MIUI 12
PRIVACY WHITE PAPER

November 2021

Statements

This document should be used as a reference guide for users of Xiaomi products and services to understand the privacy protection of the applications and services in MIUI, our Android-based smartphone system. Xiaomi provides the corresponding introductions based on the current MIUI version for overseas markets and the main hardware architecture in service. Please note that the Xiaomi Privacy Policy is the basis for this white paper. Where this document and our privacy policy differ, the privacy policy shall prevail. However, due to potential problems such as technological upgrades, product iteration, changes to applicable laws and regulations, and consistency of wording, Xiaomi explicitly declares that it makes no express or implied guarantee for the completeness, accuracy, and applicability of the contents herein.

For reasons relating to the upgrade and adjustment of Xiaomi products or services, the contents of this document may change. Xiaomi has the right to add, modify, delete, and abolish such contents without your consent. Please download the latest version from our official website. If you find errors in this document or have any questions about its contents, please contact us via Xiaomi Privacy Support.

Contents

01

Overview

Overview

Xiaomi is dedicated to providing amazing products and services so that everyone can enjoy a better life through innovative technology. In an era of intelligent interconnectedness, Xiaomi attaches great importance to privacy protection. To protect users' privacy, we adopt the concept of privacy by design in the product development process, and consistently try to use more innovative technologies and methods.

It is important that our users know what information we collect and why, and how it's used. We believe that publicizing our data collection and usage practices paves the way for Xiaomi to become a more trustworthy company than ever before. Therefore, we have prepared this MIUI Privacy White Paper (‘White Paper’) to summarize our general privacy practices.

Adhering to the principles of objectivity and transparency, this White Paper provides a more comprehensive introduction to the privacy protection practices and the typical privacy features in MIUI, as well as detailed privacy-related information about the main apps and services in MIUI.

The following is a brief introduction to this White Paper.

Chapter 1 – The Summary introduces the purpose and structure of this White Paper. This chapter establishes the preliminary concept of this White Paper and provides general information about each chapter in this White Paper.

Chapter 2 – Privacy Governance introduces Xiaomi's privacy governance principles. This chapter explains that Xiaomi has built a mature privacy governance and management system, which lays a solid foundation for privacy protection.

Chapter 3 – MIUI Privacy Features introduces the main privacy features in MIUI. This chapter introduces the functions and features provided by MIUI to help you manage and protect your privacy.

Chapter 4 – MIUI Apps and Privacy introduces the privacy practices covering the main system applications and components in the MIUI system. This chapter provides information about data collection and usage by the aforementioned applications, user controls for privacy, and other related information. To provide a simple, clear statement and to improve the understanding of our data collection and usage practice, we refer to many of the concepts in ISO/IEC 19944-1:2020 Cloud computing and distributed platforms — Data flow, data categories and data use — Part 1: Fundamentals, including data taxonomy, data use statements, and corresponding examples. Reference to the ISO standard provides additional clarity about our data collection and usage practice, and allows easy comparison with other products or services that also reference the standard.

Chapter 5 – International Data Transfer introduces our international data storage and transfer practice. This chapter details our cloud service providers, user data storage locations, and our compliance mechanism for international data transfer.

Chapter 6 – Security and Privacy Certifications introduces the security and privacy certifications we have obtained, indicating our outstanding privacy protection capabilities.

Chapter 7 – The Conclusion summarizes the purpose and main content of this White Paper.

We strive for greater transparency with this White Paper and hope that all Xiaomi users, developers, partners, and relevant regulatory authorities can better understand Xiaomi's privacy practices.

02

Privacy at Xiaomi

2.1 Privacy Governance

In 2014, Xiaomi established the Information Security and Privacy Committee and appointed a Chief Privacy Officer to manage and coordinate information security and privacy affairs across the company. Xiaomi adopts a cross-functional approach to privacy governance. Chaired by the Vice President, the committee consists of members from the Information Security and Privacy, Legal, Internal Audit and Supervision, Corporate Communications, and Human Resources teams, and all the company's business units, including but not limited to smartphones, IoT products, software and Internet services, e-commerce, and sales and services. The committee is responsible for creating and maintaining the information security and privacy management system, setting and implementing privacy principles and standards, conducting privacy impact assessments, and overseeing and managing privacy risks at all stages of product development and operations, as well as developing and promoting privacy enhancement technologies.

