

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 47469-2026

**Data security technology - Management guidance for smart
mobile terminals on the personal information processing
activities of mobile internet applications**

数据安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南

Issued on: April 30, 2026

Implemented on: November 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

5 General Principles

7.2 Transparent Display

7.3 Management of Personal Information Processing Behavior

7.4 App Lifecycle Management

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1. Structure and Drafting Rules of Standardization Documents". Drafting. Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Huawei Technologies Co., Ltd., China Electronics Technology Standardization Institute, and National Computer Network Emergency Response Technical Team/Coordination Center. Coordination Center, China Cybersecurity Review, Certification and Market Supervision Big Data Center, Bodin Shihua (Beijing) Technology Co., Ltd., OPPO Guangdong Mobile Communications Corporation Limited, Vivo Mobile Communications Co., Ltd., Ant Group Co., Ltd., Beijing Baidu Netcom Technology Co., Ltd. Tongdun Technology Co., Ltd., Zhengzhou Xinda Jiean Information Technology Co., Ltd., Beijing Qihoo Technology Co., Ltd., Beijing Kuaishou Technology Co., Ltd. The company, Daily Interactive Co., Ltd., Beijing Momo Technology Co., Ltd., Beijing Shuanxing Technology Co., Ltd., and Wuhan Antiy Information Technology Co., Ltd. Limited Liability Company, Venustech Information Technology Group Co., Ltd., Beijing Wodong Tianjun Information Technology Co., Ltd., Guangdong Midea Refrigeration Equipment Equipment Co., Ltd., Alibaba (Beijing) Software Service Co., Ltd. The main drafters of this document are. Yi Qiang, Hu Ying, Fan Hua, Ren Yan, He Yanzhe, Xue Chen, Liu Xing, Zhou Chenwei, Zhu Xuefeng, Dou Yu, and Zhang Bowen. Yang Minghui, Dong Ji, Li Teng, Jia Ke, Zhang Wei, Liu Xianlun, Yao Yinan, Lin Guanchen, Shi Yuzhen, Guo Jianling, Deng Ting, Tan Cheng, Zhao Feng, Ren Haifeng Luo Hongwei, Wang Xin, Dong Lin, Ye Xinjiang, Ji Shuai, Liu Yuhong, Chen Jialin, Yu Lina, Shi Jing, Zhai Shijun, Li Ran, Qi Jinye, Huang Tianning, Liu Aijing.

With the rapid development of the mobile internet, while mobile internet applications have brought convenience to people's lives, they have also posed challenges such as the collection of personal information. The problem lies in the collection and improper use of

mobile smart terminals. As the carrier of mobile internet applications, mobile smart terminals provide processing capabilities for these applications. A management mechanism for personal information on mobile smart terminals can effectively promote the reasonable collection and use of personal information by mobile internet applications. Personal information. To protect the legitimate rights and interests of mobile smart terminal users, this document, based on the fundamental principles of user awareness and control, proposes personal protection guidelines for mobile smart terminals. Information protection management measures to enhance the level of personal information protection in mobile internet applications. Data security technology for mobile smart terminals Internet application (App) personal information processing Event Management Guide

1.Scope This document provides recommendations for personal information protection management measures for mobile smart terminals. This document is intended to guide mobile smart terminal providers in designing and developing personal information protection features.

4.Abbreviations The following abbreviations apply to this document. App. Application IMEI. International Mobile Equipment Identity MAC. Media Access Control WLAN. Wireless Local Area Network

5 General Principles

5.1 Scope of Personal Information on Mobile Smart Terminals Mobile smart terminal personal information refers to the personal information that an app can obtain through a mobile smart terminal, including information stored on the mobile smart terminal device. Personal information stored or collected through mobile smart terminal devices, such as contacts, call logs, text messages, and media information (such as pictures, audio, and video). (Frequency), device identifier, local number, application list, location, network access information, etc.

5.2 Basic Principles for Personal Information Security Management of Mobile Smart Terminals The principles for managing personal information on mobile smart terminals include.

