管理制度等）、系统文档（例如用户手册、管理员手册、系统设计和需求文档、接口文档等）和个人信息安全相关文档（例如个人信息安全影响评估报告、审计报告、风险评估报告、安全测试报告、安全策略、应急预案、个人信息共享合同、个人信息处理记录等）等；

b) 服务端核查。测评人员在 App 服务端核查个人信息安全相关配置情况和个人信息处理活动，

寻找是否有违反个人信息安全策略的现象，比如个人敏感信息在显示时未进行脱敏、数据库访问未进行正确的权限设置和记录等;根据服务端核查,核实个人信息安全相关制度的落实情况；

c) 功能验证。对 App 进行操作试用，以验证其在个人信息主体权利保障方面的行为情况；功能验证主要依据 App 在运行时通过功能界面显示的信息；

d) 技术检测。技术检测是指测评人员通过 App 个人信息安全检测工具获得 App 未在功能界面显示的相关信息，并进行分析以帮助测评人员获取证据的过程；

e) 人员访谈。测评人员与被测评 App 内有关的管理、技术人员进行逐个沟通。根据对测评人员所提问题的回答，测评人员为测评获得相应信息，并可验证之前收集到的证据，从而提高其准确度和完整性。通过访谈管理和技术人员，测评人员可以收集到 App 相关的个人信息安全管理组织结构、个人信息共享、交换行为等信息，也可以了解到被访谈者的个人信息安全意识和个人信息安全技能等自身素质。

6 测评方法

6.1 个人信息的收集的测评

6.1.1 收集个人信息的合法性的测评

6.1.1.1 测评项：详见 GB/T 35273—2020 中 5.1 的 a）。

6.1.1.1.1 测评单元（PIC-01）

a) 指标要求：App 中不应存在以欺诈、诱骗、误导的方式收集个人信息的情况。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、技术检测、文档审查

d) 测评步骤：

1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求 App 不得以欺诈、诱骗、误导的方式收集个人信息；

2）查看 App 隐私政策，是否存在以欺诈、诱骗、误导的方式描述收集个人信息的行为；

3）通过功能验证、技术检测查看 App 是否存在以欺诈、诱骗、误导的方式收集个人信息的行为。

注：欺诈、诱骗、误导的行为参考附录 B 中描述。

e) 单元判定：如果 1）为肯定，2）、3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.2 测评项：详见 GB/T 35273—2020 中 5.1 的 b）。

6.1.1.2.1 测评单元（PIC-02）

a) 指标要求：App 不应隐瞒自身所具有的收集个人信息的业务功能；

b) 测评对象：App、文档资料

c) 测评方式：功能验证、技术检测、文档审查

d) 测评步骤：

1）通过对 App 隐私政策等文件中描述收集个人信息的业务功能及其对应收集的个人信息，和经功能验证、技术检测采集的 App 实际收集个人信息的业务功能和对应收集的个人信息的比较，判断 App 是否存在未说明的收集个人信息的业务功能。

e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.3 测评项：详见 GB/T 35273—2020 中 5.1 的 c）。

6.1.1.3.1 测评单元（PIC-03）

a) 指标要求：App 提供者不应从非法渠道获取个人信息；
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求不得从非法渠道获取个人信息；
   2）访谈 App 运营相关人员，询问获取个人信息的渠道是否合法；
   3）是否存在被监管部门认定为存在违法违规收集个人信息行为且未进行整改。
e) 单元判定：如果 1）、2）为肯定，3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2 收集个人信息的最小必要的测评

6.1.2.1 测评项：详见 GB/T 35273—2020 中 5.2 的 a）。

6.1.2.1.1 测评单元（PIC-04）

a) 指标要求：App 强制收集的个人信息的类型应是保障其基本服务类型正常运行最少够用的个人信息；
b) 测评对象：App
c) 测评方式：功能验证、技术检测
d) 测评步骤：
   1）通过功能验证查看 App 提供的基本服务类型，结合功能验证、技术检测查看 App 是否强制收集必要个人信息范围外的其他个人信息；
   注：服务类型正常运行最少够用的个人信息及相关要求见 GB/T AAAA—BBBB 附录 A。
   2）通过功能验证、技术检测查看 App 是否强制用户打开非必要权限。
e) 单元判定：如果 1）、2）均为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.1.2 测评单元（PIC-05）

a) 指标要求：App 收集的个人信息的类型应与实现其业务功能有直接关联；
b) 测评对象：App、文档资料
c) 测评方式：功能验证、技术检测、文档审查
d) 测评步骤：
   1）查看 App 隐私政策中描述的 App 收集的个人信息是否与业务功能有直接关联；
   2）通过功能验证、技术检测查看 App 申请的可收集个人信息的权限是否与业务功能有直接关联；
   3）通过功能验证、技术检测查看 App 实际收集的个人信息是否与业务功能有直接关联。
   注：直接关联是指没有该个人信息的参与，与之相对应的服务功能无法实现。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.2 测评项：详见 GB/T 35273—2020 中 5.2 的 b）。

6.1.2.2.1 测评单元（PIC-06）

a) 指标要求：App 自动采集个人信息的频率应是实现 App 的业务功能所必需的最低频率；
b) 测评对象：App、文档资料
c) 测评方式：技术检测、文档审查
d) 测评步骤：
1）通过技术检测查看 App 前台、后台和静默运行时自动收集个人信息的频率，结合 App 提供者提供的证明材料，判断 App 自动收集个人信息的频率是否是实现 App 的业务功能所必需的最低频率。

注 1：App 自动收集个人信息的频率可参考其调用可读取个人信息的 API 的频率或发送包含个人信息的网络数据包的频率；

注 2：不同场景下 App 采集个人信息的合理频率和相应的检测环境见附录 D。

e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.3 测评项：详见 GB/T 35273—2020 中 5.2 的 c）。

6.1.2.3.1 测评单元（PIC-07）

a) 指标要求：App 间接获取个人信息的数量应是实现 App 业务功能所必需的最少数量；
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、技术检测、文档审查、服务端核查、人员访谈
d) 测评步骤：
1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求间接获取个人信息的数量应是实现 App 业务功能所必需的最少数量；
2）通过查看 App 的隐私政策和功能验证查看 App 是否存在间接获取个人信息的行为；
3）通过功能验证、技术检测查看 App 间接获取的个人信息是否为实现 App 业务功能所必须的最少数量；
4）询问 App 提供者是否存在间接获取个人信息的行为；
5）查看在间接获取的场景下是否有获取个人信息的协议，协议中是否规定了获取个人信息的类型、数据量以及与业务功能的关联关系，据此判断 App 间接获取个人信息的数量是否是 App 业务功能所必需的最少数量。

注：App 间接获取个人信息的行为例如第三方账号登陆时获取昵称、头像，内嵌第三方购物平台时聚合展示不同第三方购物平台的订单信息等。

e) 单元判定：如果 2）、4）为否定，则本测评单位为不适用；如果 1）、3）、5）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3 多项业务功能的自主选择的测评

6.1.3.1 测评项：详见 GB/T 35273—2020 中 5.3 的 a）。

6.1.3.1.1 测评单元（PIC-08）

a) 指标要求：App 不应在安装时一次性要求授权其申请的全部权限；
b) 测评对象：App
c) 测评方式：功能验证，技术检测
d) 测评步骤：
1）针对 Android App，通过技术检测查看其 targetSdkVersion 是否小于 23；

2）通过功能验证查看 App 是否要求用户一次性授权其申请的全部权限才允许安装。

e) 单元判定：如果 1）、2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.1.2 测评单元（PIC-09）

a) 指标要求：App 不应在打开时一次性连续弹窗要求用户授权当前还未使用的业务功能所需的权限或要求用户填写当前未使用的业务功能所需的个人信息；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）通过功能验证查看 App 是否在首次打开时一次性连续弹窗要求用户授权当前还未使用的业务功能所需的权限；
   2）通过功能验证查看 App 是否在首次打开时要求用户填写当前未使用的业务功能所需的个人信息。
e) 单元判定：如果 1）、2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.1.3 测评单元（PIC-10）

a) 指标要求：用户未使用 App 某项业务功能的某项特定功能时，不应要求用户授权相应权限或要求用户填写相应的个人信息；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）通过功能验证查看 App 在进入某项业务功能时，是否要求用户授权当前未使用的特定功能所需求的权限或要求用户填写当前未使用的特定功能需要的个人信息。

   注：用户未使用 App 特定功能时要求用户授权相应权限的行为例如进入客服功能时，在未使用拍照和语音功能的情况下，要求用户授权摄像头和麦克风权限。
e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.2 测评项：详见 GB/T 35273—2020 中 5.3 的 b）。

6.1.3.2.1 测评单元（PIC-11）

a) 指标要求：App 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）通过功能验证查看 App 提供的业务功能类型，如地图导航、网络约车、网络支付等，查看用户打开 App 后是否能自主选择特定业务功能的开启，如通过主动点击、勾选、填写等方式。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.2.2 测评单元（PIC-12）

a) 指标要求：App 应仅在用户开启业务功能后，才开始收集该业务功能需要的个人信息；

b) 测评对象：App
c) 测评方式：功能验证、技术检测
d) 测评步骤：
   1）通过功能验证、技术检测查看 App 是否在用户点击同意隐私政策后才开始收集个人信息或打开可收集个人信息的权限；
   2）通过功能验证、技术检测查看 App 是否在用户开启特定业务功能后，App 才开始收集对应业务功能需要的个人信息或打开对应业务功能需要的权限。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求；否则不符合本测评单元指标要求。

6.1.3.2.3 测评单元（PIC-13）

a) 指标要求：App 在未向用户告知且未经用户同意，或无合理的使用场景时，不应频繁自启动或关联启动第三方 App 并收集个人信息；
b) 测评对象：App、文档资料
c) 测评方式：功能验证、技术检测、文档审查
d) 测评步骤：
   1）查看 App 的隐私政策中是否说明 App 具有自启动或关联启动第三方 App 并收集个人信息的行为；
   2）通过技术检测查看 App 是否存在自启动并在自启动后收集个人信息的行为；
   3）通过技术检测查看 App 在使用或静默状态是否存在关联启动第三方 App 并收集个人信息的行为；
   4）结合 App 提供者提供的证明材料，判断 App 自启动或关联启动第三方 App 并收集个人信息的行为是否合理。
e) 单元判定：如果 2）、3）为否定，则本测评单位为不适用；如果 1）、4）为肯定，则符合本测评单元指标要求；否则不符合本测评单元指标要求。

6.1.3.3 测评项：详见 GB/T 35273—2020 中 5.3 的 c）。

6.1.3.3.1 测评单元（PIC-14）

a) 指标要求：App 关闭或退出业务功能的途径或方式应与用户选择使用业务功能的途径或方式同样方便。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）通过 App 功能验证查看用户是否能自主选择关闭或退出特定业务功能，关闭或退出的途径是否便捷。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.3.2 测评单元（PIC-15）

a) 指标要求：用户选择关闭或退出特定业务功能后，App 应停止该业务功能的个人信息收集活动；
b) 测评对象：App
c) 测评方式：功能验证、技术检测
d) 测评步骤：

1）进入 App 某项业务功能，通过功能验证、技术检测查看 App 收集的个人信息。退出该业务功能，通过功能验证、技术检测查看 App 收集的个人信息。对比该业务功能关闭或退出前后 App 收集的个人信息，判断用户选择关闭或退出特定业务功能后，App 是否停止该业务功能的个人信息收集活动。

e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.4 测评项：详见 GB/T 35273—2020 中 5.3 的 d）。

6.1.3.4.1 测评单元（PIC-16）

a) 指标要求：用户不授权同意使用、关闭或退出特定业务功能的，App 不应频繁征求用户的授权同意；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
1）通过功能验证查看用户不同意某一业务功能收集非必要个人信息后，App 是否频繁询问用户同意收集该类个人信息；
2）通过功能验证查看用户不同意打开某类可收集个人信息的非必要权限后，App 是否频繁询问用户是否同意打开该类可收集个人信息权限；
3）通过功能验证查看用户退出特定业务功能后，App 是否频繁询问用户打开特定业务功能。
注：48 小时内询问 1 次以上可认定为频繁打扰。
e) 单元判定：如果 1）、2）、3）均为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.5 测评项：详见 GB/T 35273—2020 中 5.3 的 e）。

6.1.3.5.1 测评单元（PIC-17）

a) 指标要求：用户不授权同意使用、关闭或退出特定业务功能，App 不应暂停用户自主选择使用其他的业务功能，或降低其他业务功能的服务质量；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
1）通过功能验证查看用户关闭或退出特定业务功能，App 是否妨碍其他业务功能继续正常使用；
2）通过功能验证查看用户关闭或退出特定业务功能，App 是否故意设置障碍影响用户体验。
e) 单元判定：如果 1）、2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.5.2 测评单元（PIC-18）

a) 指标要求：App 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，若用户不同意，不应拒绝提供原有业务功能；
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
1）查看 App 的隐私政策，对比 App 新增业务功能申请收集的个人信息。进入 App 新增业务

功能界面，不同意新增业务功能申请收集的个人信息或打开可收集个人信息权限，查看否妨碍其他业务功能继续正常使用。

注：新增业务功能取代原有业务功能的除外。

e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.6 测评项：详见 GB/T 35273—2020 中 5.3 的 f）。

6.1.3.6.1 测评单元（PIC-19）

a) 指标要求：不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求用户同意收集个人信息；
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
   1）查看 App 的隐私政策，或通过功能验证，记录仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，要求用户同意收集的个人信息。通过功能验证，不提供仅以改善服务质量、提升使用体验、研发新产品、增强安全性为由收集的信息，查看 App 是否拒绝提供所有服务。

   注：为保障 App 基本的业务安全性，而非增强安全性而收集的个人信息，不在此项检测范围内。

e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4 收集个人信息时的授权同意的测评

6.1.4.1 测评项：详见 GB/T 35273—2020 中 5.4 的 a）。

6.1.4.1.1 测评单元（PIC-20）

a) 指标要求：App 收集个人信息，应向用户告知收集、使用个人信息的目的、方式和范围等规则，并获得用户的授权同意；
b) 测评对象：App
c) 测评方式：技术检测、功能验证
d) 测评步骤：
   1）查看 App 的个人信息保护政策，核实个人信息保护政策是否逐一列出 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、范围等规则；
   2）查看 App 基本业务功能开启前（如个人信息主体初始安装、首次使用等），是否通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将造成的影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；
   3）如 App 提供多项收集、使用个人信息的业务功能时，查看 App 除在个人信息保护政策外，是否在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其具体影响，并允许个人信息主体对扩展业务功能逐项选择同意；
   4）技术检测 App 是否在征得个人信息主体同意前就开始收集个人信息或打开可收集个人信息的权限；
   5）技术检测 App 是否在个人信息主体明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求个人信息主体同意、干扰个人信息主体正常使用；