Following the ISO/IEC 27701:2019 Privacy Information Management System (PIMS), Xiaomi has established a privacy protection framework that covers user communication, user data rights, data governance, data life cycle management, risk identification, security protection measures, and incident response. We strive to establish rigorous, standardized, and progressive internal privacy compliance review procedures and processes to ensure that our products and services meet our privacy protection standards. Every Xiaomi product or service available on the market has undergone a privacy impact assessment internally, which examines such aspects as data collection, storage, use, and destruction.

We provide users with a copy of our Privacy Policy and seek their consent when they use our products or services for the first time. We also provide choices and controls for users to manage their data.

We are committed to keeping your personal information secure. To prevent unauthorized access, disclosure, or other similar risks, we have put in place industry-recognized physical, electronic, and managerial procedures to safeguard and secure your information.

All our employees receive general information security privacy training and assessment every year, where they learn about security and privacy protection concepts and practices. We also provide various professional privacy training courses, covering privacy laws, management, and technology for our engineers, specialists, and professionals in different departments. Since 2020, we have also hosted Information Security and Privacy Awareness Month every year to raise security and privacy awareness among our employees and affiliates.

Our employees and our business partners and third-party service providers who access your personal information are subject to contractual confidentiality obligations.

We conduct due diligence on business partners and third-party service providers to ensure that they can protect your personal information.

We care about protecting your personal information and try to minimize any personal data breaches, which we address in compliance with applicable data protection laws. Our responses include, where required, providing notice of the breach to the relevant data protection or supervisory authority and data subjects affected by the breach.

We have obtained ISO/IEC 27001, ISO/IEC 27018, and ISO/IEC 27701 certifications, as well as the TRUSTe Enterprise Privacy certifications. We also carry out third-party audits to maintain these certifications every year.

2.2 Privacy Principles

Protecting users' privacy is our top priority. Our five privacy principles are the fundamentals of our privacy protection practices. Following the privacy principles, we adopt the concept of privacy by design in our product development process.

Transparency	We strive to be transparent about our data processing practices so you can make informed choices.
Accountability	We hold ourselves accountable for privacy protection by building a privacy culture in the company and establishing an effective privacy management system, consisting of organization, standards, and process.
Control	We seek to provide you with simple and easy-to-use methods to help you manage your information.
Security	We are dedicated to building systems and processes designed to secure and protect your personal information.
Compliance	We are committed to designing and developing our products to reflect data protection principles embodied in current privacy and data security laws and standards.

