ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 34978—2017

# 信息安全技术　移动智能终端个人信息保护技术要求

**Information security technology—Technology requirements for personal information protection of smart mobile terminal**

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:浙江长天信息技术有限公司、浙江省经济和信息化委员会、成都网安科技发展有限公司、中国软件评测中心、工业和信息化部电子工业标准化研究院、中国信息安全测评中心。

本标准主要起草人:高洁原、高炽扬、罗锋盈、高子鹏、王坤、张华熊、刘法旺、刘陶、杨建军、郭颖。

# 引　言

随着移动互联网的快速发展和移动智能终端的广泛应用，移动智能终端个人信息在人们的社会、经济活动中的地位日益凸显，滥用个人信息的现象也随之出现，给社会秩序和个人切身利益带来了危害。为促进移动智能终端个人信息的合理利用，指导和规范利用移动智能终端处理个人信息的活动，制定本标准。

# 信息安全技术　移动智能终端个人信息保护技术要求

## 1　范围

本标准规定了移动智能终端的个人信息分类及个人信息的保护原则和技术要求。

本标准适用于指导公共及商业用途的移动智能终端进行个人信息的处理，其他有关各方也可参照使用。

## 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。

GB/Z 28828—2012　信息安全技术　公共及商用服务信息系统个人信息保护指南

## 3　术语、定义和缩略语

### 3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

**移动智能终端　smart mobile terminal**

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件的手持或便携设备。

3.1.2

**移动智能终端应用程序　smart mobile terminal application**

安装在移动智能终端设备上，能够利用移动智能终端设备上操作系统提供的开发接口，实现某项或某几项特定任务的计算机程序。

3.1.3

**移动智能终端个人信息　smart mobile terminal personal information**

可为移动智能终端中操作系统或应用软件所处理、与移动智能终端用户相关，且能够单独或通过与其他信息相结合使用，从而识别该移动智能终端用户的数据信息。

3.1.4

**个人信息主体　subject of personal information**

个人信息指向的自然人。

3.1.5

**明示同意　expressed consent**

个人信息主体明确授权同意，并保留证据。

### 3.2　缩略语

下列缩略语适用于本文件。

API:应用程序编程接口(Application Programming Interface)
IMEI:国际移动设备身份码(International Mobile Equipment Identity)
UDID:唯一设备识别符(Unique Device Identifier)

## 4 移动智能终端个人信息分类

### 4.1 概述

移动智能终端个人信息主要包含通信信息、日志信息、账户信息、金融支付信息、传感采集信息、设备信息和文件信息共七大类别,涉及了包括移动智能终端设备系统固有、用户存储及应用程序生成等各类个人信息数据。

### 4.2 个人信息分类

4.2.1 通信信息是指移动智能终端用户用于发起或接受通信以及在通信过程中所产生的数据信息。包括通讯录、通讯记录、短信、彩信、邮件、即时通信消息等。
4.2.2 日志信息是指移动智能终端用户通过使用应用程序而记录的与时间相关的事件信息,或由应用程序产生的以时间为检索条件的使用记录或缓存数据。
4.2.3 账户信息是指移动智能终端应用程序在注册或登录时需要填写的信息,以及移动智能终端中各应用程序所存储的个人账号相关信息。
4.2.4 金融支付信息是指移动智能终端用户借助终端参与金融交易或支付活动而产生的数据信息。包括交易验证码、动态口令等。
4.2.5 传感采集信息是指利用移动智能终端传感器设备所采集到的、能反映移动智能终端设备用户的周边环境和身份特征的数据信息。包括地理位置信息、指纹信息等。
4.2.6 设备信息是指可标识移动智能终端唯一性的数据信息。包括 IMEI、UDID 等。
4.2.7 文件信息是指存储在移动智能终端设备存储介质中的数据信息。包括照片、音频、视频、文本等各种类型文件数据。

## 5 移动智能终端个人信息保护原则

在对移动智能终端个人信息进行处理时,一般应按 GB/Z 28828—2012 中 4.2 的要求,遵循其目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确八项原则合理的利用个人信息。

