ICS 33.030
M 21

YD

中华人民共和国通信行业标准

YD/T 3106–2016

电信和互联网服务
用户个人信息保护技术要求
移动应用商店

Telecom and internetservice technicial requirements for
user personal information protection–Mobile application market

2016–07–11 发布　　2016–10–01 实施

中华人民共和国工业和信息化部　发 布

目　　次

前　言

本标准是“电信和互联网服务 用户个人信息保护”系列标准之一，该系列标准名称和结构预计如下：

— YD/T 2781-2014 电信和互联网服务 用户个人信息保护 定义及分类

— YD/T 2782-2014 电信和互联网服务 用户个人信息保护 分级指南

— YD/T 3106-2016 电信和互联网服务 用户个人信息保护技术要求 移动应用商店

— YD/T 3105-2016 电信和互联网服务 用户个人信息保护技术要求 电子商务服务

— 电信和互联网服务 用户个人信息保护技术要求 即时通信服务

本标准按照GB/T1.1-2009给出的规则起草。

随着技术的发展，还将制定后续的相关标准。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、北京奇虎科技有限公司、北京卓易讯畅科技有限公司、阿里巴巴通信技术（北京）有限公司、中国移动通信集团公司、中国电信集团公司、中国联合网络通信集团有限公司、北京中创网信信息发展有限公司、浙江鹏信信息科技股份有限公司、北京创战纪科技有限公司、小米科技有限责任公司、北京机锋科技有限公司。

本标准主要起草人：葛雨明、顾　伟、傅　彤、刘安逸、汤立波、杨燕琳、许　青、李　成、肖启勇、甄焱鲲、李　娜、黎伟健、王兰芳、高　枫、胡莉琼、刘　旦、杨澄宇、陶波、马　峰、杨在田、于润东、张　平、刘京华。

电信和互联网服务 用户个人信息保护技术要求 移动应用商店

1 范围

本标准规定了移动应用商店服务的用户个人信息保护要求及与用户相关权益保护要求。

本标准适用于移动应用商店。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2781-2014 电信和互联网服务 用户个人信息保护定义及分类

YD/T 2782-2014 电信和互联网服务 用户个人信息保护分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动应用商店 Mobile Application Market

提供移动应用软件分发服务的平台，为用户的移动智能终端提供移动应用软件的展示、搜索、购买、下载、安装、升级和卸载等服务。移动应用商店包括仅提供网页版服务的移动应用商店和具备（PC 或移动智能终端）客户端的移动应用商店。

3.2

移动应用商店客户端 Mobile Application Market Client

实现智能终端移动应用软件分发管理的平台类应用软件，包括安装、运行在 PC 上的移动应用商店 PC 端客户端和安装、运行在智能终端操作系统上的移动应用商店智能终端客户端。

3.3

移动应用软件开发者 Moblieapplication Market Developer

经在移动应用商店平台有效注册、申请后，将其享有相应权利的各种移动应用软件接入移动应用商店平台，向用户提供各种服务的任何公司、单位、个人及其他组织。

4 缩略语

下列缩略语适用于本文件。

IMEI	International Mobile Equipment Identity	移动设备国际身份码
IMSI	International Mobile Subscriber Identificationnumber	国际移动用户识别码
PID	Product ID	产品识别码
SN	Serial Number	设备序列号
VID	Vendor ID	USB 设备供应商 ID

5 移动应用商店用户个人信息保护准则

移动应用商店收集、使用用户个人信息应符合中华人民共和国法律要求，保证用户知情权、选择权，并承担用户个人信息的保护责任。移动应用商店具有平台属性，应依照本标准规定对其提供的移动应用软件收集、使用用户个人信息的行为承担审查与管理责任。

6 移动应用商店服务分级方法

移动应用商店用户个人信息分级的对象是移动应用商店服务。

本标准依据移动应用商店服务过程中收集、转移和使用的用户个人信息要素，确定移动应用商店服务的保护级别，并提出不同级别应用商店服务的用户个人信息保护要求和用户相关权益的保护要求。