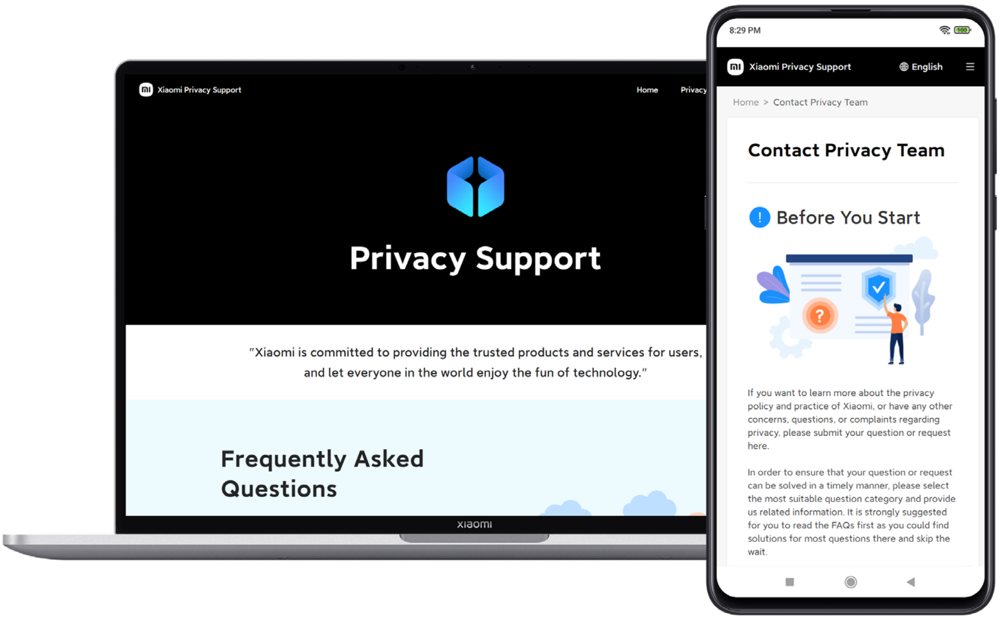
2.3 Privacy Policy

Xiaomi's Privacy Policy explains how Xiaomi collects, uses, processes, discloses, and protects personal data collected from users. Our Privacy Policy consists of a **General Privacy Policy (‘**Xiaomi Privacy Policy**’)**, and a **Separate Privacy Policy** for a specific product or service. The General Privacy Policy applies to all Xiaomi devices, websites, or apps that reference or link to it, while the Separate Privacy Policy only applies to the specific product or service. If a Xiaomi product provides a Separate Privacy Policy, the Separate Privacy Policy will govern that product, while anything not specifically covered is subject to the General Privacy Policy.

We review our Privacy Policy periodically and may update it. If we make a material change to this Privacy Policy, we will notify you via email, publish the change on Xiaomi websites, or notify you via your mobile device. Where required by law, we will ask for your explicit consent when we collect additional personal information from you or when we use or disclose your personal information for new purposes.

2.4 User Requests and Complaints

We provide various tools and methods for users to exercise their data rights. Users can apply to access, correct, or delete the data collected by visiting Xiaomi Privacy Support. We also receive and respond to comments, questions, and complaints from users. See [Figure 2-1 Xiaomi Privacy Support Portal].



Privacy Support

"Xiaomi is committed to providing the trusted products and services for users, and let everyone in the world enjoy the fun of technology."

Frequently Asked Questions

Contact Privacy Team

Before You Start

If you want to learn more about the privacy policy and practice of Xiaomi, or have any other concerns, questions, or complaints regarding privacy, please submit your question or request here.

In order to ensure that your question or request can be solved in a timely manner, please select the most suitable question category and provide us related information. It is strongly suggested for you to read the FAQs first as you could find solutions for most questions there and skip the wait.

Figure 2-1 Xiaomi Privacy Support Portal

2.5 Transparency Report

We respond to personal information requests for legitimate purposes from government agencies and authorities. We endeavor to balance the responsibility to respect our users' right to privacy with our legal obligations to disclose certain user information when requested by government agencies and authorities. We publish the Xiaomi Transparency Report to provide information about the personal information requests we receive every year.

03

Privacy Features in MIUI 12

3.1 Introduction

MIUI is designed and developed to protect your privacy and includes various privacy features to help you keep your information private and secure, protect your data, and manage the apps running on your smartphone. Below we summarize some of the key privacy features in MIUI 12. You can learn more about the security and privacy features of MIUI 12 by visiting the Official MIUI Website.

3.2 Permission Settings

Control what apps are allowed to do

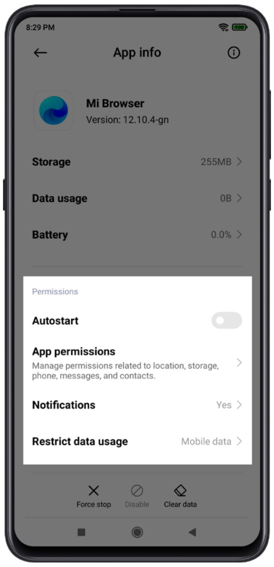
MIUI allows you to manage autostart, app permissions and notifications, restrict data usage, and clear local app data or the cache on your smartphone. You can manage and change your settings at any time[1]. See [Figure 3–1 Permission Settings]

To access this feature, go to Settings > Apps > Manage apps, and select an app to see the App info tab.