## 6 移动智能终端个人信息保护技术要求

### 6.1 概述

在移动智能终端个人信息的处理过程中可分为收集、加工、转移和删除四个主要环节。对个人信息的保护贯穿于四个阶段中:

a) 收集阶段是指移动智能终端系统和应用程序对设备中个人信息的提取和记录。
b) 加工阶段是指移动智能终端系统和应用程序对收集到的个人信息进行的操作处理,如录入、存储、修改、标注等。
c) 转移阶段是指移动智能终端系统和应用程序对收集和处理的个人信息进行发送和传输,从而将个人信息转移复制到其他信息系统。

d) 删除阶段指使移动智能终端个人信息在收集、加工处理和传输存储过程结束后，个人信息不再可用时应删除相应数据。

## 6.2 个人信息收集阶段

6.2.1 移动智能终端操作系统应对系统资源的调用进行监控、保护和提醒，确保涉及收集个人信息的行为总是在受控的状态下，不会造成出现用户不可控的行为的执行。

6.2.2 移动智能终端系统和应用程序，在通过调用操作系统或其他安装的第三方软件系统提供的 API 接口收集个人信息时，应告知用户，让用户知晓当前操作会收集个人信息的种类，以及收集的个人信息的用途。

6.2.3 在收集个人信息过程中，移动智能终端系统和应用程序只应收集能够达到已告知目的的最少信息。

6.2.4 持续收集个人信息时，应允许移动智能终端用户配置、调整或关闭个人信息收集功能。

6.2.5 移动智能终端系统和应用程序不应该采取隐蔽手段或以间接方式收集个人信息。

6.2.6 收集涉及个人敏感信息和身份特征的个人信息数据时应采用明示同意的告知许可方式。

6.2.7 收集阶段的告知提醒，应明确一个时间有效期，包括一段时间或长期等。

6.2.8 个人信息收集方在收集阶段进行告知提醒时，应提供对个人信息进行全过程安全保护的证据。

## 6.3 个人信息加工阶段

6.3.1 移动智能终端系统和应用程序在对个人信息进行加工处理时，应告知加工目的、方法或手段。

6.3.2 不对收集阶段告知范围以外的个人信息数据进行加工处理。

6.3.3 保证个人信息在加工处理过程中的安全性，在整个过程中个人信息不应被三方无关人员或组织获知，过程数据和结果数据都应加密处理，且加密处理方式和强度应符合公共或商用标准。

6.3.4 移动智能终端系统和应用程序对个人信息进行加工处理时，应保证系统稳定运行，不造成个人信息的损毁、泄露和丢失等，加工过程完毕时应进行数据完整性和正确性检查。

6.3.5 移动智能终端中个人信息加工处理过程应可控，移动智能终端设备用户可配置、调整或关闭加工过程。

6.3.6 移动智能终端系统和应用程序的设计者或开发者不应该在加工过程中采取隐蔽手段挖掘和分析归纳用户的身份特征数据。

## 6.4 个人信息转移阶段

6.4.1 移动智能终端系统和应用程序在进行个人信息数据传输转移时，应告知移动智能终端设备用户当前个人信息转移的目的、转移信息的获得者、转移数据的使用范围。

6.4.2 不对收集阶段告知范围以外的个人信息数据进行转移处理。

6.4.3 基于最少够用的原则，对于在本地加工处理能满足功能需求的个人信息数据，则不需要进行数据的传输转移。

6.4.4 通讯数据和环境数据类等涉及个人敏感信息或身份特征的个人信息，经移动智能终端设备用户同意授权后才可转移。

6.4.5 个人信息的数据转移过程应保证所转移数据的安全性、完整性及正确性，转移或转存的个人信息数据其过程和结果都应进行加密处理，且加密处理方式和强度应符合公共或商用标准。

6.4.6 个人信息数据的转移过程应可控，移动智能终端设备用户可对当前转移操作进行配置、调整或关闭操作。

## 6.5 个人信息删除阶段

6.5.1 移动智能终端系统和应用程序对收集、加工、转移阶段所使用的个人信息的缓存数据，应该提供

自动删除或者手动删除功能。

6.5.2 移动智能终端系统和应用程序提供的删除功能应该具备数据彻底删除能力，以保证被删除的个人信息数据不可被恢复。

6.5.3 移动智能终端设备遗失或被盗时，移动智能终端系统和应用程序应确保原设备中的个人信息数据可以被远程销毁。

## 参 考 文 献

[1] YD/T 2407—2013 移动智能终端安全能力技术要求