6）技术检测 App 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个人信息主体授权范围；

7）技术检测 App 是否未经个人信息主体同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将个人信息主体设置的权限恢复到默认状态。

e) 单元判定：如果 1）、2）、3）为肯定且 4）至 7）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.2 测评项：详见 GB/T 35273—2020 中 5.4 的 b）。

6.1.4.2.1 测评单元（PIC-21）

a) 指标要求：App 收集个人敏感信息前，应征得用户的明示同意，并应确保用户的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1）查看 App 的个人信息保护政策，了解收集个人敏感信息场景和类型，确认个人信息保护政策中是否对需要收集的个人敏感信息进行了明确标识或突出显示；

2）进入 App 功能界面，验证 App 在收集用户身份证号、银行账号、行踪轨迹等个人敏感信息前，是否通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式）向个人信息主体明确告知收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其具体影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

3）查看 App 在申请打开可收集个人敏感信息的权限时，是否同步告知用户其目的，且目的说明清晰明确。

注：收集用户实名信息时仅说明用于实名制认证，收集地理位置信息时仅说明用于基于地理位置的相关服务，申请存储权限时仅说明用于改进用户体验等可认为属于说明不清晰的情况。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.3 测评项：详见 GB/T 35273—2020 中 5.4 的 c）。

6.1.4.3.1 测评单元（PIC-22）

a) 指标要求：App 收集个人生物识别信息前，应单独向用户告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得用户的明示同意；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1）查看 App 的个人信息保护政策，了解收集个人生物识别信息的场景和类型，确认个人信息保护政策中是否对需要收集的个人生物识别信息进行了明确标识或突出显示；

2）进入 App 功能界面，验证 App 在收集个人生物识别信息前，是否通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式）向个人信息主体明确告知收集、使用该个人生物识别信息的目的、方式和范围以及存储时间等规则，以便个人信息主体在作出具体的授权同意前，能充分考虑对其具体影响，并通过个人信息主体对生物识别信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意。

e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.4 测评项：详见 GB/T 35273—2020 中 5.4 的 d）。

6.1.4.4.1 测评单元（PIC-23）

a) 指标要求：App 收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；
b) 测评对象：App
c) 测评方式：功能验证、人员访谈
d) 测评步骤：
   1）查看 App 的个人信息保护政策中是否告知了征得未成年人监护人同意的机制；
   2）如果 App 中存在设定生日、年龄等相关功能，设置年龄为 14 周岁以下，查看 App 是否有相应机制征得监护人的明示同意；
   3）询问 App 提供者在收集年满 14 周岁的未成年人的个人信息前，是否具备相应措施去征得未成年人或其监护人的明示同意。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5 测评项：详见 GB/T 35273—2020 中 5.4 的 e）。

6.1.4.5.1 测评单元（PIC-24）

a) 指标要求：App 提供者间接获取个人信息时，应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；
b) 测评对象：文档资料
c) 测评方式：人员访谈、文档审查
d) 测评步骤：
   1）访谈 App 提供者相关人员，确认 App 提供者是否通过间接渠道获取个人信息；
   2）查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议保障个人信息来源的合法性；
   3）询问 App 提供者间接获取的个人信息的类型以及来源，是否对其来源的合法性进行确认。
e) 单元判定：如果 1）为否定，则本测评单位为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5.2 测评单元（PIC-25）

a) 指标要求：App 提供者间接获取个人信息时，应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露、删除等；
b) 测评对象：文档资料
c) 测评方式：人员访谈、文档审查
d) 测评步骤：
   1）访谈 App 提供者相关人员，确认 App 提供者是否通过间接渠道获取个人信息；
   2）查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议明确提供方已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露、删除等；

3）询问 App 提供者是否了解已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露等；

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5.3 测评单元（PIC-26）

a) 指标要求：App 间接获取个人信息时，如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得用户的明示同意，或通过个人信息提供方征得用户的明示同意；
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、文档审查、服务端核查、人员访谈
d) 测评步骤：
1）查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议明确提供方已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露、删除等；
2）询问 App 提供者是否了解已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露等；
3）通过询问 App 提供者或服务端核查，查看 App 提供者开展业务需进行的个人信息处理活动是否超出该授权同意范围；
4）通过功能验证查看 App 是否对超出范围部分征得用户的明示同意。
e) 单元判定：如果 3）为否定，则本测评单元不适用。如果 3）为肯定，且 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5 个人信息保护政策的测评

6.1.5.1 测评项：详见 GB/T 35273—2020 中 5.5 的 a）。

6.1.5.1.1 测评单元（PIC-27）

a) 指标要求：应制定个人信息保护政策，个人信息保护政策内容应满足 GB/T 35273—2020 中 5.5 的 a）的要求；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
1）通过功能验证查看 App 的个人信息保护政策是否包括了相应内容并记录相应结果是否满足 GB/T 35273—2020 中 5.5 的 a）的要求。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.2 测评项：详见 GB/T 35273—2020 中 5.5 的 b）。

6.1.5.2.1 测评单元（PIC-28）

a) 指标要求：App 的个人信息保护政策所告知的信息应真实、准确、完整；
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、技术检测、服务端核查、人员访谈
d) 测评步骤：
1）查看 App 的个人信息保护政策披露的个人信息控制者的基本情况，包括主体身份、联系

方式，通过工商信息查询、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

2）技术检测 App 的业务功能及其收集个人信息的行为，验证 App 的业务功能以及各业务功能分别收集的个人信息类型是否与个人信息保护政策告知的信息相符；

3）技术检测 App 的个人信息收集方式，验证 App 的个人信息收集方式是否与个人信息保护政策披露的个人信息收集方式相符；

4）查看 App 的个人信息保护政策披露的个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法等，通过操作 App 相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

5）查看 App 的个人信息保护政策披露的处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式，通过操作 App 相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

6）通过人员访谈和服务端核查验证个人信息保护政策对个人信息存储期限的告知是否真实、准确、完整；

7）通过人员访谈和服务端核查验证个人信息保护政策对个人信息的共享、转让、公开披露行为的告知是否真实、准确、完整；

8）通过人员访谈和服务端核查验证个人信息保护政策对个人信息安全防护措施的告知是否真实、准确、完整。

e) 单元判定：如果 1）至 8）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.3 测评项：详见 GB/T 35273—2020 中 5.5 的 c）。

6.1.5.3.1 测评单元（PIC-29）

a) 指标要求：App 的个人信息保护政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1）查看 App 是否提供简体中文版个人信息保护政策；

2）查看 App 个人信息保护政策的字体大小、颜色、排版是否易于阅读；

3）查看 App 个人信息保护政策语言是否通顺且易于理解，不存在概念混淆、逻辑混乱、冗长繁琐等；

4）查看 App 个人信息保护政策是否存在错别字，错别字是否造成理解上的歧义。

e) 单元判定：如果 1）、2）、3）为肯定且 4）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.4 测评项：详见 GB/T 35273—2020 中 5.5 的 d）。

6.1.5.4.1 测评单元（PIC-30）

a) 指标要求：App 个人信息保护政策应公开发布且易于访问；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：
   1）查看 App 首次运行时是否通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；
   2）进入注册及登录页面（若有注册、登录功能），查看是否具有个人信息保护政策或个人信息保护政策有效链接；
   3）查看 App 运行并进入主界面后，是否通过 4 次及以下点击等操作能访问到个人信息保护政策。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.5 测评项：详见 GB/T 35273—2020 中 5.5 的 e）。

6.1.5.5.1 测评单元（PIC-31）

a) 指标要求：App 个人信息保护政策应逐一送达用户；当成本过高或有显著困难时，可以公告的形式发布；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）查看 App 中是否可以找到被测 App 提供的个人信息保护政策；
   2）若在 App 中未找到个人信息保护政策，则判断是否存在逐一送达个人信息保护政策时成本过高或有显著困难的情况，例如当 App 不存在用户交互界面时，此种情况下，查看 App 提供者是否在其官方网站公开发布个人信息保护政策。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.6 测评项：详见 GB/T 35273—2020 中 5.5 的 f）。

6.1.5.6.1 测评单元（PIC-32）

a) 指标要求：App 提供者在个人信息保护政策所载事项发生变化时，应及时更新个人信息保护政策并重新告知用户；
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、服务端核查、人员访谈
d) 测评步骤：
   1）查看个人信息保护政策是否标注了更新日期；
   2）根据测评单元 PIC-28 的符合情况，查看 App 是否存在个人信息保护政策所载事项发生变化时，未及时更新个人信息保护政策的情况；
   3）若个人信息保护政策更新过，查看 App 是否向用户明示了更新后的个人信息保护政策并告知了个人信息保护政策的更新情况。
   4）询问 App 提供者是否有在个人信息保护政策更新后，重新告知用户的机制。
e) 单元判定：如果 2）为否定且 1）、3）、4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.6 征得授权同意的例外的测评

6.1.6.1 测评项：详见 GB/T 35273—2020 中的 5.6。

6.1.6.1.1 测评单元（PIC-33）

a) 指标要求：个人信息控制者收集、使用个人信息不必征得用户的授权同意的情形，应满足 GB/T 35273—2020 中 5.6 的要求；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1）查看个人信息保护政策是否告知了“征得授权同意的例外”；
   2）查看“征得授权同意的例外”中是否包含不合理的例外情形。
e) 单元判定：如果 1）为肯定且 2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2 个人信息的存储的测评

6.2.1 个人信息存储时间最小化的测评

6.2.1.1 测评项：详见 GB/T 35273—2020 中 6.1 的 a）。

6.2.1.1.1 测评单元（PIS-01）

a) 指标要求：App 提供者保存个人信息的期限应为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或者用户另行同意的除外。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者是否针对个人信息设立保存期限的相关制度，是否明确要求保存个人信息的期限为实现用户授权使用目的所需最短时间；
   2）询问 App 提供者针对各类个人信息的保存期限，包括制度中规定的、程序中设置的等，判断保存期限是否满足最短时间要求；
   3）查看 App 服务端是否有针对超期数据的甄别方式；
   4）对于超过最短保存时间的个人信息，查看 App 提供者是否能提供法律法规的另行规定或者用户另外同意的证明材料。
e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.1.2 测评项：详见 GB/T 35273—2020 中 6.1 的 b）。

6.2.1.2.1 测评单元（PIS-02）

a) 指标要求：超出个人信息保存期限后，应对个人信息进行删除或匿名化处理。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者是否有针对超期数据进行处理的相关制度；
   2）询问并查看 App 提供者是否有针对已超期数据处理的技术手段；
   3）查看 App 提供者针对超期数据进行处理的日志信息，是否对超期数据进行了处理；
   4）查看删除或匿名化处理数据的结果是否达到制度的要求。
e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标

要求。

6.2.2 去标识化处理的测评

6.2.2.1 测评项：详见 GB/T 35273—2020 中的 6.2。

6.2.2.1.1 测评单元（PIS-03）

a) 指标要求：收集个人信息后，App 提供者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的信息与可用于恢复识别个人的信息分开存储并加强访问与使用权限管理。
b) 测评对象：App 服务端
c) 测评方式：服务端核查
d) 测评步骤：
   1）查看 App 服务端是否在收集个人信息后，立即进行去标识处理。
   2）询问并查看 App 提供者是否有相关的管理制度，规定收集个人信息后将去标识化后的信息与可用于恢复识别个人的信息分开存储，可用于恢复识别个人的信息在访问权限、审批流程、日志记录、安全审计等方面是否有更严格的规定；
   3）查看 App 服务端，验证去标识化后的信息与可用于恢复识别个人的信息是否分开存储；
   4）查看 App 服务端，验证可用于恢复识别个人的信息的访问和使用权限相关的审批流程、日志记录、安全审计方面是否有效。
e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3 个人敏感信息的传输和存储的测评

6.2.3.1 测评项：详见 GB/T 35273—2020 中 6.3 的 a）。

6.2.3.1.1 测评单元（PIS-04）

a) 指标要求：传输和存储个人敏感信息时，应采用加密等安全措施。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：技术检测、服务端核查、文档审查
d) 测评步骤：
   1）查看 App 的设计文档，在传输和存储个人敏感信息时是否采用加密等安全措施；
   2）采用技术手段检测 App，是否以明文形式通过网络传输用户个人敏感信息；
   3）采用技术手段检测 App，是否以明文形式将个人敏感信息存储在用户终端中；
   4）查看 App 服务端是否以明文形式存储个人敏感信息。
e) 单元判定：如果 2）、3）、4）均为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3.2 测评项：详见 GB/T 35273—2020 中 6.3 的 b）。

6.2.3.2.1 测评单元（PIS-05）

a) 指标要求：App 收集个人生物识别信息的，应将其与收集的个人身份信息分开存储。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：服务端核查、人员访谈
d) 测评步骤：

1）查看 App 提供者的个人信息安全相关管理制度或 App 设计文档是否明确将收集的个人生物识别信息与个人身份信息分开存储；
2）采用技术手段检测 App 本地是否将收集的个人生物识别信息与个人身份信息分开存储；
3）查看 App 服务端，是否将收集的个人生物识别信息与个人身份信息分开存储。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3.3 测评项：详见 GB/T 35273—2020 中 6.3 的 c）。

6.2.3.3.1 测评单元（PIS-06）

a) 指标要求：App 应采取恰当措施以避免存储原始个人生物识别信息。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：技术检测、服务端核查、文档审查
d) 测评步骤：
1）查看 App 提供者的个人信息安全相关管理制度或 App 设计文档是否明确不存储个人生物识别信息的原始信息；
2）通过技术手段检测 App 是否通过网络传输个人生物识别信息的原始信息；
3）通过技术手段检测 App 是否将个人生物识别信息的原始信息存储在用户终端中；
4）查看 App 服务端是否存储个人生物识别信息的原始信息。

注 1：可采取的措施包括但不限于：仅存储不可逆的个人生物识别信息的摘要信息；在用户终端中完成身份识别、认证等功能；身份识别、认证完成后删除可提取个人生物识别信息的原始图像。

注 2：App 提供者履行法律法规规定的义务相关的情形除外。

e) 单元判定：如果 1）为肯定且 2）、3）、4）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4 个人信息控制者停止运营的测评

6.2.4.1 测评项：详见 GB/T 35273—2020 中 6.4 的 a）。

6.2.4.1.1 测评单元（PIS-07）

a) 指标要求：App 提供者应确保停止运营后及时停止继续收集个人信息的活动，并有相应机制保障实施。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求停止运营产品或服务后及时停止继续收集个人信息的活动；
2）询问 App 提供者是否存在停止运营产品或服务的情况；
3）如果存在停止运营产品或服务的情况，询问是否及时停止继续收集个人信息，查看 App 服务端确保停止继续收集个人信息的机制和相关记录。

注：例如停止某服务后，是否移除仅供该服务使用的收集个人信息的代码。

e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，如果 1）为肯定且 2）为否定，也符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4.2 测评项：详见 GB/T 35273—2020 中 6.4 的 b）。