3.3 Secure Photo Sharing

Share without oversharing

Photos taken with digital devices usually contain location information and other sensitive metadata (e.g. the time the photo was taken and the specs of your device). In MIUI 12, you can choose to remove this information when you share photos from Gallery or File Manager. See [Figure 3–2 Secure Photo Sharing]



8:29 PM

App info

Mi Browser
Version: 12.10.4-gn

Storage 255MB

Data usage 0B

Battery 0.0%

Permissions

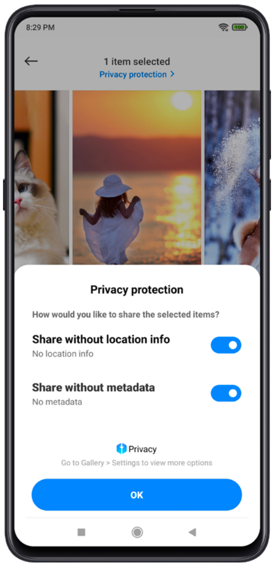
Autostart

App permissions
Manage permissions related to location, storage, phone, messages, and contacts.

Notifications Yes

Restrict data usage Mobile data

Figure 3–1 Permission Settings



8:29 PM

1 item selected
Privacy protection >

Privacy protection

How would you like to share the selected items?

Share without location info
No location info

Share without metadata
No metadata

Privacy
Go to Gallery > Settings to view more options

Figure 3–2 Secure Photo Sharing

[1] Autostart refers to the process whereby an application uses certain system mechanisms to start by itself without the user's active operation. Some autostart is necessary to achieve certain functions you need. However, other autostarts often do not suit your needs, and may cause performance loss or security and privacy risks.

Some system apps may not be subject to these controls, and the scope of such apps is strictly controlled. For example, the Security Center is a system application that protects the security of the operating system running on your smartphone. Many security checks and defense mechanisms rely on this application, so the auto-start for Security Center is mandatory.

3.4 Private Spaces

Keep private things in a place of their own.

MIUI provides you with a series of private spaces in Messaging, Gallery, and File Manager. You can access messages that contain private contacts, as well as private photos, videos, and files, only by entering the privacy protection password or verifying your fingerprint. You can also decide whether notifications about private messages should be displayed in the Notification shade. See [Figure 3-3 Private Spaces]

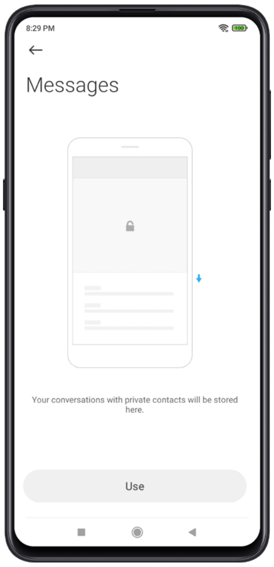
To access this feature, go to Settings > Passwords & security > Privacy protection.

3.5 Find or Lock a Lost Device

Protect your data when at risk

MIUI lets you find your lost device and control it. This is designed to help you further protect your data. You can locate your phone, mark it as lost, or erase data remotely in the Xiaomi Cloud. A phone marked as lost is under your control, even if it is wiped or restored to factory settings. See [Figure 3-4 Find or Lock a Lost Device]

To access this feature, go to Settings > Mi Account > Xiaomi Cloud > Find device.

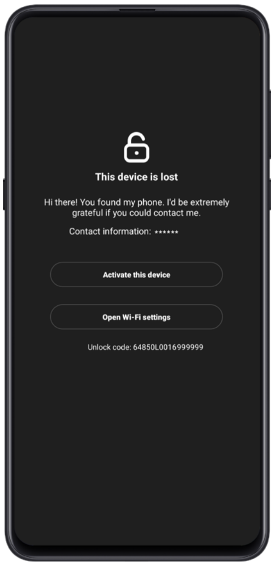


8:29 PM

Messages

Your conversations with private contacts will be stored here.

Figure 3-3 Private Spaces



This device is lost

Hi there! You found my phone. I'd be extremely grateful if you could contact me.

Contact information: ******

Unlock code: 64850L0016999999

Figure 3-4 Find or Lock a Lost Device

3.6 Privacy Features in Mi Browser

Protect your privacy when surfing the web

Mi Browser provides many privacy-oriented features that can help protect your privacy when you browse websites.