用户个人信息的定义及分类见YD/T 2781-2014，用户个人信息保护的分级方法见YD/T 2782-2014

7 移动应用商店用户个人信息保护环节及用户个人信息保护内容

7.1 概述

本标准将对移动应用商店服务涉及的用户个人信息保护相关环节进行描述。

移动应用商店服务的用户个人信息保护环节，如图1所示，可包括：

— 移动应用商店的平台管理，包括用户的注册、登录管理，数据库管理和支付交易管理3个部分；

— 移动应用软件的审查和管理，包括移动应用软件开发者的审查和管理、移动应用软件上架前审查和移动应用软件上架后分发管理；

— 移动应用商店的客户端管理。

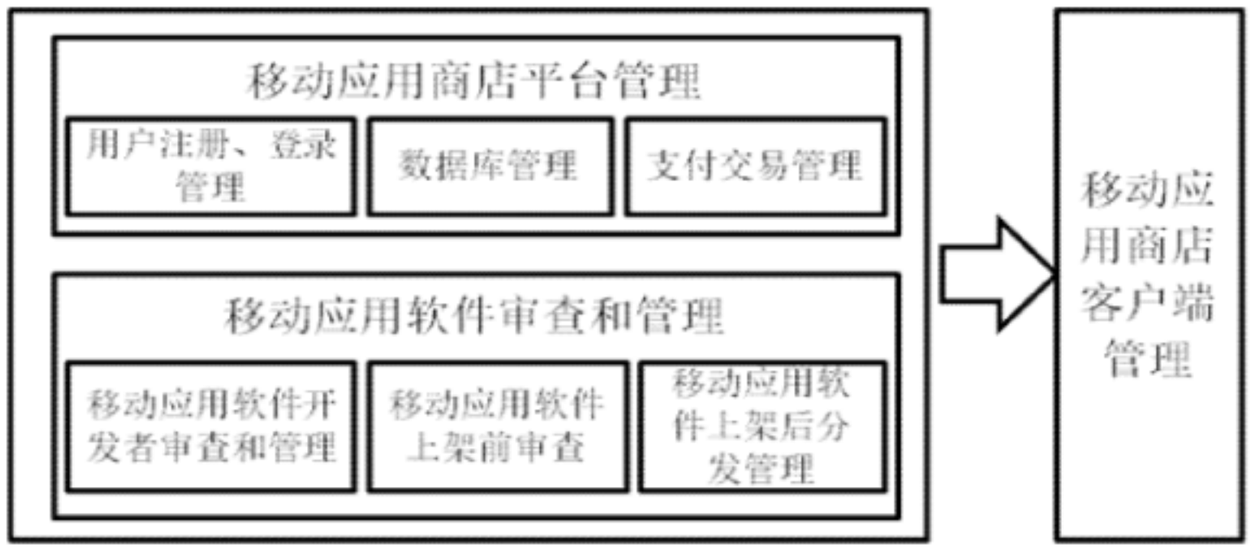

图1 移动应用商店的用户个人信息保护环节示意

仅提供网页版移动应用软件分发服务的移动应用商店，用户个人信息保护环节包括移动应用商店的平台管理、移动应用软件的审查和管理。

具备客户端移动应用软件分发服务的移动应用商店，用户个人信息保护环节包括移动应用商店的平台管理、移动应用软件的审查和管理、移动应用商店的客户端管理。

7.2 移动应用商店的平台管理

7.2.1 用户的注册、登录管理

用户的注册、登录管理涉及用户个人信息可包括：

— 用户基本资料：如姓名、证件类型及号码、年龄、性别、职业、工作单位、地址等；

— 普通用户身份标识和鉴权信息：如电话号码、账号、昵称、登录密码、IP地址、邮箱地址以及服务涉及的密码、口令、密码保护答案等。

7.2.2 数据库管理

数据库管理涉及用户个人信息可包括：

— 交易类服务身份标识和鉴权信息：如交易账号和密码（交易类电子商务服务）、密码保护答案等。

— 用户基本资料：如姓名、证件类型及号码、年龄、性别、职业、工作单位、地址等；

— 普通用户身份标识和鉴权信息：如电话号码、账号、昵称、登录密码、IP地址、邮箱地址等；

— 服务记录和日志：如业务日志、移动应用软件下载记录等；

— 业务订购、订阅关系：如业务订购信息、业务注册时间、修改、注销状况信息等。

7.2.3 支付交易管理

支付交易管理涉及用户个人信息可包括：

— 交易类服务身份标识和鉴权信息：如交易账号和密码（交易类电子商务服务）、密码保护答案等。

7.3 移动应用软件的审查和管理

7.3.1 移动应用软件开发者的审查和管理

移动应用软件开发者的审查和管理用户个人信息可包括：

— 移动应用软件开发者的身份标识和鉴权信息，如个人开发者的个人账号、昵称、登录密码、IP地址、邮箱地址，以及公司、单位组织开发者的营业执照、联系方式等。

7.3.2 移动应用软件上架前审查

移动应用软件上架前，移动应用商店应按照本标准规定对移动应用软件进行必要的审查和检测。

7.3.3 移动应用软件上架后的分发管理

移动应用软件上架后的分发管理涉及移动应用商店内移动应用软件的购买、下载、安装、升级和卸载等服务，用户个人信息可包括：

— 移动应用商店的移动应用软件购买服务涉及交易类服务身份标识和鉴权信息等用户个人信息；