6.2.4.2.1 测评单元（PIS-08）

a) 指标要求：App 提供者应明确要求在停止运营其产品或服务时，将停止运营的通知以逐一送达或公告的形式通知用户，并有相应机制保障实施。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）查看相关管理制度，是否明确要求在停止运营其产品或服务时，将停止运营的通知以逐一送达或公告的形式通知用户；
   2）询问 App 提供者是否存在停止运营产品或服务的情况；
   3）如果存在停止运营产品或服务的情况，询问是否将停止运营的通知以逐一送达或公告的形式通知用户，查看 App 服务端发送通知的实现机制和相关记录。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，如果 1）为肯定且 2）为否定，也符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4.3 测评项：详见 GB/T 35273—2020 中 6.4 的 c）。

6.2.4.3.1 测评单元（PIS-09）

a) 指标要求：App 提供者应明确要求在停止运营其产品或服务时，对其所持有的个人信息进行删除或匿名化处理，并有相应机制保障实施。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）查看相关管理制度，是否明确要求在停止运营其产品或服务时，对其所持有的个人信息进行删除或匿名化处理；
   2）询问 App 提供者是否存在停止运营产品或服务的情况；
   3）如果存在停止运营产品或服务的情况，询问是否对其所持有的个人信息进行删除或匿名化处理，查看 App 服务端相应的实现机制和相关记录；
   4）查看删除或匿名化处理结果是否符合相关要求。
e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，如果 1）为肯定且 2）为否定，也符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3 个人信息的使用的测评

6.3.1 个人信息访问控制措施的测评

6.3.1.1 测评项：详见 GB/T 35273—2020 中 7.1 的 a）。

6.3.1.1.1 测评单元（UPI-01）

a) 指标要求：App 提供者应对被授权访问个人信息的人员，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个人信息，且仅具备完成职责所需的最少的数据操作权限。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查
d) 测评步骤：

1） 查看App提供者的个人信息安全相关管理制度，是否建立访问控制策略，访问控制策略是否体现最少授权原则，如各类角色仅能访问职责所需的最少够用的个人信息；是否建立个人信息访问授权审批流程；
2） 服务端核查App服务端是否符合个人信息访问控制策略要求，例如不同权限的账号所能访问的个人信息类型、相关API接口等是否满足最小授权机制；App服务端的角色账号访问和操作个人信息是否经过授权审批；
3） 核查是否存在相应的记录，如：针对个人信息访问权限和时效进行审批的记录、App服务端的角色定义和账号分配进行审批的记录。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.2 测评项：详见 GB/T 35273—2020 中 7.1 的 b）。

6.3.1.2.1 测评单元（UIP-02）

a) 指标要求：App 提供者应对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查
d) 测评步骤：
1） 查看App提供者的个人信息安全相关管理制度是否明确了各类个人信息的重要操作范围；是否针对个人信息重要操作定义了内部审批流程，审批流程是否覆盖所有定义的个人信息重要操作范围；
2） 核查App服务端的账号角色执行个人信息重要操作时是否符合审批流程要求；
3） 核查是否存在相应的个人信息重要操作审批记录，App 服务端的重要操作是否有日志留存。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.3 测评项：详见 GB/T 35273—2020 中 7.1 的 c）。

6.3.1.3.1 测评单元（UPI-03）

a) 指标要求：App 提供者应对安全管理人员、数据操作人员、审计人员的角色进行分离设置。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查
d) 测评步骤：
1） 查看相关管理制度是否明确定义了安全管理人员、数据操作人员、审计人员各类角色的岗位职责，是否对各类角色的岗位分离有明确要求；
2） 核查实际岗位人员职责是否与管理制度一致，是否进行了岗位分离；
3） 核查App服务端账号角色是否覆盖安全管理人员、数据操作人员、审计人员，各类角色是否相互独立，是否不存在同一账号配置多个角色的情况。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.4 测评项：详见 GB/T 35273—2020 中 7.1 的 d）。

6.3.1.4.1 测评单元（UPI-04）

a) 指标要求：App 提供者确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评步骤：
   1） 查看App提供者的个人信息安全相关管理制度是否明确超权限处理个人信息的规定或流程设置，是否明确由个人信息保护责任人或个人信息保护工作机构对超权限处理个人信息进行审批；
   2） 核查App提供者是否由个人信息保护责任人或个人信息保护工作机构对超权限处理个人信息进行审批；
   3） 核查App提供者针对超权限处理个人信息是否存在相应的记录。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。如果 App 提供者的相关管理制度规定不允许出现超权限处理个人信息的情形，则本测评单元为不适用。

6.3.1.5 测评项：详见 GB/T 35273—2020 中 7.1 的 e）。

6.3.1.5.1 测评单元（UPI-05）

a) 指标要求：对于访问、修改个人敏感信息等操作行为，App 提供者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。
b) 测评对象：App 服务端
c) 测评方式：服务端核查
d) 测评步骤：
   1） 核查App服务端是否具备相应机制实现按照业务流程的需求触发操作授权。
   注：例如当收到客户投诉时，投诉处理人员才可访问该个人信息主体的相关信息。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.2 个人信息的展示限制的测评

6.3.2.1 测评项：详见 GB/T 35273—2020 中的 7.2。

6.3.2.1.1 测评单元（UPI-06）

a) 指标要求：涉及通过界面展示个人信息的，App 提供者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。
   1） App提供者应明确存在展示个人信息的系统范围（如App的个人设置功能界面、App服务端的客服系统等）；
   2） App提供者应明确定义各类型和各级别个人信息的展示对象范围（如内部人员、个人信息主体）；
   3） App提供者应明确定义在各系统进行个人信息展示的安全管控要求，如去标识等。
b) 测评对象：文档资料、App、App 服务端
c) 测评方式：文档审查、功能验证、服务端核查
d) 测评步骤：

1） 查看App提供者的个人信息安全相关管理制度或设计文档中是否明确了各类各级个人信息在进行展示时的安全管理要求，如去标识化等；
2） 通过功能验证查看App中涉及个人信息展示的界面在展示个人信息时是否按管理要求对个人信息进行了去标识化处理等措施；
3） 通过服务端核查查看App服务端中涉及个人信息展示的界面在展示个人信息时是否按管理要求对个人信息进行了去标识化处理等措施。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3 个人信息使用的目的限制的测评

6.3.3.1 测评项：详见 GB/T 35273—2020 中 7.3 的 a）。

6.3.3.1.1 测评单元（UPI-07）

a) 指标要求：App 提供者使用个人信息时，不应超出与收集个人信息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个人信息的，应再次征得个人信息主体明示同意。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
1） 查看App提供者的个人信息安全相关管理制度是否要求收集使用个人信息应征求个人信息主体的明示同意；是否要求超出征求同意范围收集使用个人信息的，应再次征得个人信息主体明示同意；
2） 通过功能验证查看App的个人信息保护政策说明的个人信息收集使用目的，服务端核查App提供者使用个人信息时，是否超出与收集个人信息时所声称的目的具有直接或合理关联的范围；
3） 服务端核查App提供者因业务需要，确需超出征求同意范围使用个人信息时，是否存在再次征得个人信息主体明示同意的机制；
4） 核查App提供者是否存在超出征求同意范围使用个人信息的历史行为，是否为此再次征得个人信息主体的明示同意。
e) 单元判定：如果 1）、3）、4）为肯定且 2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3.2 测评项：详见 GB/T 35273—2020 中 7.3 的 b）。

6.3.3.2.1 测评单元（UPI-08）

a) 指标要求：App 提供者对收集的个人信息进行加工处理而产生的信息，能够单独或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，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、人员访谈、服务端核查
d) 测评步骤：
1） 查看App提供者处理个人信息活动环节中是否对加工处理产生的，能够单独或与其他信息结合识别特定自然人身份或反映特定自然人活动情况的个人信息，提供对应的管理制度、处理策略及相应技术措施；

2） 服务端核查个人信息加工处理的情况，产生的信息是否能够单独或与其他信息结合识别特定自然人身份或反映自然人活动情况；
3） 服务端核查针对加工处理后产生的个人信息的管理和使用等是否符合收集个人信息时获得的授权同意范围。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，如果 2）不存在个人信息加工处理后产生的信息能够被认定为个人信息的情况，则判定为不适用；否则不符合本测评单元指标要求。

6.3.4 用户画像的使用限制的测评

6.3.4.1 测评项：详见 GB/T 35273—2020 中 7.4 的 a）。

6.3.4.1.1 测评单元（UPI-09）

a) 指标要求：App 提供者不应对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查、人员访谈
d) 测评步骤：
1） 查看App提供者的个人信息安全管理制度中是否禁止对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述；
2） 询问相关管理人员、技术人员、产品经理，了解用户画像的分析活动中，是否禁止对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述；
3） 检查App端的用户标签管理页面（若有）中对用户标签的类型、列表与配置规则，是否包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容；
4） 检查包含用户标签管理的App服务端（若有）中对用户标签的类型、列表与配置规则，是否包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容。
e) 单元判定：如果 1）、2）为肯定且 3）、4）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4.2 测评项：详见 GB/T 35273—2020 中 7.4 的 b）。

6.3.4.2.1 测评单元（UPI-10）

a) 指标要求：App 提供者在业务运行或对外业务合作中使用用户画像时，不应侵害公民、法人、和其他组织的合法权益，不能危害国家安全，宣扬恐怖主义，宣扬民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查、人员访谈
d) 测评步骤：
1） 查看App提供者的个人信息安全相关管理制度中是否包含对用户画像的相关管理规定；
2） 通过服务端核查、人员访谈查看用户画像的使用是否涉及侵害保护公民、法人和其他组织的合法权益；

3） 通过服务端核查、人员访谈查看用户画像的使用是否危害国家安全，宣扬恐怖主义，宣扬民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序等内容。

e) 单元判定：如果1）为肯定且2）、3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4.3 测评项：详见GB/T 35273—2020中7.4的c）。

6.3.4.3.1 测评单元（UPI-11）

a) 指标要求：App提供者除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。
b) 测评对象：文档资料、App服务端
c) 测评方式：文档审查、服务端核查
d) 测评步骤：
1） 查看管理制度中是否包含对用户画像使用的相关管理规定，是否明确除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人；
2） 核查App服务端功能或日志，检查用户画像的使用情况，确认是否存在非必要场景中使用明确身份指向性信息进行精确画像的情况，例如生成用于推送广告的人物画像中不应使用可识别个人的信息；
e) 单元判定：如果1）为肯定且2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5 个性化展示的使用的测评

6.3.5.1 测评项：详见GB/T 35273—2020中7.5的a）。

6.3.5.1.1 测评单元（UPI-12）

a) 指标要求：App提供者在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
1） 通过功能验证查看App是否向个人信息主体同时提供包含个性化展示和非个性化展示的业务功能；
2） 当App提供的业务功能使用个性化展示时，检查App是否通过标注“定推、推荐、关注、猜你喜欢”等字样显著区分个性化展示和非个性化展示的内容；
3） 当App提供的业务功能使用个性化展示时，查看App是否通过不同的栏目、板块、页面等显著区分个性化展示和非个性化展示内容；
4） 当App提供的业务功能使用个性化展示时，查看App是否通过其他显著方式区分个性化展示和非个性化展示内容；
5） 通过功能验证查看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。
e) 单元判定：App不涉及个性化展示服务时，本测评单元为不适用；如果1）、5）为肯定，并且2）、3）、4）其中任一项为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标

要求。

6.3.5.2 测评项：详见 GB/T 35273—2020 中 7.5 的 b）。

6.3.5.2.1 测评单元（UPI-13）

a) 指标要求：App 提供者向个人信息主体提供电子商务服务的过程中，根据用户的兴趣爱好，消费习惯等特征向用户提供商品或者服务搜索结果的个性化展示的，应当同时向该用户提供不针对其个人特征的选项。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1） 通过功能验证查看App提供者是否向个人信息主体提供电子商务服务；
   2） 当App提供者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示时，检查是否同时对该消费者提供不针对其个人特征的选项。

   注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5.3 测评项：详见 GB/T 35273—2020 中 7.5 的 c）。

6.3.5.3.1 测评单元（UPI-14）

a) 指标要求：App 提供者向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；当个人信息主体选择退出或关闭个性化展示模式时，应向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、服务端核查、人员访谈
d) 测评步骤：
   1） 通过功能验证查看App是否在向个人信息主体推送新闻信息服务过程中使用个性化展示；
   2） 通过功能验证查看App向个人信息主体推送新闻信息服务过程中使用个性化展示时，是否提供简单直观的退出或关闭个性化展示模式的选项；
   3） 通过核查App服务端、访谈相关技术人员，当个人信息主体选择退出或关闭个性化展示模式时，在App服务端是否提供删除或匿名化定向推送活动所基于的个人信息的选项。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5.4 测评项：详见 GB/T 35273—2020 中 7.5 的 d）。

6.3.5.4.1 测评单元（UPI-15）

a) 指标要求：App 提供者在使用个性化展示时，宜建立个人信息主体对个性化展示所依赖的个人信息的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。
b) 测评对象：App
c) 测试方式：功能验证
d) 测评步骤：

1） 通过功能验证查看App提供业务功能的过程中是否使用个性化展示；
2） 通过功能验证查看App是否建立个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制选项；
3） 通过功能验证查看用户能否调控个性化展示模块的相关性程度。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.6 基于不同业务目的所收集个人信息的汇聚融合的测评

6.3.6.1 测评项：详见 GB/T 35273—2020 中 7.6 的 a）。

测评规范参考 6.3.3 章节。

6.3.6.2 测评项：详见 GB/T 35273—2020 中 7.6 的 b）。

6.3.6.2.1 测评单元（UPI-16）

a) 指标要求：App 提供者应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查
d) 测评步骤：
1) 服务端核查App提供者是否根据汇聚融合后个人信息所用于的目的开展个人信息安全影响评估；
2) 服务端核查App提供者是否根据个人信息安全影响评估结果采取有效的个人信息保护措施；
3) 核查App提供者开展个人信息安全影响评估及相关个人信息保护措施是否存在相应的记录。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.7 信息系统自动决策机制的使用的测评

6.3.7.1 测评项：详见 GB/T 35273—2020 中 7.7 的 a）。

6.3.7.1.1 测评单元（UPI-17）

a) 指标要求：App 提供者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
1) 通过功能验证查看App是否具备自动决策机制且能对个人信息主体权益造成显著影响；
2) 通过服务端核查，查看App服务端是否具备自动决策机制且能对个人信息主体权益造成显著影响；

3) 核查App提供者是否在规划设计阶段或首次使用前开展个人信息安全影响评估并输出评估报告；
4) 核查评估报告中说明会采取有效的保护个人信息主体的措施是否落地实施。

e) 单元判定：如果 1）、2）均为否定，则该测评单元为不适用；如果 1）或 2）为肯定且 3）、4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.7.2 测评项：详见 GB/T 35273—2020 中 7.7 的 b）。