- a) User awareness. The App records and notifies the User of the processing of personal information on the mobile smart terminal in a reasonable manner, so that the User has a clear understanding of the App's processing methods. The behavior of processing personal information on mobile smart terminals can be used to determine this;
- b) User controllability. Provides a mechanism for users to manage their personal information on mobile smart terminals, allowing users to either allow or refuse access to their personal information. deal with;
- c) Security Measures. Provide security mechanisms such as secure storage for personal information processed by the App on mobile smart terminals to prevent attackers from

accessing the app. Attacking mobile smart terminals by means of tampering or theft;

d) Meticulous Management. Implementing fine-grained management measures for sensitive personal information on mobile smart terminals;

e) Appropriate Management. Mobile smart terminals shall manage personal information on mobile smart terminals using reasonable means to avoid interfering with users and negatively impacting their lives. To ensure the normal operation of the app;

f) Clear rules. The rules for managing personal information on mobile smart terminals must be clear and explicit.

6. Personal Information Security Risks of Mobile Smart Terminals The main risks to personal information security on mobile smart terminals include the following.

a) Risk of misuse of personal information due to collection without user knowledge. Apps running on mobile smart terminals may collect personal information in an unreasonable manner. Collecting personal information from mobile smart terminals without the user's knowledge or consent in business scenarios, and without the mobile smart terminal providing the user with [certain information/resources]. Effective prompts or behavior display mechanisms.

b) Risk of harm to user rights due to users' weak control over their personal information. Mobile smart terminals do not protect users' personal information. The lack of effective control measures prevents apps from collecting users' personal information beyond their scope or frequency, or from engaging in coercion, inducement, or fraud. The risk of users consenting to the collection of personal information from mobile smart terminals is increasing, which infringes on users' personal information rights.

c) Personal information security risks arising from key stages of the App lifecycle. Apps running on mobile smart terminals, their installation, launch... The processes of updating, uninstalling, and other operations on mobile smart terminals may pose security risks to personal information, including but not limited to. 1) During the installation phase, an app that poses a risk of stealing user personal information was installed without the user's authorization; 2) During the startup phase, the app may automatically start or be launched by an associated entity without the user's knowledge, potentially resulting in the app not being used after startup. Risks associated with users consenting to the processing of their personal information; 3) During the update phase, the app may introduce vulnerabilities or viruses, leading to the risk of unauthorized collection and use of personal information; 4) If personal information is not deleted in time during the uninstallation process, there is a risk that the personal information may be maliciously used by other apps.

7. Measures for the Management of Personal Information Processing on Mobile Smart Terminals

7.1 Classification of Management Measures for Personal Information Processing on Mobile

Smart Terminals Based on the different levels of personal information protection for mobile smart terminals, the management measures for processing personal information on mobile smart terminals are divided into two categories. There are two levels. Basic and Enhanced. Enhanced management measures are indicated in bold.

7.2 Transparent Display

7.2.1 Notice Regarding the Collection and Use of Personal Information During periods when an app continuously or frequently requests permissions that allow the collection of personal information (such as microphone, camera, and location permissions), the mobile smart terminal... Prompt users through methods such as displaying icons. When displaying icons, the following elements should be considered.

- a) Display method. Displayed in a prominent position on the screen, including but not limited to the status bar at the top of the screen, a colored icon in the corner, or a drop-down menu. Column display, etc.;
- b) Timing of notification display. When the app is running in the foreground and background, the user is notified that the app is using permissions that allow the collection of personal information;
- c) Brief Explanation of Logo Meaning. Provide users with a brief explanation of the logo's meaning;
- d) Permission Query and Adjustment. Allows users to query the names of apps that are currently using permissions to collect personal information, and to grant permissions accordingly. The status needs to be adjusted.

Note. Frequent calls refer to calls made at short intervals, resulting in a continuous call effect.

7.2.2 Records of Personal Information Collection and Use Mobile smart terminals record the personal information collected and used by apps, and provide statistical and query interfaces for users. The system provides a clear overview of how personal information is collected and used, and the behavioral records take into account the following factors.

- a) Recorded actions include, but are not limited to. 1) Read location information, read contacts, read media information (such as pictures, audio and video), read text messages, and read biometric information. Data collection, reading unique device identifiers (such as IMEI, WLAN MAC address), reading call logs, accessing the microphone, Camera, background screenshot/screen recording behavior; 2) App auto-start and associated startup behaviors; 3) Record the behavior of reading the application list and reading clipboard information.
- b) Display of recorded information, including but not limited to. 1) When statistics are based on total volume, the displayed information includes the App name, the behavior name, and