— 移动应用商店的移动应用软件下载服务涉及业务订阅和订购关系、设备信息、服务记录和日志、位置信息等用户个人信息；

— 移动应用商店的移动应用软件安装服务涉及用户虚拟身份和鉴权信息、服务记录和日志、设备信息、位置信息等用户个人信息；

— 移动应用商店的移动应用软件升级服务涉及用户虚拟身份和鉴权信息、设备信息等用户个人信息；

— 移动应用商店的移动应用软件卸载服务涉及用户虚拟身份和鉴权信息等用户个人信息。

7.4 移动应用商店的客户端管理

移动应用商店客户端为了实现对用户移动智能终端移动应用软件的管理，在明确告知并征得用户同意的情况下，移动应用商店会通过客户端收集、使用用户个人信息可包括：

— 服务记录和日志：如业务日志、移动应用软件安装列表等；

— 用户硬件设备信息：如USB设备供应商ID和产品识别码、设备序列号、手机的国际移动设识码、设备型号、手机系统版本号、系统编号、屏幕分辨率、移动智能终端操作系统版本、IP地址、用户网络状态、运营商等；

— 用户位置信息：如用户所在的经纬度、地区代码、小区代码、基站号等。

此外，具备存储数据管理功能的移动应用商店客户端，移动应用商店通过客户端可收集、使用用户服务内容和资料数据等用户个人信息：

— 服务内容信息：如通话内容、短信、彩信等；

— 联系人信息：如通讯录、好友列表、群组列表等用户资料数据；

— 用户私有资料数据：如用户终端、SD 卡等存储的用户文字、多媒体等资料数据信息。

8 移动应用商店用户个人信息保护技术要求

8.1 概述

移动应用商店服务提供方应按照本标准规定的1～5级的用户个人信息保护技术要求对其提供服务过程中涉及的用户个人信息的收集、转移和使用进行规范化管理。

同等级别的移动应用商店服务应当遵循同等程度的用户个人信息保护技术要求。

8.2 第5级移动应用商店用户个人信息保护要求

8.2.1 移动应用商店平台管理的用户个人信息保护要求

8.2.1.1 用户注册、登录管理

用户注册、登录管理环节的用户个人信息保护要求包括：

— 用户基本资料的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 普通用户身份标识和鉴权信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施。

8.2.1.2 数据库管理

数据库管理环节的用户个人信息保护要求包括：

— 用户交易类身份标识和鉴权信息的存储、转移应采取确保数据机密性和完整性的加密措施，应采取严格的访问控制措施，应设置内部数据审批流程及制度，宜对用户个人信息使用进行监控及预警；

— 用户基本资料的存储、转移应采取必要的加密措施，应采取严格的访问控制措施，应设置内部数据审批流程及制度，宜对用户个人信息使用进行监控及预警；

— 普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系的存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.2.1.3 交易支付管理