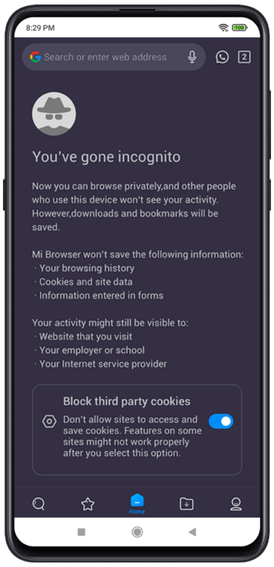
Incognito mode

Users can limit Mi Browser's collection and recording of data by switching to incognito mode. See [Figure 3–5 Incognito Mode]. When the user enables incognito mode, the following information will not be stored on the user's device or uploaded to Xiaomi's servers:

- Basic browsing history information, such as visited websites and search history
- Actions on and downloads from visited web pages
- Information entered into online forms
- Changes to cookies, and
- Other website data

Once incognito mode is enabled, no one else who uses the device will be able to see your searches and websites visited in incognito mode. Moreover, your browsing history, bookmarks, and tabs will not be synchronized to the cloud (if cloud synchronization is enabled). In incognito mode, each tab's information is independent from the information on the others, so the website cannot track between multiple sessions.

Incognito mode does not make you completely invisible on the Internet. The website you visit may record your access. In incognito mode, your browsing actions are not hidden from your Internet service provider or the websites you browse. Incognito mode automatically turns off once users exit the browser process so as to ensure a satisfactory browser experience.



You've gone incognito

Now you can browse privately,and other people who use this device won't see your activity. However,downloads and bookmarks will be saved.

Mi Browser won't save the following information:
· Your browsing history
· Cookies and site data
· Information entered in forms

Your activity might still be visible to:
· Website that you visit
· Your employer or school
· Your Internet service provider

Block third party cookies
Don't allow sites to access and save cookies. Features on some sites might not work properly after you select this option.

Figure 3–5 Incognito Mode

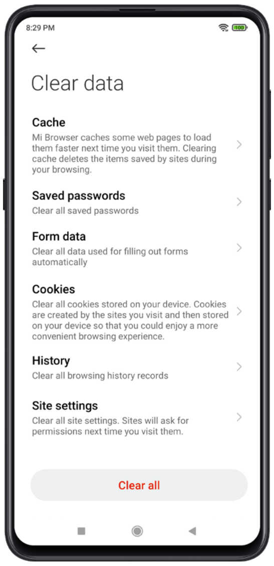
Clearing history

Mi Browser saves your history and website data on the device when incognito mode is not enabled. This gives users a better browsing experience, making it easy to access websites they have previously visited. This data includes visited websites, search term history, and so on.

Mi Browser provides convenient functions to clear this data. You can clear the website cache, saved passwords, form autofill data, all cookie data, and history and website settings. You can also clear all the above data with one click via Mi Browser > My > Settings > Clear Data. See [Figure 3–6 Clear Data]

Moreover, you can set the browser to automatically clear the history each time you exit by using Mi Browser > My > Bookmarks/History > History > Clear History on Exit. See [Figure 3–7 Clear History Upon Exit]

If you are logged into a Mi Account on a device and clear bookmarks and history with data synchronization enabled, and then log into the same Mi Account on another device, the bookmarks and history will also be cleared on that device.



8:29 PM

Clear data

Cache
Mi Browser caches some web pages to load them faster next time you visit them. Clearing cache deletes the items saved by sites during your browsing.

Saved passwords
Clear all saved passwords

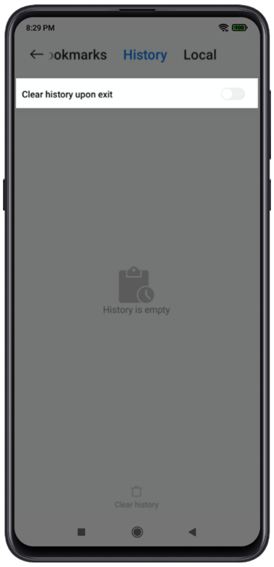
Form data
Clear all data used for filling out forms automatically

Cookies
Clear all cookies stored on your device. Cookies are created by the sites you visit and then stored on your device so that you could enjoy a more convenient browsing experience.