6.3.7.2.1 测评单元（UPI-18）

a) 指标要求：App 提供者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），在使用过程中应定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
1) 通过功能验证查看App是否具备自动决策机制且能对个人信息主体权益造成显著影响；
2) 通过服务端核查，查看App服务端是否具备自动决策机制且能对个人信息主体权益造成显著影响；
3) 核查App提供者是否在制度文件中明确对于具备自动决策机制且能对个人信息主体权益造成显著影响的信息系统，使用过程中定期（至少每年一次）开展个人信息安全影响评估；
4) 服务端核查App提供者对于具备自动决策机制且能对个人信息主体权益造成显著影响的系统是否每年至少有一份个人信息安全影响评估报告；
5) 服务端核查评估报告中说明会采取有效的保护个人信息主体的措施是否落地实施。

e) 单元判定：如果 1）、2）为否定，则该测评单元为不适用；如果 1）或 2）为肯定且 3）、4）、5）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.7.3 测评项：详见 GB/T 35273—2020 中 7.7 的 c）。

6.3.7.3.1 测评单元（UPI-19）

a) 指标要求：App 提供者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。
b) 测评对象：App、App 服务端、过程文档
c) 测评方式：功能验证、服务端核查、文档审查、
d) 测评步骤：
1) 通过功能验证查看App是否具备自动决策机制且能对个人信息主体权益造成显著影响；
2) 通过服务端核查，查看App服务端是否具备自动决策机制且能对个人信息主体权益造成显著影响；
3) 通过功能验证查看App是否向个人信息主体提供针对自动决策结果的申诉渠道，并支持对自动决策结果的人工复核；
4) 核查App服务端是否向个人信息主体提供针对自动决策结果的申诉渠道，并对自动决策结果进行人工复核。

e) 单元判定：如果 1）、2）为否定，则该测评单元为不适用；如果 1）或 2）为肯定且 3）、4）

均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4 个人信息主体的权利的测评

6.4.1 个人信息查询的测评

6.4.1.1 测评项：详见 GB/T 35273—2020 中 8.1 的 a）。

6.4.1.1.1 测评单元（RPI-01）

a) 指标要求：App 应对个人信息主体提供对其所持有的关于该主体的个人信息或个人信息类型的查询功能或方式。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 通过功能验证查看App个人信息保护政策中是否向个人信息主体提供了查询其个人信息或个人信息类型的具体方式，例如客服电话、客服邮箱、个人信息保护机构或个人信息保护负责人的电话、邮箱等；
   2) 验证App个人信息保护政策中提供的查询个人信息的方式是否有效；
   3) 通过功能验证查看App功能界面中是否提供对于该主体的个人信息或个人信息类型的查询功能，例如个人信息展示页面、在线客服等；
   4) 验证App功能界面中提供的个人信息查询方式是否有效。
e) 单元判定：如果 1）、2），或 3）、4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.1.2 测评项：详见 GB/T 35273—2020 中 8.1 的 b）。

6.4.1.2.1 测评单元（RPI-02）

a) 指标要求：App 应对个人信息主体提供对其所持有的关于该主体的个人信息的来源及所用于的目的的查询功能或方式。
b) 测评对象：App
c) 测评方式：功能验证。
d) 测评步骤：
   1) 查看App个人信息保护政策中是否向个人信息主体明示了个人信息的采集方式、对应的业务功能及使用目的；
   2) 查看App功能界面中是否提供关于该主体的个人信息的来源及所用于目的的查询功能；
   3) 验证App提供的客服电话、邮箱、在线客服，个人信息保护机构或个人信息保护负责人的联系电话、邮箱等个人信息查询方式是否支持查询App提供者所持有的用户个人信息的来源及所用于的目的。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.1.3 测评项：详见 GB/T 35273—2020 中 8.1 的 c）。

6.4.1.3.1 测评单元（RPI-03）

a) 指标要求：App 应对个人信息主体提供已经获得该主体个人信息的第三方身份或类型的查询功

能或方式。

b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 查看App个人信息保护政策中是否向个人信息主体明示了对外共享、转让和披露的规则，其中是否包含可能获得该主体个人信息的第三方身份或类型；
   2) 查看App功能界面中是否提供了获取该主体个人信息的第三方身份或类型的查询功能；
   3) 验证App提供的客服电话、邮箱、在线客服，个人信息保护机构或个人信息保护负责人的联系电话、邮箱等个人信息查询方式是否支持查询已获得用户个人信息的第三方身份或类型。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.2 个人信息更正的测评

6.4.2.1 测评项：详见 GB/T 35273—2020 中的 8.2。

6.4.2.1.1 测评单元（RPI-04）

a) 指标要求：App 应为个人信息主体提供对其所持有的个人信息请求更正或补充信息的渠道或功能。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 查看App个人信息保护政策或功能界面中是否向个人信息主体提供了更正或补充其个人信息的具体途径，包括App内个人信息修改界面、App内客服渠道、联系电话、联系邮箱等；
   2) 验证所提供的个人信息更正或补充途径是否有效。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.3 个人信息删除的测评

6.4.3.1 测评项：详见 GB/T 35273—2020 中 8.3 的 a）。

6.4.3.1.1 测评单元（RPI-05）

a) 指标要求：App 违反法律法规规定，或违反与个人信息主体的约定，收集、使用个人信息的情形下，个人信息主体要求删除个人信息时，App 应提供删除功能或方式并及时删除。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查、人员访谈
d) 测评步骤：
   1) 查看App提供者的个人信息安全相关管理制度，是否明确要求在App违反法律法规规定，收集、使用个人信息，或违反与个人信息主体的约定，收集、使用个人信息的情形下，个人信息主体要求删除个人信息时，App应提供删除功能或方式并及时删除，并明确删除个人信息的流程设计、响应时间等内容；

2) 查看App个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径，并明确在App违反法律法规规定，收集、使用个人信息的情形下，及时响应个人信息主体要求删除个人信息；
3) 查看App的功能界面中是否向个人信息主体提供个人信息删除功能，并能迅速处理；
4) 询问App提供者并查看App服务端是否具备按照要求删除个人信息的相应机制；
5) 核查App声明删除个人信息后，App服务端是否存在个人信息残留。

e) 单元判定：如果 1）至 4）为肯定，5）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.3.2 测评项：详见 GB/T 35273—2020 中 8.3 的 b）。

6.4.3.2.1 测评单元（RPI-06）

a) 指标要求：App 违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除时，App 应立即停止共享、转让的行为，并通知第三方及时删除。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查、人员访谈
d) 测评步骤：
1) 查看App提供者的个人信息安全相关管理制度，是否明确要求在App违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息的情形下，个人信息主体要求删除个人信息时，立即停止共享、转让的行为，并通知第三方及时删除；
2) 查看App个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径，并明确在违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息的情形下，及时响应个人信息主体要求立即停止共享、转让的行为，并通知第三方及时删除；
3) 询问App提供者并查看App服务端是否具备停止共享、转让行为，并通知第三方及时删除的实现机制。

e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.3.3 测评项：详见 GB/T 35273—2020 中 8.3 的 c）。

6.4.3.3.1 测评单元（RPI-07）

a) 指标要求：App 提供者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除时，App 提供者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应信息。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
1) 查看App提供者的个人信息安全相关管理制度，是否明确要求在App违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息的情形下，个人信息主体要求删除个人信息时，立即停止公开披露的行为，并发布通知要求相关接收方及时删除。
2) 查看App个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径，并明确在违反法律法规规定或违反与个人信息主体的约定公开披露个人信息的情形下，及时响应个人信息主体要求立即停止公开披露的行为，并发布通知要求相关接收方及时删除；

3) 询问App提供者并查看App服务端是否具备立即停止公开披露行为，并发布通知要求相关接收方删除相应信息的机制。

e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.4 个人信息主体撤回授权同意的测评

6.4.4.1 测评项：详见 GB/T 35273—2020 中 8.4 的 a）。

6.4.4.1.1 测评单元（RPI-08）

a) 指标要求：App 应在个人信息保护政策或功能界面中告知个人信息主体撤回收集、使用个人信息的授权同意的有效途径和方式，且撤回授权同意后，个人信息控制者后续不应再处理相应的个人信息。

b) 测评对象：App、App 服务端

c) 测评方式：功能验证、技术检测、服务端核查

d) 测评步骤：

1) 查看App个人信息保护政策或功能界面中是否告知个人信息主体撤回收集、使用其个人信息的授权同意的方法，包括个人信息和权限；

2) 验证App个人信息保护政策或功能界面中撤回收集、使用其个人信息的授权同意的方法是否有效；

3) 通过技术检测验证个人信息主体撤回同意后，App是否继续收集和使用已撤回授权同意的个人信息；

4) 核查App服务端，在用户撤回同意后，App服务端是否不再处理相应的个人信息。

e) 单元判定：如果 1）、2）、4）为肯定，3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.4.2 测评项：详见 GB/T 35273—2020 中 8.4 的 b）。

6.4.4.2.1 测评单元（RPI-09）

a) 指标要求：App 应在个人信息保护政策或功能界面中提供基于个人信息推送广告的拒绝途径或关闭选项。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 查看App是否具有基于个人信息的商业广告推送行为；

2) 若App存在基于个人信息的商业广告推送行为，则查看个人信息保护政策或功能界面中是否提供基于个人信息推送广告的拒绝途径或关闭选项；

3) 验证拒绝或关闭定向广告推送后，App是否继续推送定向广告信息。

e) 单元判定：如果 1）为否定，则该单元测评项判定为不适用；如果 1）、2）为肯定，3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.4.2.2 测评单元（RPI-10）

a) 指标要求：App 应在个人信息保护政策或功能界面中向个人信息主体提供针对对外共享、转让、公开披露个人信息撤回授权同意的途径和方式。

b) 测评对象：App、App 服务端

c) 测评方式：功能验证、技术检测、服务端核查
d) 测评步骤：
   1) 通过功能验证、技术检测查看App是否存在对外共享、转让、公开披露个人信息的行为；
   2) 核查App服务端是否存在对外共享、转让、公开披露个人信息的行为；
   3) 查看App的个人信息保护政策或功能界面中是否提供撤回授权同意的途径和方式；
   4) 通过功能验证、技术检测查看用户撤回授权同意后，App是否继续对外共享、转让、公开披露个人信息的行为；
   5) 核查App服务端，在用户撤回授权同意后，是否停止对外共享、转让、公开披露其个人信息。

   注：常见的撤回对外共享授权的场景包括对第三方获取账号信息的授权、对小程序获取地理位置等权限的授权、对免密支付和自动支付等的授权等。
e) 单元判定：如果 1）、2）为否定，则本测评单元为不适用；如果 1）、3）、4）为肯定，或 2）、3）、5）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5 个人信息主体注销账户的测评

6.4.5.1 测评项：详见 GB/T 35273—2020 中 8.5 的 a）。

6.4.5.1.1 测评单元（RPI-11）

a) 指标要求：通过注册账户提供产品或服务的 App 提供者，应向个人信息主体提供注销账户的方法，且方法简便易操作。
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、服务端核查
d) 测评步骤：
   1) 通过功能验证查看App个人信息保护政策或功能界面中是否向个人信息主体提供了注销账户的途径和方式；
   2) 验证App提供的账户注销途径和方式是否可以正常执行，且易于操作；
   3) 服务端核查用户注销账户后，App服务端是否对用户的个人信息作删除或匿名化处理。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.2 测评项：详见 GB/T 35273—2020 中 8.5 的 b）。

6.4.5.2.1 测评单元（RPI-12）

a) 指标要求：App 受理账户注销请求后，需人工处理的，应在 15 个工作日内完成核查和处理。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 查看App提供者的相关管理制度，是否明确人工处理账户注销的核查和处理流程，流程是否可在15个工作日内完成；
   2) 通过功能验证查看App人工受理账户注销后，是否可在15个工作入内完成核查和处理；
   3) 核查App服务端对用户注销账号的处理机制，是否能在15个工作日内完成核查和处理。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.3 测评项：详见 GB/T 35273—2020 中 8.5 的 c）。

6.4.5.3.1 测评单元（RPI-13）

a) 指标要求：App 在账户注销时，如需进行身份核验，则所需提供的个人信息不应多于注册、使用等服务环节收集的个人信息类型。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 通过功能验证查看App在注册和使用等服务环节收集的个人信息类型；通过功能验证查看App在注销账户验证身份过程中，所需提供的个人信息是否多于注册、使用等服务环节收集的个人信息类型。
e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.4 测评项：详见 GB/T 35273—2020 中 8.5 的 d）。

6.4.5.4.1 测评单元（RPI-14）

a) 指标要求：App 不应在注销账户功能中设置不合理或不必要的额外要求。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 通过功能验证查看App在用户注销账户的流程中是否设置不合理的条件或提出额外要求增加用户义务。

   注：注销账户时的不合理条件如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等。
e) 单元判定：如果 1）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.5 测评项：详见 GB/T 35273—2020 中 8.5 的 e）。

6.4.5.5.1 测评单元（RPI-15）

a) 指标要求：App 注销账户的过程中收集了个人敏感信息，应明确对收集个人敏感信息后的处理措施。
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、服务端核查
d) 测评步骤：
   1) 通过功能验证查看App注销账户的过程中是否需要收集个人敏感信息核验身份；
   2) 通过功能验证查看App个人信息保护政策或功能界面中是否明确注销账户过程中对收集的个人敏感信息使用后的处理措施，如达成目的后立即删除或匿名化处理等；
   3) 核查App服务端是否在用户注销账户结束后，立即对所收集的个人敏感信息进行了删除或匿名化处理。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.6 测评项：详见 GB/T 35273—2020 中 8.5 的 f）。

6.4.5.6.1 测评单元（RPI-16）

a) 指标要求：App 应在个人信息主体注销操作完成后，及时删除或匿名化个人信息。因法律法规规定需要留存的个人信息，不能再次将其用于日常业务活动中。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 通过功能验证查看App个人信息保护政策中是否明确账户注销后如何处理个人信息；
   2) 核查App服务端在用户完成账户注销后，是否对用户个人信息进行删除或匿名化处理；
   3) 对于因法律法规规定需要留存的个人信息，核查App提供者提供的相关法律法规要求与实际留存的个人信息是否一致，核查是否有相应机制保障上述个人信息不再用于日常业务活动中。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本单元测评指标要求，否则不符合本测评单元指标要求。

6.4.6 个人信息主体获取个人信息副本的测评

6.4.6.1 测评项：详见 GB/T 35273—2020 中的 8.6。

6.4.6.1.1 测评单元（RPI-17）

a) 指标要求：根据个人信息主体的请求，个人信息控制者宜为个人信息主体提供获取本人的基本资料、身份信息、健康生理信息、教育工作信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方。
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
   1) 通过功能验证向App提供者提出获取本人基本资料、身份信息、健康生理信息、教育工作信息副本，核实其是否可按需求提供副本信息；
   2) 通过功能验证向App提供者提出将本人基本资料、身份信息、健康生理信息、教育工作信息副本传输给第三方，核实其是否可满足要求。
e) 单元判定：如果 1）或 2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7 响应个人信息主体的请求的测评