交易支付管理环节的用户个人信息保护要求包括：

— 用户交易类身份标识和鉴权信息的收集、转移和使用应具有充分的必要性并且征得用户明示同意，存储、转移应采取确保数据机密性和完整性的加密措施；

— 使用第三方支付交易过程中，移动应用商店不得记录用户交易类鉴权信息，不得向第三方泄露与用户特定交易无关的用户个人信息。

8.2.2 移动应用软件审查和管理的用户个人信息保护要求

8.2.2.1 移动应用软件开发者的审查和管理

移动应用软件开发者使用移动应用商店平台分发移动应用软件，应保护用户的知情权、选择权及其他合法权益，遵循软件行为不越界、操作应征得用户明示同意的原则。

移动应用软件开发者应保证向移动应用商店所提供信息的真实性、准确性和及时性。

移动应用软件开发者应保证对外沟通电子邮件及联系人发生变更时及时进行信息更新。

8.2.2.2 移动应用软件上架前的审查

移动应用软件上架前，移动应用商店要对移动应用软件进行必要的审查和检测，包括移动应用软件功能的审查和检测、用户个人信息收集、转移和使用的合规性审查和检测，以及本标准规定的用户权益保护的审查和检测。

a）移动应用软件功能的审查和检测，包括：

— 上架移动应用软件应声明移动应用软件开发者真实身份信息；

— 上架移动应用软件应声明获取用户个人信息的权限，不得申请与移动应用软件功能无关的用户个人信息使用权限；

— 上架移动应用软件获取敏感用户个人信息，应逐条解释敏感信息的用途及原因；

— 未经明确提示和获得用户同意，上架移动应用软件不得包含与软件功能描述不符的隐藏功能；

— 未经明确提示和获得用户同意，上架移动应用软件不得屏蔽用户通信功能；

— 上架移动应用软件应明确标示应用软件内付费的类型。

b）用户个人信息收集、转移和使用的合规性，包括：

— 上架移动应用软件不得未提示用户有收集信息的行为而收集用户个人信息；

— 上架移动应用软件不得篡改用户个人信息；

— 上架移动应用软件对于用户个人信息的转移，应告知用户如何使用信息以及在何处使用信息，应做到转移必加密原则。

c）用户相关权益保护的审查和检测，包括：

— 上架移动应用软件下载安装后在提供功能体验前不得强制要求用户下载其他无关移动应用软件；

— 上架移动应用软件不得存在用户不知情的情况下，后台自动捆绑下载其他应用软件；

— 上架移动应用软件不得存在无法卸载等行为；

— 上架移动应用软件中的弹窗类广告行为应提供一键关闭功能；

— 上架移动应用软件不得强制或误导用户点击广告内容；

— 上架移动应用软件不得在任何不经用户允许的情况下进行任何扣费行为；

— 上架移动应用软件的扣费行为提示应明确、明显，不得以误导方式实现用户付费；

— 应用开发者在上架移动应用软件内的计费点应明确提示用户付费的金额；

— 上架移动应用软件内扣费，应经过用户的二次确认，即用户需要对购买和支付分别进行一次确认。

8.2.2.3 移动应用软件上架后的分发管理

移动应用软件上架后分发管理的用户个人信息保护要求包括：

— 移动应用商店的应用软件购买服务，用户交易类身份标识和鉴权信息的收集、转移和使用应具有充分的必要性并且征得用户明示同意，存储、转移应采取确保数据机密性和完整性的加密措施；

— 移动应用商店的应用软件下载、安装、升级和卸载服务，用户位置信息的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 移动应用商店的移动应用软件下载、安装、升级和卸载服务，普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系、设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施；

— 移动应用商店要对上架后的移动应用软件进行抽样检测，保护技术要求同第8.2.2.2节。

8.2.3 移动应用商店客户端管理的用户个人信息保护要求

移动应用商店客户端管理的用户个人信息保护要求包括：

— 用户位置信息、联系人信息的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 服务内容信息、用户私有资料数据、服务记录和日志、用户硬件设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.3 第4级移动应用商店用户个人信息保护要求