History
Clear all browsing history records

Site settings
Clear all site settings. Sites will ask for permissions next time you visit them.

Figure 3-6 Clear Data



8:29 PM

Clear history upon exit ○

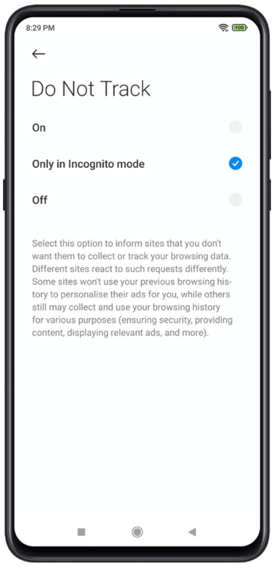
History is empty

Figure 3-7 Clear History Upon Exit

Do Not Track

User action tracking is mature, long-standing technology, and some websites embed multiple user behavior tracking devices from multiple partners on their pages to provide more accurate ad recommendations to users. For example, when users view a product online, they will often see advertisements for the same product on other websites. See [Figure 3-8 Do Not Track]

Users can enable the Do Not Track function in the browser via the Do Not Track item in Mi Browser >My > Settings > Privacy and Security. Once enabled, Mi Browser will notify websites not to collect or track the user's browsing data while the user is browsing. Keep in mind that not all websites respond to browser Do Not Track signals and responses will vary. For example, if requested, some websites will not display advertisements based on other websites that the user has visited. Some websites also collect and use browsing data for a number of reasons (increased security, to provide content, advertising, recommendations, etc.).



8:29 PM

Do Not Track

On ○

Only in Incognito mode ✓

Off ○

Select this option to inform sites that you don't want them to collect or track your browsing data. Different sites react to such requests differently. Some sites won't use your previous browsing history to personalise their ads for you, while others still may collect and use your browsing history for various purposes (ensuring security, providing content, displaying relevant ads, and more).

Figure 3-8 Do Not Track

04

MIUI Apps and Privacy

4.1 Overview

In this section, we provide additional details on our privacy practices related to the main apps and services in MIUI, including **Xiaomi Cloud, Mi Account, Find Device, Themes, App Vault, Get Apps, Mi Browser, Mi Video, Mi Pay, App Usage Data, Advertisement and AI Technology**.

The content for each app or service normally consists of the following sections,

- **Introduction**
- **Data Inventory**, which summarizes data collection and usage in a table for the application or service. The data inventory includes the data types we collected, the identification qualifier of the data, the purpose for collecting the data, the encryption methods used when the data is in transit and at rest, and the data retention policy. The data type, identification qualifier, and purpose concepts are derived from ISO/IEC 19944-1:2020.
- **Data Collection and Usage**, which details the data collection and purpose for each function or module of a certain application or service. The relevant introduction can be considered as the use of data statements defined in ISO/IEC 19944-1:2020.
- **Privacy Controls**, which gives you the guidance on how to manage your data and exercise your data rights within the application or service.
- **Conclusion**

For additional information about our privacy practices that is not provided in this White Paper, please review the Xiaomi Privacy Policy.

4.2 Xiaomi Cloud

Introduction

Xiaomi Cloud is a personal cloud storage service provided by Xiaomi. You can securely store your important data, such as photos, contacts, and notes in Xiaomi Cloud. The data can be synchronized between your devices at your control. Xiaomi Cloud is easy-to-use and integrated into Xiaomi's mobile phones, TVs, IoT products and applications, and it can also be accessed via your PC and the web.

Xiaomi Cloud is built to protect your privacy. The data synchronized and stored in Xiaomi Cloud is strictly encrypted. We will not access and view the data that you choose to store in the Xiaomi Cloud, nor will we conduct any form of analysis on the data.