6.4.7.1 测评项：详见 GB/T 35273—2020 中 8.7 的 a）。

6.4.7.1.1 测评单元（RPI-18）

a) 指标要求：App 应在验证个人信息主体身份后，及时响应个人信息主体基于 GB/T 35273—2020 8.1~8.6 提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
   1) 查看App提供者的个人信息安全相关管理制度，是否明确及时响应个人信息主体基于GB/T 35273—2020 8.1~8.6提出的请求，在三十天内或法律法规规定的期限内作出答复及合理解释，并告知外部纠纷解决途径。

2) 基于GB/T 35273—2020 8.1~8.6向App提供者提出相关请求，验证其是否可在三十天内或法律法规规定的期限内作出答复及合理解释。

e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.2 测评项：详见 GB/T 35273—2020 中 8.7 的 b）。

6.4.7.2.1 测评单元（RPI-19）

a) 指标要求：App 功能界面宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；
b) 测评对象：App
c) 测评方式：功能验证
d) 测评步骤：
1) 通过功能验证查看App功能界面是否提供有效的在线访问、更正、删除、撤回授权同意、注销账户等功能。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.3 测评项：详见 GB/T 35273—2020 中 8.7 的 c）。

6.4.7.3.1 测评单元（RPI-20）

a) 指标要求：App 对合理的请求不应收取费用，但对一定时期内多次重复的请求，可视情况收取一定成本费用，同时 App 的个人信息保护政策应特别针对请求收取费用事项进行说明。
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
1) 通过功能验证查看App响应用户请求是否涉及收费项目；
2) 查看App提供者的个人信息安全相关管理制度中是否建立响应用户请求的收费机制，并对收费事项及成本费用进行说明；
3) 查看App个人信息保护政策中是否针对收取费用事项进行说明；
4) 验证App响应用户的请求收费功能是否合理以及收取的成本费用是否合理。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.4 测评项：详见 GB/T 35273—2020 中 8.8 的 d）。

6.4.7.4.1 测评单元（RPI-21）

a) 指标要求：直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，App 提供者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益。
b) 测评对象：制度文件
c) 测评方式：文档审查
d) 测评步骤：
1) 查看App提供者的个人信息安全相关管理制度中是否梳理直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的情形，提出替代方法，并在个人信息保护政策中做出相应说明。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.5 测评项：详见 GB/T 35273—2020 中 8.7 的 e）。

6.4.7.5.1 测评单元（RPI-22）

a) 指标要求：App 提供者不响应个人信息主体基于 GB/T 35273—2020 8.1~8.6 提出的请求的情形应在 GB/T 35273—2020 中 8.7 节 e）项规定范围内。
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
   1) 查看App提供者的个人信息安全相关管理制度中是否规定可不响应个人信息主体基于GB/T 35273—2020 8.1~8.6提出的请求的情形；
   2) 查看规定的情形是否在GB/T 35273—2020中8.7节e）项规定范围内；
   3) 询问并查看App提供者是否有不响应用户个人信息安全请求的记录；
   4) 查看不响应的情形是否在GB/T 35273—2020中8.7节e）项规定范围内。
e) 单元判定：如果 1）、3）为否定，或者 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.6 测评项：详见 GB/T 35273—2020 中 8.8 的 f）。

6.4.7.6.1 测评单元（RPI-23）

a) 指标要求：App 提供者如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
   1) 通过功能验证查看App是否存在不响应个人信息主体的请求的情况；
   2) 查看App提供者的个人信息安全相关管理制度中是否梳理不响应个人信息主体的请求的情形及理由，是否明确决定不响应请求时应向个人信息主体告知理由，并提供投诉的途径；
   3) 查看App个人信息保护政策中是否提供了投诉的途径；
   4) 验证投诉途径是否有效。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.8 投诉管理的测评

6.4.8.1 测评项：详见 GB/T 35273—2020 中的 8.8。

6.4.8.1.1 测评单元（RPI-24）

a) 指标要求：App 提供者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行响应。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 查看App提供者的个人信息安全相关管理制度是否建立投诉管理机制和投诉跟踪流程，并明确了投诉响应时限；
   2) 核查App服务端是否建立投诉管理机制和投诉跟踪流程；

3) 查看App个人信息保护政策或功能界面中其是否向用户提供了投诉渠道或功能；
4) 通过投诉渠道或功能就个人信息相关问题进行投诉，验证其是否在十五个工作日内进行响应。

e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5 个人信息的委托处理、共享、转让、公开披露的测评

6.5.1 委托处理的测评

6.5.1.1 测评项：详见 GB/T 35273—2020 中 9.1 的 a）。

6.5.1.1.1 测评单元（EPI-01）

a) 指标要求：App 提供者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守 GB/T 35273—2020 5.6 所列情形；
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：技术检测、服务端核查、文档审查、人员访谈
d) 测评步骤：
1） 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；
2） 查看App提供者的个人信息安全相关管理制度，是否明确规定委托行为不得超出已征得个人信息主体授权同意的范围或应遵守GB/T35273—2020 5.6所列情形；
3） 查看委托行为的相关记录，是否超出已征得个人信息主体授权同意的范围或未遵守GB/T 35273—2020 5.6所列情形。
e) 单元判定：如果 1）为否定，则本测试单元为不适用。如果 1）、2）为肯定，3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.2 测评项：详见 GB/T 35273—2020 中 9.1 的 b）。

6.5.1.2.1 测评单元（EPI-02）

a) 指标要求：App 提供者应对委托行为进行个人信息安全影响评估，确保受委托者达到 GB/T 35273—2020 11.5 节数据安全能力要求。
b) 测评对象：文档资料
c) 测评方式：人员访谈、文档审查
d) 测评步骤：
1) 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；
2) 查看App提供者的个人信息安全相关管理制度，是否明确规定对委托行为进行个人信息安全影响评估，确保受委托者达到GB/T 35273—2020 11.5节数据安全能力要求；
3) 询问App提供者是否对委托行为进行个人信息安全影响评估，并查看是否提供个人信息安全影响评估相关记录文档；
4) 查看个人信息安全影响评估记录文档，是否确保受委托者达到GB/T 35273—2020 11.5节数据安全能力要求。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评

单元指标要求，否则不符合本测评单元指标要求。

6.5.1.3 测评项：详见 GB/T 35273—2020 中 9.1 的 c）。

6.5.1.3.1 测评单元（EPI-03）

a) 指标要求：App 提供者应要求受委托者达到 GB/T 35273—2020 中 9.1 的 c）中 1）至 5）项要求。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1) 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；
   2) 询问并查看App提供者是否具有对受委托者做出安全要求的管理制度，且要求内容覆盖GB/T 35273—2020中9.1的c）中1）至5）项的要求；
   3) 询问并查看App提供者是否对委托行为签署合同等文件;
   4) 查看委托合同等文件中是否规定GB/T 35273—2020 9.1 c）所列的5条安全要求。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.4 测评项：详见 GB/T 35273—2020 中 9.1 的 d）。

6.5.1.4.1 测评单元（EPI-04）

a) 指标要求：App 提供者应对受委托者进行监督，通过合同等方式规定受委托者的责任和义务，并对受委托者进行审计。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1) 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；
   2) 查看委托合同等相关文档，是否规定了受委托者的责任和义务；
   3) 询问App提供者是否对受委托者进行审计；
   4) 查看相关审计记录是否包含对受委托者处理个人信息行为的审计情况。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.5 测评项：详见 GB/T 35273—2020 中 9.1 的 e）。

6.5.1.5.1 测评单元（EPI-05）

a) 指标要求：App 提供者应准确记录和保存委托处理个人信息的情况。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1) 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；

2) 询问并查看App提供者是否制定相关制度，明确规定委托处理个人信息时准确记录和保存相关情况；
3) 询问并查看App提供者是否记录委托处理行为以及保存委托处理行为的相关文档；
4) 查看相关文档是否包括受委托方及其联系方式、委托处理个人信息类型、委托处理个人信息数量、委托处理个人信息目的等内容。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.6 测评项：详见 GB/T 35273—2020 中 9.1 的 f）。

6.5.1.6.1 测评单元（EPI-06）

a) 指标要求：App 提供者得知或者发现受委托者未按照委托要求处理个人信息时，或未能有效履行个人信息安全保护责任时，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
1) 通过技术检测App、查看相关文档资料及询问App提供者等方式，查看App提供者是否存在委托处理行为；
2) 查看App提供者的个人信息安全相关管理制度，是否要求在得知或者发现受委托者未按照委托要求处理个人信息时，应采取行动控制或者消除个人信息面临的安全风险；
3) 询问App提供者是否曾出现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的情况；若曾出现上述情况，查看当时的处理记录，判断App提供者是否立即要求受委托方停止相关行为，且采取或要求受委托方采取有效补救措施控制或消除个人信息面临的安全风险；
4) 核查App服务端是否具备在上述情况下立即控制或消除个人信息安全风险的技术措施。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2 个人信息共享、转让的测评

6.5.2.1 测评项：详见 GB/T 35273—2020 中 9.2 的 a）。

6.5.2.1.1 测评单元（EPI-07）

a) 指标要求：App 提供者共享、转让个人信息前，应事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；
2) 查看App提供者的个人信息安全相关管理制度，是否明确个人信息共享、转让前应开展个人信息安全影响评估；
3) 查看是否有个人信息安全影响评估报告以及依据评估结果实施的保护措施的相关文档；

4) 核查App服务端、询问App提供者、查看相关的文档，判断保护措施是否有效实施。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.2 测评项：详见 GB/T 35273—2020 中 9.2 的 b）。

6.5.2.2.1 测评单元（EPI-08）

a) 指标要求：App 提供者应向用户告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。去标识化后且无法重新识别个人信息主体的信息除外。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、技术检测、服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；

2) 查看App提供者的个人信息安全相关管理制度，是否明确规定告知用户共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意；

3) 查看App的个人信息保护政策，其中是否向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并征得用户授权同意；

4) 通过技术检测App中共享给第三方的个人信息和第三方类型，判断是否与App个人信息保护政策中说明的一致；

5) 核查App服务端共享给第三方的个人信息和第三方类型，判断是否与App个人信息保护政策中说明的一致；

6) 询问App提供者是否存在向接入的第三方应用提供个人信息的行为，若存在则判断是否与App个人信息保护政策中说明的一致；

7) 询问并查看未告知的个人信息是否是经去标识化处理的个人信息。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 7）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.3 测评项：详见 GB/T 35273—2020 中 9.2 的 c）。

6.5.2.3.1 测评单元（EPI-09）

a) 指标要求：App 提供者共享、转让个人敏感信息前，除 GB/T 35273—2020 9.2 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、技术检测、服务端核查、文档审查

d) 测评步骤：

1) 通过功能验证和技术检测App，查看App是否收集个人敏感信息；

2) 技术检测App是否直接向第三方共享个人敏感信息；

3) 询问并核查App服务端是否向第三方共享、转让个人敏感信息；

4) 查看App的个人信息保护政策是否向个人信息主体告知除GB/T 35273—2020 9.2 b）中告知的内容外，涉及的个人敏感信息的类型、数据接收方的身份和数据安全能力，并通过弹窗、界面文字说明、用户主动点击同意等明示方式征得个人信息主体同意；

5) 查看App提供者的个人信息安全相关管理制度，是否明确规定共享、转让个人敏感信息应额外告知涉及的个人敏感信息的类型、数据接收方身份和数据安全能力，并事先征得个人信息主体的明示同意。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 5）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.4 测评项：详见 GB/T 35273—2020 中 9.2 的 d）。

6.5.2.4.1 测评单元（EPI-10）

a) 指标要求：App 提供者在共享、转让个人信息时，应通过合同等方式规定数据接收方的责任和义务。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评步骤：
1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；
2) 查看App提供者的数据共享、转让合同或协议，是否通过合同等方式规定数据接收方的责任和义务。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.5 测评项：详见 GB/T 35273—2020 中 9.2 的 e）。

6.5.2.5.1 测评单元（EPI-11）

a) 指标要求：App 提供者应准确记录和保存个人信息的共享、转让的情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；
2) 查看App提供者的个人信息安全相关管理制度，是否明确规定应准确记录和保存个人信息的共享、转让的情况；
3) 询问并查看个人信息的共享、转让的记录，是否包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；
4) 对于实时进行的共享行为，查看系统中是否有相应记录。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.6 测评项：详见 GB/T 35273—2020 中 9.2 的 f）。

6.5.2.6.1 测评单元（EPI-12）

a) 指标要求：App 提供者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接

收方及时删除从个人信息控制者获得的个人信息。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；

2) 查看App提供者的个人信息安全相关管理制度，是否明确发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即采取行动控制或消除个人信息面临的安全风险；

3) 询问是否曾出现数据接收方违反法律法规要求或双方约定处理个人信息的情况；若曾出现上述情况，查阅当时的处理记录，验证被评估对象是否立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施控制或消除个人信息面临的安全风险；

4) 服务端核查App提供者是否具备在上述情况下立即控制或消除个人信息安全风险的技术措施。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.7 测评项：详见 GB/T 35273—2020 中 9.2 的 g）。

6.5.2.7.1 测评单元（EPI-13）

a) 指标要求：App 提供者应承担因共享、转让个人信息对个人信息主体合法权益造成损害的相应责任。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；

2) 查阅App个人信息保护政策等相关文档是否有在对个人信息主体合法权益造成损害时承担相应责任的说明。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.8 测评项：详见 GB/T 35273—2020 中 9.2 的 h）。

6.5.2.8.1 测评单元（EPI-14）

a) 指标要求：App 提供者应帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况，以及个人信息主体的权利。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、服务端核查、文档审查

d) 测评步骤：

1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在共享、转让个人信息的行为；

2) 查看App提供者的个人信息安全相关管理制度，是否明确应帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况，以及个人信息主体的权利；

3) 通过功能验证查看App是否提供了个人信息主体了解数据接收方对个人信息的保存、使用等情况以及个人信息主体权利的途径；
4) 验证个人信息主体了解数据接收方对个人信息的保存、使用等情况以及个人信息主体权利的途径是否有效。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.9 测评项：详见 GB/T 35273—2020 中 9.2 的 i）。

6.5.2.9.1 测评单元（EPI-15）

a) 指标要求：因业务需要，App 提供者确需共享、转让个人生物识别信息的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评实施：
1) 通过功能验证查看App是否存在共享个人生物识别信息的行为；
2) 询问并核查App服务端是否存在将收集的个人生物识别信息进行共享、转让的行为；
3) 若存在上述行为，验证App是否通过弹窗告知、显著标识等方式单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。
e) 单元判定：如果 1）、2）为否定，则本测评单元为不适用；如果 1）或 2）为肯定，且 3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3 收购、兼并、重组、破产时的个人信息转让的测评