8.3.1 移动应用商店平台管理的用户个人信息保护要求

8.3.1.1 用户注册、登录管理

用户注册、登录管理环节的用户个人信息保护要求包括：

— 用户基本资料的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 普通用户身份标识和鉴权信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施。

8.3.1.2 数据库管理

数据库管理环节的用户个人信息保护要求包括：

— 用户基本资料的存储、转移应采取必要的加密措施，应采取严格的访问控制措施，应设置内部数据审批流程及制度，宜对用户个人信息使用进行监控及预警；

— 普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系的存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.3.2 移动应用软件审查和管理的用户个人信息保护要求

8.3.2.1 移动应用软件开发者的审查和管理

移动应用软件开发者使用移动应用商店平台分发移动应用软件，应保护用户的知情权、选择权及其他合法权益，遵循软件行为不越界、操作应征得用户明示同意的原则。

移动应用软件开发者应保证向移动应用商店所提供信息的真实性、准确性和及时性。

移动应用软件开发者应保证对外沟通电子邮件及联系人发生变更时及时进行信息更新。

8.3.2.2 移动应用软件上架前的审查

移动应用软件上架前，移动应用商店要对移动应用软件进行必要的审查和检测，包括移动应用软件功能的审查和检测、用户个人信息收集、转移和使用的合规性审查和检测，以及本标准规定的用户权益保护的审查和检测。

a）移动应用软件功能的审查和检测，包括：

— 上架移动应用软件应声明移动应用软件开发者真实身份信息；

— 上架移动应用软件应声明获取用户个人信息的权限，不得申请与移动应用软件功能无关的用户个人信息使用权限；

— 上架移动应用软件获取敏感用户个人信息，应逐条解释敏感信息的用途及原因；

— 未经明确提示和获得用户同意，上架移动应用软件不得包含与软件功能描述不符的隐藏功能；

— 未经明确提示和获得用户同意，上架移动应用软件不得屏蔽用户通信功能；

— 上架移动应用软件应明确标示应用软件内付费的类型。

b）用户个人信息收集、转移和使用的合规性，包括：

— 上架移动应用软件不得未提示用户有收集信息的行为而收集用户个人信息；

— 上架移动应用软件不得篡改用户个人信息；

— 上架移动应用软件对于用户个人信息的转移，应告知用户如何使用信息以及在何处使用信息，应做到转移必加密原则。

c）用户相关权益保护的审查和检测，包括：

— 上架移动应用软件下载安装后在提供功能体验前不得强制要求用户下载其他无关移动应用软件；

— 上架移动应用软件不得存在用户不知情的情况下，后台自动捆绑下载其他应用软件；

— 上架移动应用软件不得存在无法卸载等行为；

— 上架移动应用软件中的弹窗类广告行为应提供一键关闭功能；

— 上架移动应用软件不得强制或误导用户点击广告内容；

— 上架移动应用软件不得在任何不经用户允许的情况下进行任何扣费行为；

— 上架移动应用软件的扣费行为提示应明确、明显，不得以误导方式实现用户付费；

— 应用开发者在上架移动应用软件内的计费点应明确提示用户付费的金额；

— 上架移动应用软件内扣费，应经过用户的二次确认，即用户需要对购买和支付分别进行一次确认。

8.3.2.3 移动应用软件上架后的分发管理

移动应用软件上架后分发管理的用户个人信息保护要求包括：

— 移动应用商店的应用软件下载、安装、升级和卸载服务，用户位置信息的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 移动应用商店的移动应用软件下载、安装、升级和卸载服务，普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系、设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施；

— 移动应用商店要对上架后的移动应用软件进行抽样检测，保护技术要求同8.3.2.2节。

8.3.3 移动应用商店客户端管理的用户个人信息保护要求

移动应用商店客户端管理的用户个人信息保护要求包括：

— 用户位置信息、联系人信息的收集、转移和使用应征得用户明示同意，存储、转移应采取必要的加密措施；

— 服务内容信息、用户私有资料数据、服务记录和日志、用户硬件设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.4 第3级移动应用商店用户个人信息保护要求