Xiaomi Cloud is available in all markets.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified[1]	App functionality[2]	HTTPS	Plain[3]	Per user's request
Purchases	Purchase History	Identified	App functionality	HTTPS	AES-128	Per user's request
Contacts	Contacts	Identified	App functionality	HTTPS	AES-128	Per user's request
Browsing History	Browsing History	Identified	App functionality	HTTPS	AES-128	Per user's request
User Content	Text Messages	Identified	App functionality	HTTPS	AES-128	Per user's request
	Photos or Videos	Identified	App functionality	HTTPS	AES-128	Per user's request
	Call History	Identified	App functionality	HTTPS	AES-128	Per user's request
	Notes	Identified	App functionality	HTTPS	AES-128	Per user's request
	Recordings	Identified	App functionality	HTTPS	AES-128	Per user's request
	Frequent Phrase	Identified	App functionality	HTTPS	AES-128	Per user's request
Other Data	Calendar Events	Identified	App functionality	HTTPS	AES-128	Per user's request
	Home Screen Settings	Identified	App functionality	HTTPS	AES-128	Per user's request
	Wi-Fi Settings	Identified	App functionality	HTTPS	AES-128	Per user's request

[1] Identified means that the data is linked to you. If data is linked with a user/system/device level identifiers, such as Mi Account ID, IMEI, or Android ID, it will be classified as Identified.

[2] App functionality means that the purpose for collecting the data is to provide a function or service to you.

[3] Plain means that the data is not encrypted at the field level, but we still take other necessary technical and management measures to ensure its security, such as strict access control.

Data Collection and Usage

1) Data Synchronization

Xiaomi Cloud is a cloud storage service that currently supports the following apps and system settings in MIUI:

- **App Data: Gallery, Messages, Contacts, Call History, Notes, Recordings, Calendar, and Mi Browser**[4]
- **System Setting: Wi-Fi, Home Screen, and Frequent Phrase.**

You have full control when using Xiaomi Cloud. You can enable or cancel synchronization at any time, or you can select just the apps that you need to synchronize at any time. When you enable the data synchronization of an app, we encrypt the synchronized data both in transit and at rest in our server. We are committed to meeting stringent security controls to protect your data in Xiaomi Cloud.

The details of the data synchronized for each section are as follows.

ICON	Name of apps and settings	Details of the data synchronized
	Gallery	**Photos**, **pictures**, **and videos** in albums and folders selected to be synced
	Message	**Phone number** of the current SIM card in your phone **Short messages** in your phone, including the messages marked as favorites
	Contacts	**Contacts** associated with your Mi Account
	Call History	**Phone number** of the current SIM card in your phone and **call history**, including incoming calls, outgoing calls, time, and duration
	Recordings	**Audio and recording files**
	Notes	**Notes and tasks**, including privacy notes
	Calendar	**Events** in your calendar
	Mi Browser	**Browsing history** and **favorite sites**
	Wi-Fi	**Wi-Fi settings** data, including Wi-Fi SSID and encrypted passwords
	Frequent Phrase	Words and phrases added to the **frequent phrase list**
	Home Screen	**Home screen settings**, including installed apps list, home screen layout, and wallpaper

[4] Data synchronization for Mi Browser is only available in some countries or regions, including India, Russia, and European Economic Area (EEA) countries.

2) Cloud File Trash

When the data in Gallery, Notes, Messages, Contacts, and Recordings synchronized or stored in the cloud is deleted, the relevant files will be moved to trash for a period. The data retention period in trash is subject to the user's membership plan and its validity period, with a minimum retention of 30 days and maximum retention of 180 days. During the retention period, you can try to restore the data at any time. When the retention period has expired, or you manually delete the files in trash, the files will be permanently deleted and cannot be restored.

3) Membership

Xiaomi Cloud provides users with extra storage space, more frequent synchronization, and extended trash retention periods via membership plans. We retain the **purchase records** after you purchase any membership plan.

TIPS
You can learn more about how Xiaomi Cloud collects and processes your personal information by reviewing the Xiaomi Cloud Privacy Policy.

Manage Your Privacy

1) Access and Retrieve Copies of Your Data

Xiaomi Cloud provides you with two ways to access your data.

① Synchronize and access the data in the local app. The most common way to access the data is to synchronize and view it on a mobile phone in the local app.