6.5.3.1 测评项：详见 GB/T 35273—2020 中 9.3 的 a）。

6.5.3.1.1 测评单元（EPI-16）

a) 指标要求：当 App 提供者发生收购、兼并、重组、破产等变更时，应向个人信息主体告知有关情况。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
1) 查看App提供者是否有收购、兼并、重组、破产时的个人信息转让的管理制度，制度中应明确向个人信息主体告知有关情况；
2) 如果存在收购、兼并、重组的情况，查阅是否有告知的相关记录。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3.2 测评项：详见 GB/T 35273—2020 中 9.3 的 b）。

6.5.3.2.1 测评单元（EPI-17）

a) 指标要求：当 App 提供者发生收购、兼并、重组、破产等变更时，变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息

主体的明示同意。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、文档审查、人员访谈

d) 测评步骤：

1) 查看App提供者是否有收购、兼并、重组、破产时的个人信息转让的管理制度；

2) 如果App提供者是变更后的个人信息控制者，询问并查看其是否继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，是否重新取得个人信息主体的明示同意。

e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3.3 测评项：详见 GB/T 35273—2020 中 9.3 的 c）。

6.5.3.3.1 测评单元（EPI-18）

a) 指标要求：App 提供者如破产且无承接方，应对数据做删除处理。

b) 测评对象：文档资料

c) 测评方式：文档审查

d) 测评步骤：

1) 查看App提供者的相关管理文档，是否明确在破产且无承接方时，对数据做删除处理。

e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4 个人信息公开披露的测评

6.5.4.1 测评项：详见 GB/T 35273—2020 中 9.4 的 a）。

6.5.4.1.1 测评单元（EPI-19）

a) 指标要求：App 提供者公开披露个人信息前，应事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施。

b) 测评对象：文档资料、App 服务端、App

c) 测评方式：文档审查、人员访谈、服务端核查、功能验证

d) 测评步骤：

1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；

2) 查看App提供者是否建立个人信息公开披露时的个人信息安全影响评估制度；

3) 查看是否有个人信息安全影响评估报告以及依据评估结果应实施的保护措施内容；

4) 通过App功能验证、核查App服务端，查看保护措施是否有效实施。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.2 测评项：详见 GB/T 35273—2020 中 9.4 的 b）。

6.5.4.2.1 测评单元（EPI-20）

a) 指标要求：App 提供者应向用户告知公开披露个人信息的目的、类型，并事先征得个人信息主体的明示同意。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、文档审查

d) 测评步骤：

1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；
2) 查看App提供者是否有个人信息公开披露的管理制度明确规定告知用户公开披露个人信息的目的、类型，并事先征得个人信息主体的明示同意；
3) 通过App功能验证，查看App个人信息保护政策或涉及公开披露个人信息的功能界面中是否向个人信息主体告知公开披露个人信息的目的、类型，并征得用户明示同意。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.3 测评项：详见 GB/T 35273—2020 中 9.4 的 c）。

6.5.4.3.1 测评单元（EPI-21）

a) 指标要求：App 提供者公开披露个人敏感信息前，除 GB/T 35273—2020 9.4 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容。
b) 测评对象：App、文档资料
c) 测评方式：功能验证、文档审查
d) 测评步骤：
1) 通过App功能验证，询问App提供者，判断是否存在个人敏感信息公开披露的行为；
2) 如果App存在公开披露个人敏感信息的行为，查看是否在公开披露前，除GB/T 35273—2020 9.4 b）中规定告知的内容外，还向个人信息主体告知涉及的个人敏感信息的内容；
3) 查看App提供者是否有相应的管理制度，要求公开披露个人敏感信息前，应向个人信息主体告知涉及的个人敏感信息的内容。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.4 测评项：详见 GB/T 35273—2020 中 9.4 的 d）。

6.5.4.4.1 测评单元（EPI-22）

a) 指标要求：App 提供者应准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；
b) 测评对象：App、文档资料、App 服务端
c) 测评方式：功能验证、人员访谈、文档审查、服务端核查
d) 测评步骤：
1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；
2) 查看App提供者是否有个人信息公开披露的管理制度明确规定应准确记录和保存个人信息的公开披露的情况；
3) 通过App功能验证、核查App服务端、询问App提供者，查看是否存在个人信息公开披露的情况，如果存在则查看个人信息的公开披露的记录，查看记录内容是否包括公开披露的日期、规模、目的、公开范围等；
4) 对于App中进行的公开披露行为，查看系统中是否有相应记录。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.5 测评项：详见 GB/T 35273—2020 中 9.4 的 e）。

6.5.4.5.1 测评单元（EPI-23）

a) 指标要求：App 提供者应承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任。
b) 测评对象：App
c) 测评方式：文档审查
d) 测评步骤：
   1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；
   2) 查阅App个人信息保护政策等相关文档是否有因公开披露个人信息对个人信息主体合法权益造成损害时承担相应责任的说明。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.6 测评项：详见 GB/T 35273—2020 中 9.4 的 f）。

6.5.4.6.1 测评单元（EPI-24）

a) 指标要求：App 提供者不得公开披露个人生物识别信息。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；
   2) 查看App提供者是否有不得公开披露个人生物识别信息的管理制度；
   3) 通过功能验证、服务端核查，查看App提供者是否存在公开披露个人生物识别信息的情况。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定且 3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.7 测评项：详见 GB/T 35273—2020 中 9.4 的 g）。

6.5.4.7.1 测评单元（EPI-25）

a) 指标要求：App 提供者不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 通过App功能验证，询问App提供者，判断是否存在个人信息公开披露的行为；
   2) 查看App提供者是否有不得公开披露种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果的管理制度；
   3) 通过功能验证、服务端核查，查看App是否存在公开披露种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果的情况。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定且 3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.5 共享、转让、公开披露个人信息时事先征得授权同意的例外的测评

6.5.5.1 测评项：详见 GB/T 35273—2020 中的 9.5。

6.5.5.1.1 测评单元（EPI-26）

a) 指标要求：App 提供者共享、转让、公开披露个人信息时事先征得授权同意的例外的情形应在 GB/T 35273—2020 9.5 列举范围内。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 查看App的个人信息保护政策，是否声明了不合理的共享、转让、公开披露个人信息时事先征得授权同意的例外；
   2) 通过App功能验证、核查App服务端、询问App提供者等方式，判断是否存在未征得用户授权同意共享、转让、公开披露个人信息，且不在事先征得授权同意的例外范围的行为。
e) 单元判定：如果 1）、2）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.6 共同个人信息控制者的测评

6.5.6.1 测评项：详见 GB/T 35273—2020 中 9.6 的 a）。

6.5.6.1.1 测评单元（EPI-27）

a) 指标要求：当 App 提供者与第三方为共同个人信息控制者时，应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知。
b) 测评对象：App、文档资料
c) 测评方式：功能验证、技术检测、文档审查、人员访谈
d) 测评步骤：
   1) 通过App功能验证、技术检测，询问App提供者，判断是否存在与第三方为共同个人信息控制者的情况；
   2) 查看App提供者是否建立相关管理制度，要求通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知；
   3) 查看合同等与第三方签订的文件是否包含应满足个人信息安全方面的要求，以及在个人信息安全方面双方分别承担的责任和义务；
   4) 查看是否通过个人信息保护政策等方式向用户明确告知关于共同个人信息者应满足的个人信息安全要求以及双方分别承担的责任和义务等内容。

   注：如个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者。
e) 单元判定：如果 1）为否定，则本测试单元为不适用。如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.6.2 测评项：详见 GB/T 35273—2020 中 9.6 的 b）。

6.5.6.2.1 测评单元（EPI-28）

a) 指标要求：App 提供者如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，应承担因第三方引起的个人信息安全责任。
b) 测评对象：App、文档资料

c) 测评方式：功能验证、技术检测、文档审查、人员访谈
d) 测评步骤：
   1) 通过App功能验证、技术检测，询问App提供者，判断是否存在与第三方为共同个人信息控制者的情况；
   2) 查看是否在个人信息保护政策或其他文档中向用户明确告知第三方身份以及在个人信息安全方面自身和第三方应分别承担的责任和义务；
   3) 如果未告知，检查是否有对第三方引起的个人信息安全责任的免责声明。。
e) 单元判定：如果 1）为否定，则本测评单元为不适用。如果 1）、2）为肯定，或 1）为肯定且 2）、3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7 第三方接入管理的测评

6.5.7.1 测评项：详见 GB/T 35273—2020 中 9.7 的 a）。

6.5.7.1.1 测评单元（EPI-29）

a) 指标要求：App 提供者应建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1) 查看App提供者的相关管理制度，是否明确第三方产品或服务接入管理机制、工作流程、安全评估制度等；
   2) 核查App服务端、询问App提供者的第三方产品或服务业务相关责任人，记录是否按照相关管理制度的要求进行了第三方接入管理，是否形成了相关的第三方接入管理记录，第三方接入安全评估记录等文档。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，其他情况不符合本测评单元指标要求。

6.5.7.2 测评项：详见 GB/T 35273—2020 中 9.7 的 b）。

6.5.7.2.1 测评单元（EPI-30）

a) 指标要求：App 提供者应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评步骤：
   1) 查看App提供者是否具备与第三方产品或服务提供者签订的接入有关合同等文件，明确双方应承担的责任、义务、个人信息保护方面采取的措施；
   2) 查看合同等相关文件是否明确第三方产品或服务收集的个人信息类型、申请的系统权限、个人信息收集目的、所收集的个人信息保存期限和个人信息处理方式。
e) 单元判定：如果以上 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.3 测评项：详见 GB/T 35273—2020 中 9.7 的 c）。

6.5.7.3.1 测评单元（EPI-31）

a) 指标要求：App 提供者应向个人信息主体明确标识产品或服务由第三方提供。
b) 测评对象：App、App 服务端
c) 测评方式：功能验证、技术检测、人员访谈、服务端核查
d) 测评步骤：
   1) 通过App功能验证、技术检测，核查App服务端，以及询问App提供者等方式，判断App是否存在由第三方提供的功能；
   2) 如果存在第三方接入，通过功能验证查看App功能界面中是否明确标识产品或服务由第三方提供。
e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.4 测评项：详见 GB/T 35273—2020 中 9.7 的 d）。

6.5.7.4.1 测评单元（EPI-32）

a) 指标要求：App 提供者应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1) 询问App提供者是否有第三方接入有关合同和管理记录；
   2) 查看第三方接入有关合同和管理记录的文件资料是否完整；
   3) 查看管理记录，是否涵盖了第三方产品或服务接入、评估、更改、停止、责任落实情况等记录。
e） 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.5 测评项：详见 GB/T 35273—2020 中 9.7 的 e）。

6.5.7.5.1 测评单元（EPI-33）

a) 指标要求：App 提供者应要求第三方根据 GB/T 35273—2020 相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式。
b) 测评对象：App、App 服务端、文档资料
c) 测评方式：功能验证、服务端核查、文档审查
d) 测评步骤：
   1) 通过功能验证查看App中的第三方收集个人信息时是否征得用户同意；
   2) 查看App提供者与第三方签订的合同或合作协议，是否明确要求第三方根据GB/T 35273—2020相关要求向个人信息主体征得收集个人信息的授权同意；
   3) 核查App服务端是否具备必要时核验第三方向个人信息主体征得收集个人信息的授权同意的实现方式的机制。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.6 测评项：详见 GB/T 35273—2020 中 9.7 的 f）。

6.5.7.6.1 测评单元（EPI-34）

a) 指标要求：App 提供者应要求第三方产品或服务建立响应个人信息主体请求和投诉的机制，以供个人信息主体查询、使用。
b) 测评对象：App、文档资料
c) 测试方式：功能验证、文档审查
d) 测评步骤：
   1) 查看App提供者与第三方签订的合同或合作协议，是否明确要求第三方产品或服务建立响应个人信息主体请求和投诉的机制；
   2) 通过App功能验证查看第三方产品或服务的个人信息保护政策或功能页面，查看第三方产品或服务的投诉链接或联系方式；验证第三方产品或服务的投诉链接或联系方式是否有效；
   3) 查看是否可以通过App提供者的反馈渠道向第三方进行请求和投诉。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.7 测评项：详见 GB/T 35273—2020 中 9.7 的 g）。

6.5.7.7.1 测评单元（EPI-35）

a) 指标要求：App 提供者应监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、人员访谈、服务端核查
d) 测评步骤：
   1) 查看App提供者有关接入第三方产品或服务的管理机制、评估机制和工作流程资料，是否有对第三方产品或服务动态监测或定期进行个人信息安全审计的方式说明；查看管理机制中是否规定停止接入的情形；
   2) 查看接入第三方产品或服务管理记录，是否有第三方产品或服务未落实安全管理要求和责任的记录。对于未落实安全管理要求和责任的第三方产品或服务，是否有整改或停止接入记录；
   3) 核查App服务端是否具备停止接入第三方产品或服务的技术机制。
e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.8 测评项：详见 GB/T 35273—2020 中 9.7 的 h）。

6.5.7.8.1 测评单元（EPI-36）

a) 指标要求：产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜开展技术检测确保其个人信息收集、使用行为符合约定要求。对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。
b) 测评对象：文档资料、App 服务端
c) 测评方式：人员访谈、服务端核查、技术检测
d) 测评步骤：
   1）查看 App 提供者的第三方产品或服务相关管理制度，是否规定对第三方自动化工具进行个人信息收集、使用行为进行技术检测，从而使其符合管理要求；是否规定对第三方嵌入

或接入的自动化工具收集个人信息的行为进行审计，以及发现超出约定的行为的处理方式；

2）服务端核查并询问 App 提供者是否对接入的第三方自动化工具进行技术检测，查看检测报告内容是否覆盖个人信息收集、使用行为等方面；

3）询问并查看 App 提供者是否对接入的第三方自动化工具收集个人信息的行为进行审计，是否具备发现超出约定行为时及时切断接入的机制；查看第三方工具对收集个人信息行为的审计记录及超出约定行为的切断接入记录。

e) 单元判定：如果 1）、2）、3）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.8 个人信息跨境传输的测评

6.5.8.1 测评项：详见 GB/T 35273—2020 中的 9.8。

6.5.8.1.1 测评单元（EPI-37）

a) 指标要求：App 提供者向境外提供在中华人民共和国境内运营中收集和产生的个人信息时，应遵循国家相关规定和标准要求对向境外传输个人信息的业务进行安全评估。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：技术检测、服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 通过App技术检测、核查App服务端、询问App提供者等方式，查看App是否存在向境外传输个人信息的业务场景；