8.4.1 移动应用商店平台管理的用户个人信息保护要求

8.4.1.1 用户注册、登录管理

用户注册、登录管理环节的用户个人信息保护要求包括：

— 普通用户身份标识和鉴权信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施。

8.4.1.2 数据库管理

数据库管理环节的用户个人信息保护要求包括：

— 普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系的存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.4.2 移动应用软件审查和管理的用户个人信息保护要求

8.4.2.1 移动应用软件开发者的审查和管理

移动应用软件开发者使用移动应用商店平台分发移动应用软件，应保护用户的知情权、选择权及其他合法权益，遵循软件行为不越界、操作应征得用户明示同意的原则。

移动应用软件开发者应保证向移动应用商店所提供信息的真实性、准确性和及时性。

移动应用软件开发者应保证对外沟通电子邮件及联系人发生变更时及时进行信息更新。

8.4.2.2 移动应用软件上架前的审查

移动应用软件上架前，移动应用商店要对移动应用软件进行必要的审查和检测，包括移动应用软件功能的审查和检测、用户个人信息收集、转移和使用的合规性审查和检测，以及本标准规定的用户权益保护的审查和检测。

a）移动应用软件功能的审查和检测，包括：

— 上架移动应用软件应声明应用软件开发者真实身份信息；

— 上架移动应用软件应声明获取用户个人信息的权限，不得申请与移动应用软件功能无关的用户个人信息使用权限；

— 上架移动应用软件获取敏感用户个人信息，应逐条解释敏感信息的用途及原因；

— 未经明确提示和获得用户同意，上架移动应用软件不得包含与软件功能描述不符的隐藏功能；

— 未经明确提示和获得用户同意，上架移动应用软件不得屏蔽用户通信功能；

— 上架移动应用软件应明确标示应用软件内付费的类型。

b）用户个人信息收集、转移和使用的合规性，包括：

— 上架移动应用软件不得未提示用户有收集信息的行为而收集用户个人信息；

— 上架移动应用软件不得篡改用户个人信息；

— 上架移动应用软件对于用户个人信息的转移，应告知用户如何使用信息以及在何处使用信息，应做到转移必加密原则。

c）用户相关权益保护的审查和检测，包括：

— 上架移动应用软件下载安装后在提供功能体验前不得强制要求用户下载其他无关移动应用软件；

— 上架移动应用软件不得存在用户不知情的情况下，后台自动捆绑下载其他应用软件；

— 上架移动应用软件不得存在无法卸载等行为；

— 上架移动应用软件中的弹窗类广告行为应提供一键关闭功能；

— 上架移动应用软件不得强制或误导用户点击广告内容；

— 上架移动应用软件不得在任何不经用户允许的情况下进行任何扣费行为；

— 上架移动应用软件的扣费行为提示应明确、明显，不得以误导方式实现用户付费；

— 应用开发者在上架移动应用软件内的计费点应明确提示用户付费的金额；

— 上架移动应用软件内扣费，应经过用户的二次确认，即用户需要对购买和支付分别进行一次确认。

8.4.2.3 移动应用软件上架后的分发管理

移动应用软件上架后分发管理的用户个人信息保护要求包括：

— 移动应用商店提供的移动应用软件下载、安装、升级和卸载服务，普通用户身份标识和鉴权信息、服务记录和日志、业务订购和订阅关系、设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施；

— 移动应用商店要对上架后的移动应用软件进行抽样检测，保护技术要求同8.4.2.2节。

8.4.3 移动应用商店客户端管理的用户个人信息保护要求

移动应用商店客户端管理的用户个人信息保护要求包括：

— 服务内容信息、用户私有资料数据、服务记录和日志、用户硬件设备信息的收集、转移应征得用户明示同意，存储、转移应采取必要的加密措施，必要的访问控制措施，必要的安全管理规范。

8.5 第2级移动应用商店用户个人信息保护要求

不作要求。

8.6 第1级移动应用商店用户个人信息保护要求

不作要求。