2) 查看涉及个人信息出境的业务功能、个人信息类型、境外传输的目的、传输的境外区域等信息；核查App提供者是否依据相关要求进行了申报和安全评估。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.8.1.2 测评单元（EPI-38）

a) 指标要求：App 不应存在私自向境外传输个人信息的行为。

b) 测评对象：App、App 服务端

c) 测评方式：技术检测、服务端核查

d) 测评步骤：

1) 通过App技术检测，查看与境外IP或域名有通信连接的IP地址、域名、传输的数据包；

2) 对向境外传输的数据进行分析，判断通信数据中是否存在个人信息。如传输数据采用加密技术或无法直接分析传输数据类型，则要求App提供者提供相关澄清材料；

3) 根据1）、2）的检测结果判断App是否存在私自向境外传输个人信息的情况。

e) 单元判定：如果 3）为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6 个人信息安全事件处置的测评

6.6.1 个人信息安全事件应急处置和报告的测评

6.6.1.1 测评项：详见 GB/T 35273—2020 中 10.1 的 a）。

6.6.1.1.1 测评单元（HPI-01）

a) 指标要求：App 提供者应制定个人信息安全事件应急预案。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评实施：
   1) 查看App提供者是否制定个人信息安全事件应急预案的相关制度文件，应急预案应内容完整，能够满足相关法律法规要求，并满足公司实际情况。
e) 单元判定：如果 1）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.1.2 测评项：详见 GB/T 35273—2020 中 10.1 的 b）。

6.6.1.2.1 测评单元（HPI-02）

a) 指标要求：App 提供者应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责、应急处置策略和规程。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评实施：
   1) 检查App提供者是否具有应急演练相关记录，应急预案演练记录是否记录演练时间、操作内容、演练结果等；
   2) 检查App提供者是否具有应急响应培训记录，如：培训时间、培训计划、培训方案、培训效果等；
   3) 访谈App提供者是否要求相关人员定期（至少每年一次）参加应急响应培训和应急演练；
   4) 访谈事件处置人员是否掌握岗位职责以及应急处置策略和规程。
e) 单元判定：如果 1）至 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.1.3 测评项：详见 GB/T 35273—2020 中 10.1 的 c）。

6.6.1.3.1 测评单元（HPI-03）

a) 指标要求：发生个人信息安全事件后，App 提供者应根据应急响应预案进行以下处置：
   1) 记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；
   2) 评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；
   3) 按照有关规定及时报告，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；
   4) 个人信息泄露事件可能会给个人信息主体的合法权益造成严重危害的，如个人敏感信息的泄露，按照GB/T 35273—2020 10.2的要求实施安全事件的告知。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评实施：
   1) 访谈App提供者，是否发生过个人信息安全事件；如发生个人信息安全事件，访谈个人信息安全事件的处置情况；

2) 核查App提供者在发生个人信息安全事件后是否对事件内容进行记录，记录事件内容包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；
3) 核查个人信息安全事件评估报告，内容是否包括安全事件可能造成的影响、处置过程、补救措施等；
4) 检查个人信息安全事件报告及相关记录，是否按照有关规定及时报告，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；
5) 访谈App提供者，是否评估个人信息泄露事件对个人信息主体的合法权益造成的危害，如涉及个人敏感信息泄露的，是否按照GB/T 35273—2020 10.2中安全事件告知要求进行告知。

e) 单元判定：如果 1）为否定，则本测评单元为不适用；如果 1）至 5）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.1.4 测评项：详见 GB/T 35273—2020 中 10.1 的 d）。

6.6.1.4.1 测评单元（HPI-04）

a) 指标要求：App 提供者应根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评实施：
1) 查看App提供者的管理制度或应急预案相关更新条款，是否包含应急预案更新要求；
2) 查看应急预案修订记录是否根据相关法律法规变化情况，以及事件处置情况，修订完善应急预案。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.2 安全事件告知的测评

6.6.2.1 测评项：详见 GB/T 35273—2020 中 10.2 的 a）。

6.6.2.1.1 测评单元（HPI-05）

a) 指标要求：App 提供者应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评实施：
1) 查看App提供者的个人信息安全事件处置相关的管理制度，是否包含个人信息安全事件告知要求；
2) 访谈App提供者的个人信息安全事件处置相关人员，是否曾发生个人信息安全事件，如发生个人信息安全事件，查阅是否具备相关告知记录，检查是否及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体；难以逐一告知个人信息主体时，是否采取合理、有效的方式发布与公众有关的警示信息。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要

求。

6.6.2.2 测评项：详见 GB/T 35273—2020 中 10.2 的 b）。

6.6.2.2.1 测评单元（HPI-06）

a) 指标要求：个人信息安全事件告知内容应包括但不限于：
   1）安全事件的内容和影响；
   2）已采取或将要采取的处置措施；
   3）个人信息主体自主防范和降低风险的建议；
   4）针对个人信息主体提供的补救措施；
   5）个人信息保护负责人和个人信息保护工作机构的联系方式。
b) 测评对象：文档资料
c) 测评方式：文档审查
d) 测评实施：
   1) 查看App提供者的个人信息安全事件处置相关的管理制度，是否包含个人信息安全事件告知内容，内容是否完备；
   2) 访谈个人信息安全事件处置相关人员，是否曾发生个人信息安全事件，如发生个人信息安全事件，查阅相关告知记录，检查安全事件告知是否包括安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范和降低风险的建议、针对个人信息主体提供的补救措施、个人信息保护负责人和个人信息保护工作机构的联系方式等方面内容。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7 组织的个人信息安全管理要求的测评

6.7.1 明确责任部门与人员的测评

6.7.1.1 测评项：详见 GB/T 35273—2020 中 11.1 的 a）。

6.7.1.1.1 测评单元（PIO-01）

a) 指标要求：App 提供者应明确法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确了法定代表人或主要负责人在个人信息安全方面的领导责任；
   2）对信息安全负责人进行访谈，确认其是否了解相关的个人信息安全管理制度并按照管理制度的要求履行其个人信息安全领导义务；
   3）对相关的管理记录进行查验并结合访谈，以确认是否有充分的人力、物力、财力保障个人信息安全管理制度得到有效运行。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.2 测评项：详见 GB/T 35273—2020 中 11.1 的 b）。

6.7.1.2.1 测评单元（PIO-02）

a) 指标要求：App 提供者应任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确了个人信息保护负责人和个人信息保护机构；
   2）对个人信息保护负责人的个人资料进行查验并对其进行访谈，确认其是否具有相关管理工作经历和个人信息保护专业知识；
   3）对相关的活动记录进行查验并结合访谈，以确认个人信息保护负责人是否能参与有关个人信息处理活动的重要决策并直接向组织主要负责人报告工作。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.3 测评项：详见 GB/T 35273—2020 中 11.1 的 c）。

6.7.1.3.1 测评单元（PIO-03）

a) 指标要求：App 提供者应在满足 GB/T 35273—2020 中 11.1 的 c）中的 1）2）3）项条件之一时，设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）通过审查相关文档并结合访谈确认：该组织内的该 App 从业人员规模是否大于 200 人；
   2）核查 App 服务端，并结合文档审查及访谈确认：该组织处理的个人信息规模是否超过 100 万人，或未来 12 个月内预计处理的个人信息规模超过 100 万人；
   3）核查 App 服务端，并结合文档审查及访谈确认：该组织处理的个人敏感信息规模是否超过 10 万人；
   4）如果以上 1）、2）、3）其中一项为肯定，则需通过文档审查及人员访谈确认：组织是否设立了专职的个人信息保护负责人和个人信息保护工作机构以负责个人信息安全工作。
e) 单元判定：如果 1）、2）、3）均为否定，则本测评单元为不适用；如果 4）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.4 测评项：详见 GB/T 35273—2020 中 11.1 的 d）。

6.7.1.4.1 测评单元（PIO-04）

a) 指标要求：个人信息保护负责人和个人信息保护工作机构的职责应覆盖 GB/T 35273—2020 中 11.1 的 d）中 1）~10）的内容。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，其个人信息保护负责人和个人信息保护机构的职责是否覆盖了 GB/T 35273—2020 中 11.1 的 d）中 1）~10）的所有内容；

2）对个人信息保护负责人及个人信息保护机构中的人员进行访谈，确认其是否了解 GB/T 35273—2020 中 11.1 的 d）中 1）~10）的内容，并按照管理制度的要求履行其个人信息安全保护义务；

3）对相关的过程记录进行查验并结合访谈，以确认个人信息保护负责人及个人信息保护机构的职责得到有效贯彻和运行；

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.5 测评项：详见 GB/T 35273—2020 中 11.1 的 e）。

6.7.1.5.1 测评单元（PIO-05）

a) 指标要求：App 提供者应为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1）查看 App 提供者的个人信息安全相关管理制度，是否明确了个人信息保护负责人和个人信息保护工作机构的资源配置（人力、物力、财力等）；

2）通过人员访谈及查验过程记录等方式，确认管理制度所规定的个人信息保护负责人和个人信息保护工作机构的资源配置得到有效落实；

3）通过人员访谈及查验过程记录等方式，确认个人信息保护负责人和个人信息保护工作机构是否能独立履行职责。

e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.2 个人信息安全工程的测评

6.7.2.1 测评项：详见 GB/T 35273—2020 中的 11.2。

6.7.2.1.1 测评单元（PIO-06）

a) 指标要求：在开发 App 时，App 提供者宜根据国家有关标准在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1）查看 App 提供者的个人信息安全相关管理制度，是否明确了 App 开发过程在需求、设计、开发、测试、发布等阶段的个人信息保护要求；

2）通过人员访谈、服务端核查、文档审查等手段进行核实，记录 App 提供者是否按照管理制度的要求在开发过程中将个人信息保护措施同步规划、同步建设和同步使用。

e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.3 个人信息处理活动记录的测评

6.7.3.1 测评项：详见 GB/T 35273—2020 中 11.3 的 a）。

6.7.3.1.1 测评单元（PIO-07）

a) 指标要求：App 提供者宜建立、维护和更新所收集、使用的个人信息处理活动记录，记录的内容可包括：所涉及个人信息的类型、数量、来源（例如从个人信息主体直接收集或通过间接获取方式获得）。
b) 测评对象：App 服务端、文档资料
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求需建立、维护和更新所收集、使用的个人信息处理活动记录；
   2）通过人员访谈、服务端核查、文档审查等手段进行核实，记录 App 提供者是否保存了个人信息处理活动记录，并按制度的规定进行维护和更新；
   3）查看个人信息处理活动记录，是否包含所涉及个人信息类别、数量、来源。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.3.2 测评项：详见 GB/T 35273—2020 中 11.3 的 b）。

6.7.3.2.1 测评单元（PIO-08）

a) 指标要求：App 提供者宜建立、维护和更新所收集、使用的个人信息处理活动记录，记录的内容可包括：根据业务功能和授权情况区分个人信息的处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境等情况。
b) 测评对象：App 服务端、文档资料
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确了对以下内容的记录：根据业务功能和授权情况区分个人信息的处理目的、使用场景，委托处理、共享、转让、公开披露、是否涉及出境等情况；
   2）通过人员访谈、服务端核查、文档审查等手段进行核实，App 提供者是否保存了：根据业务功能和授权情况区分个人信息的处理目的、使用场景，委托处理、共享、转让、公开披露、是否涉及出境等情况的记录。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.3.3 测评项：详见 GB/T 35273—2020 中 11.3 的 c）。

6.7.3.3.1 测评单元（PIO-09）

a) 指标要求：App 提供者宜建立、维护和更新所收集、使用的个人信息处理活动记录，记录的内容可包括：与个人信息处理活动各环节相关的信息系统、组织或人员。
b) 测评对象：App 服务端、文档资料
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，其中是否需明确记录：与个人信息处理活动各环节相关的信息系统、组织或人员；
   2）通过人员访谈、服务端核查、文档审查等手段进行核实，App 提供者是否保存了：个人信

息处理活动各环节相关的信息系统、组织或人员的记录。

e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4 开展个人信息安全影响评估的测评

6.7.4.1 测评项：详见 GB/T 35273—2020 中 11.4 的 a）。

6.7.4.1.1 测评单元（PIO-10）

a) 指标要求：应建立个人信息安全影响评估制度，评估并处置个人信息处理活动存在的安全风险。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 的个人信息安全影响评估相关制度，是否包含评估并处置个人信息处理活动存在的安全风险的内容；
   2）通过访谈 App 提供者的相关人员，是否了解制度中评估并处置个人信息处理活动存在的安全风险等相关内容；
   3）通过人员访谈、服务端核查、文档审查等手段进行核实，App 提供者是否有评估并处置个人信息处理活动存在的安全风险的相关记录。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.2 测评项：详见 GB/T 35273—2020 中 11.4 的 b）。

6.7.4.2.1 测评单元（PIO-11）

a) 指标要求：个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于 GB/T 35273—2020 中 11.4 的 b）中的 1）至 6）的要求。
b) 测评对象：App 服务端、文档资料
c) 测评方式：服务端核查、文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全影响评估相关管理制度，是否明确个人信息安全影响评估的内容应包括 GB/T 35273—2020 中 11.4 的 b）中的 1）至 6）的要求；
   2）查看 App 提供者的个人信息安全影响评估记录，核查个人信息安全影响评估内容是否覆盖 GB/T 35273—2020 中 11.4 的 b）中的 1）至 6）的要求。

   注：App 提供者可能针对不同的场景产生不同的个人信息安全影响评估报告，因此，个人信息安全影响评估报告可以是多个，总体上涵盖 GB/T 35273—2020 中 11.4 的 b）中的 1）至 6）的要求即可。
e) 单元判定：如果 1）、2）为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.3 测评项：详见 GB/T 35273—2020 中 11.4 的 c）。

6.7.4.3.1 测评单元（PIO-12）

a) 指标要求：App 提供者应在产品或服务发布前，或业务功能发生重大变化时，应进行个人信息安全影响评估。

b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全影响评估相关制度，是否包含在产品或服务发布前，或业务功能发生重大变化时，应进行个人信息安全影响评估的相关内容；
   2）通过访谈 App 提供者的相关人员，是否了解制度中产品或服务发布前，或业务功能发生重大变化时，进行个人信息安全影响评估的相关内容；
   3）通过服务端核查、文档审查等方式，核查 App 提供者是否有产品或服务发布前，或业务功能发生重大变化时，进行个人信息安全影响评估的相关记录。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.4 测评项：详见 GB/T 35273—2020 中 11.4 的 d）。

6.7.4.4.1 测评单元（PIO-13）

a) 指标要求：在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，App 提供者应进行个人信息安全影响评估。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全影响评估相关制度，在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，是否有个人信息安全影响评估的相关要求，是否详细界定了法律法规新要求、是否定义了业务模式、信息系统、运行环境发生重大变更的情形，是否定义了重大个人信息安全事件；
   2）通过访谈 App 提供者的相关人员，核查其是否了解制度中的相关规定；
   3）通过文档审查等方式，核查 App 提供者是否有相关的评估记录。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.5 测评项：详见 GB/T 35273—2020 中 11.4 的 e）。

6.7.4.5.1 测评单元（PIO-14）

a) 指标要求：App 提供者应形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平。
b) 测评对象：App、App 服务端、文档材料
c) 测评方式：功能验证、技术检测、服务端核查、文档审查
d) 测评步骤：
   1）查看 App 提供者的个人信息安全影响评估报告，其中是否明确了保护个人信息主体的措施；
   2）通过 App 功能验证、技术检测，核查 App 服务端，核查个人信息安全影响评估报告中明确的个人信息主体保护措施是否有效实施。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.6 测评项：详见 GB/T 35273—2020 中 11.4 的 f）。

6.7.4.6.1 测评单元（PIO-15）

a) 指标要求：App 提供者应妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 的个人信息安全影响评估相关制度，是否明确妥善留存个人信息安全影响评估报告的具体方式，从而确保可供相关方查阅，并明确了对外公开的具体途径；
   2）查看 App 提供者是否按照制度的规定留存了个人信息安全影响评估报告，制度所规定的对外公开个人信息安全影响评估报告的途径是否真实有效。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.5 数据安全能力的测评

6.7.5.1 测评项：详见 GB/T 35273—2020 中的 11.5。

6.7.5.1.1 测评单元（PIO-16）

a) 指标要求：App 提供者应根据有关国家标准的要求，建立适当的数据安全能力，并落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确了数据安全管理组织架构、数据安全管理人员及角色、数据安全管理策略、数据分类分级管理策略等制度；
   2）查看相关管理制度是否明确数据安全生命周期各阶段的数据安全管理要求，是否设置数据安全管理相关岗位或角色，并规范数据安全管理相关人员的操作；
   3）查看 App 提供者建立的数据安全能力是否符合 App 所属类型有关国家标准要求，是否存在缺失或遗漏；
   4）通过文档审查、服务端核查、人员访谈等方式，核查 App 提供者是否按制度要求建立数据安全能力，落实在数据采集、传输、存储、处理、共享、销毁等过程的安全管理和安全技术保障措施。
e) 单元判定：如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6 人员管理与培训

6.7.6.1 测评项：详见 GB/T 35273—2020 中 11.6 的 a）。

6.7.6.1.1 测评单元（PIO-17）

a) 指标要求：App 提供者应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：

1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；
2）通过访谈，以确认是否明确个人信息处理岗位，以及大量接触个人敏感信息的岗位，并形成相应岗位人员名单；
3）通过文档审查，查看是否与所有从事个人信息处理岗位上的相关人员签署保密协议；
4）通过文档审查，查看是否对接触个人敏感信息的人员进行背景审查、评审等形成相关记录，查看现有大量接触个人敏感信息的人员是否均通过背景审查。

e) 单元判定：如果 1）至 4）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.2 测评项：详见 GB/T 35273—2020 中 11.6 的 b）。

6.7.6.2.1 测评单元（PIO-18）

a) 指标要求：App 提供者应明确内部涉及个人信息处理不同岗位的安全职责，建立发生安全事件的处罚机制。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
1）查看 App 提供者的个人信息安全相关管理制度，是否明确内部涉及个人信息处理不同岗位的安全职责，是否建立发生安全事件的处罚机制；
2）通过访谈，验证岗位人员是否明确且满足岗位要求；
3）查看如果发生安全事件是否按相关处罚机制进行处理。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.3 测评项：详见 GB/T 35273—2020 中 11.6 的 c）。

6.7.6.3.1 测评单元（PIO-19）

a) 指标要求：App 提供者应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
1）查看 App 提供者的个人信息安全相关管理制度，是否要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；
2）通过访谈和文档审查，验证相关管理制度要求是否有效落实，是否在劳动合同、入职协议、保密协议、离职保密协议等文件中要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；
3）通过访谈相关人员及互联网信息搜集，查看 App 是否存在终止劳务合同的人员发生泄密事件。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.4 测评项：详见 GB/T 35273—2020 中 11.6 的 d）。

6.7.6.4.1 测评单元（PIO-20）

a) 指标要求：App 提供者应明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，与其签署保密协议，并进行监督。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，并要求与其签署保密协议，并进行监督的要求；
   2）通过访谈和文档审查，核查App提供者是否形成可能访问个人信息的外部服务人员名单，是否与其签订保密协议，并进行有效监督。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.5 测评项：详见 GB/T 35273—2020 中 11.6 的 e）。

6.7.6.5.1 测评单元（PIO-21）

a) 指标要求：App 提供者应建立相应的内部制度和政策对员工提出个人信息保护的指引和要求。
b) 测评对象：文档资料
c) 测评方式：人员访谈、文档审查
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确建立相应的内部制度和政策对员工提出个人信息保护的指引和要求；
   2）通过访谈方式，以确认相关指引和要求是否有效传达，是否对员工的个人信息保护的指引和要求执行情况进行评估。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.6 测评项：详见 GB/T 35273—2020 中 11.6 的 f）。

6.7.6.6.1 测评单元（PIO-22）

a) 指标要求：App 提供者应定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核的要求；
   2）通过查验培训、考核等相关记录资料，是否按照规定定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核；
   3）访谈个人信息处理岗位相关人员，以确认是否掌握个人信息保护政策和相关规程。
e) 单元判定：如果 1）、2）、3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单

元指标要求。

6.7.7 安全审计

6.7.7.1 测评项：详见 GB/T 35273—2020 中 11.7 的 a）。

6.7.7.1.1 测评单元（PIO-23）

a) 指标要求：App 提供者应对个人信息保护政策、相关规程和安全措施的有效性进行定期审计。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确了对个人信息保护政策、相关规程和安全措施的有效性进行定期审计的要求，是否明确审计管理岗位职责及人员、审计流程、审计策略、审计范围、审计频率、审计报告、审计问题的预防措施等具体内容；
   2）通过访谈审计相关人员、查验审计过程资料、服务端核查等方式，验证对个人信息保护政策、相关规程和安全措施的审计是否有效。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.2 测评项：详见 GB/T 35273—2020 中 11.7 的 b）。

6.7.7.2.1 测评单元（PIO-24）

a) 指标要求：App 提供者应建立自动化审计系统，监测记录个人信息处理活动。
b) 测评对象：App 服务端、文档资料
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）核查 App 服务端是否建立自动化审计系统，监测记录个人信息处理活动；
   2）通过人员访谈、文档审查，查看 App 提供者是否对自动化审计系统监测情况有效性进行核查分析处理。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.3 测评项：详见 GB/T 35273—2020 中 11.7 的 c）。

6.7.7.3.1 测评单元（PIO-25）

a) 指标要求：App 提供者对审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确要求针对审计过程形成记录能对安全事件的处置、应急响应和事后调查提供支撑；
   2）通过人员访谈、文档审查等方式，查验审计过程形成的记录是否包含审计问题、计划整改措施、计划整改结果、计划整改时间、计划整改责任人等内容以对安全事件的处置、应急响应和事后调查提供支撑。

e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.4 测评项：详见 GB/T 35273—2020 中 11.7 的 d）。

6.7.7.4.1 测评单元（PIO-26）

a) 指标要求：App 提供者应防止非授权访问、篡改或删除审计记录。
b) 测评对象：文档资料、App 服务端
c) 测评方式：文档审查、服务端核查、人员访谈
d) 测评步骤：
   1）查看 App 提供者的个人信息安全相关管理制度，是否明确应防止非授权访问、篡改或删除审计记录的要求；
   2）通过核查 App 服务端审计系统访问控制情况、人员访谈及文档审查等方式，查看是否有防止非授权访问、篡改或删除审计记录的安全策略或预防措施，如设置访问审计记录权限、对删除修改操作审批等，以确认安全策略或预防措施得到有效落实。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.5 测评项：详见 GB/T 35273—2020 中 11.7 的 e）。

6.7.7.5.1 测评单元（PIO-27）

a) 指标要求：App 提供者应及时处理审计过程中发现的个人信息违规使用、滥用等情况。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者相关管理制度，是否明确针对审计过程中发现的个人信息违规使用、滥用等情况建立及时处理的机制和流程的要求；
   2）通过人员访谈及文档审查等方式，查看 App 提供者是否按照相关机制和流程处理个人信息违规使用、滥用等情况。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.6 测评项：详见 GB/T 35273—2020 中 11.7 的 f）。

6.7.7.6.1 测评单元（PIO-28）

a) 指标要求：App 提供者审计产生的审计记录和留存时间应符合法律法规的要求。
b) 测评对象：文档资料
c) 测评方式：文档审查、人员访谈
d) 测评步骤：
   1）查看 App 提供者相关管理制度，是否明确审计记录和留存时间要求；
   2）通过文档审查和人员访谈，以确认审计记录和留存时间是否符合法律法规或内部管理制度的要求。
e) 单元判定：如果 1）、2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7 结果判定

测评人员进行 App 个人信息安全整体测评结果判定时，应首先给出每一个测评单元的判定结果。在进行测评单元结果判定时，不同测评方式的采信顺序按照：技术检测、功能验证、服务端核查、文档审查、人员访谈的顺序排列。根据测评单元的判定结果确定每一个测评项的判定结果时，仅当每一个测评项下的测评单元全部符合时，判定该测评项为符合。当所有测评项的结果均为符合时，App 个人信息安全测评的结论为符合。GB/T 35273—2020 中宜达到的要求，不作为必须符合的测评项要求。

附 录 A
（资料性）
App 提供者基本信息采集表

开始测评前，App提供者可参考下列表格提供App收集使用个人信息的基本情况。

表 A.1 App 基本信息表

App 名称		**操作系统类型**	
版本号		**运营者名称**	
样本获取时间		**App 提供者联系人和联系方式**	
基本业务功能		**App 个人信息保护负责人/机构和联系方式**	
业务功能描述			

表 A.2 App 收集个人信息基本情况表

服务类型	**功能模块**	**功能**	**收集个人信息**	**收集方式**	**对应权限**	**收集目的**	**收集时机或频率**	**必要性**	**用户授权方式**	**保存方式**	**保存期限**	**超期处理方式**
				自动采集、主动提供、间接获取								

表 A.3 第三方服务基本情况表

服务名称	**收集个人信息**	**用户授权方式**	**服务提供者名称**	**第三方收集的个人信息**	**App 共享给第三方的个人信息**	**第三方提供给 App 的个人信息**	**第三方服务访问方式**	**是否签署合同或数据保护协议**

表 A.4 第三方 SDK 基本情况表

SDK 名称	**SDK 版本**	**SDK 提供者名称**	**SDK 获取方式**	**SDK 使用目的**	**是否签署合同或数据保护协议**	**SDK 收集的个人信息**	**SDK 收集个人信息频率**	**对应权限**	**收集个人信息目的**	**向第三方提供个人信息的方式（委托处理/共享/转让）**

附 录 B
（资料性）
App 欺诈、诱骗、误导方式收集个人信息行为举例

表B.1给出了App通过欺诈、诱骗、误导方式收集个人信息的典型行为。

表B.1 App通过欺诈、诱骗、误导方式收集个人信息行为举例

序号	举例
1	以红包、积分、福利、抽奖等奖励为由收集与奖励内容不相关的个人信息。
2	以红包、积分、福利、抽奖等奖励为由要求用户额外提供个人信息，用户提供个人信息后未给予说明的奖励，或将以此为由收集的个人信息用于说明以外的目的。
3	申请权限时的说明与获得权限后的实际行为不符，如以添加联系人为由申请通讯录权限，用户打开权限后上传整个通讯录。
4	应用市场描述与 App 实际业务功能存在较大的不一致。例如，应用市场中描述 App 为阅读类应用，用户下载后，App 在服务端修改内嵌 H5 页面的内容，向用户提供网络借贷服务。
5	App 本身是欺诈、诱骗、误导的 App。例如，App 是其他 App 的仿冒版。
6	App 隐私政策或界面描述中误导用户多提供信息，例如将某项业务功能的非必要个人信息描述为该项业务功能的必要个人信息。
7	App 内欺诈、诱骗、误导用户下载其他 App，特别是具有分发功能的 App 欺骗、误导用户下载非用户所自愿下载 App 的行为。
8	采用伪造、欺骗下载或其他不正当方式操纵用户评论、误导用户行为，影响在应用商店中的排名，如刷量行为。
9	在应用中展现钓鱼网站，欺骗用户访问，盗取用户重要的认证凭据或其他敏感信息。
10	伪装成系统或其他应用发送的通知，欺骗用户执行操作。
11	直接展示虚假的系统或应用界面，滥用悬浮窗权限，在其他应用或系统界面之上展示虚假的界面，欺骗用户执行操作。
12	通过图标或内容等方式，伪装成系统应用，在用户不知情的情况下实施恶意行为。

附 录 C
（资料性）
测试单元编号说明

测评单元编号为 2 组数据，格式为 xxx-xx，各组含义和编码规则如下：

第 1 组由字母组成，字母代表对个人信息安全要求的类别：个人信息的收集为 PIC（PI collection），个人信息的存储为 PIS（PI storage），个人信息的使用为 UPI（Use of PI），个人信息主体的权利为 RPI（Rights of PI Subjects），个人信息的委托处理、共享、转让、公开披露为 EPI（Entrusted processing, sharing, transfer and public disclosure of PI），个人信息安全事件处置为 HPI（Handling of PI security incidents），组织的个人信息安全管理要求为 PIO（PI security management requirements for organizations）。

第 2 组由 2 位数字组成，按类对测试单元进行顺序编号。

附 录 D
（资料性）
不同场景下 App 收集个人信息的频率参考

表 D.1 给出了 App 在不同场景下收集个人信息的频率参考。

表 D.1 不同场景下 App 收集个人信息的频率参考

个人信息	场景	合理频率	备注
地理位置	地图导航、位置追踪等实时定位场景	持续读取（每秒 1 次）	户外开阔地带，设备 GPS 定位成功后。
	展示周边可用服务等场景	周期性读取（每 30 秒 1 次）	
	识别当前地址等场景	一次性读取（进入功能界面时读取 1 次或者用户主动刷新时读取 1 次）	
通讯录	添加特定通讯录好友、分享特定通讯录联系人、设置特定通讯录联系人为紧急联系人等场景	用户主动触发时读取特定条目 1 次	
	通讯录备份、未知联系人骚扰拦截等场景	用户主动触发时读取或经用户明确授权后在通讯录出现变更时自动读取	
人脸信息	各类人脸识别应用场景	用户主动触发时读取	
应用程序列表	应用管理等场景	用户主动触发时读取	
短信	短信备份、短信骚扰拦截等场景	用户主动触发时读取或经用户明确授权后在接收到新短信时自动读取	
通话记录	通话记录备份	用户主动触发时读取或经用户明确授权后在通话记录变更时自动读取	

参 考 文 献

[1] 《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）
[2] 《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》
[3] 《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》
[4] 《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》
[5] GB/T 34975—2017《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》