② Access the data in the Xiaomi Cloud web portal. You can also view and download your photos there. See [Figure 4-1 Xiaomi Cloud web portal]

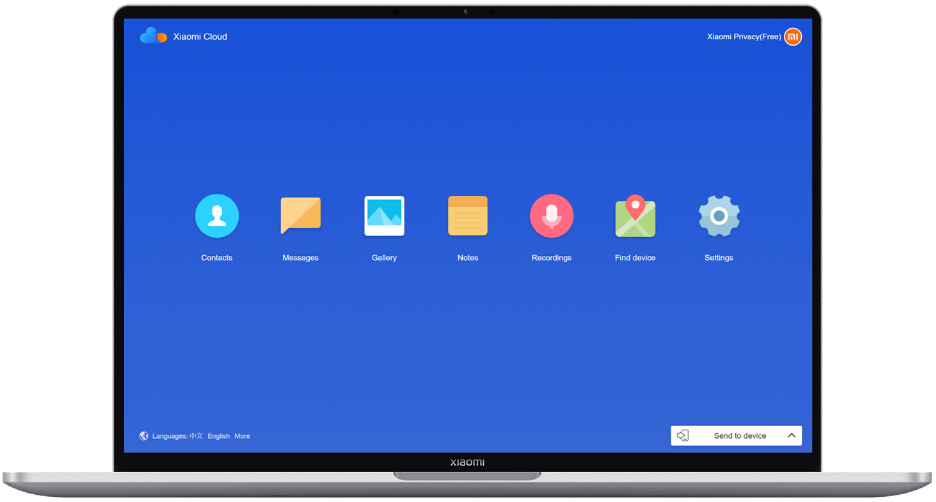


Figure 4-1 Xiaomi Cloud web portal

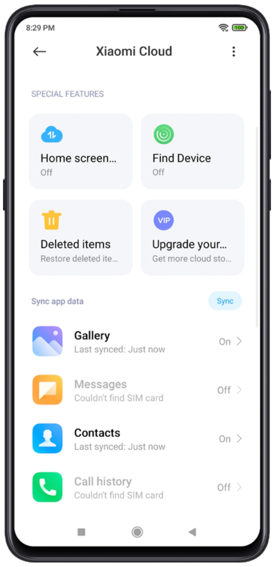
2) Manage Data Synchronization

You have full control of data synchronization. Specifically, you can:

① Enable or disable the data synchronization for each app or setting at any time. Go to Settings > Xiaomi Cloud, and then turn data synchronization on or off, or manage other options. See [Figure 4–2 Synchronization Settings]

② Determine whether to only use Wi–Fi to synchronize data.

③ Set a detailed synchronization configuration for some items, e.g. choose which folder to synchronize in Gallery See [Figure 4–3 Gallery Sync Settings] and arrange the backup schedule for Home Screen. See [Figure 4–4 Cloud Backup Settings].



8:29 PM

Xiaomi Cloud

SPECIAL FEATURES

Home screen... Off

Find Device Off

Deleted items Restore deleted ite...

Upgrade your... Get more cloud sto...

Sync app data — Sync

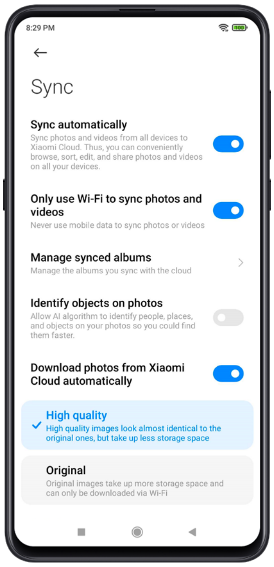
Gallery — Last synced: Just now — On

Messages — Couldn't find SIM card — Off

Contacts — Last synced: Just now — On

Call history — Couldn't find SIM card — Off

Figure 4–2 Synchronization Settings



8:29 PM

Sync

Sync automatically — Sync photos and videos from all devices to Xiaomi Cloud. Thus, you can conveniently browse, sort, edit, and share photos and videos on all your devices.

Only use Wi-Fi to sync photos and videos — Never use mobile data to sync photos or videos

Manage synced albums — Manage the albums you sync with the cloud

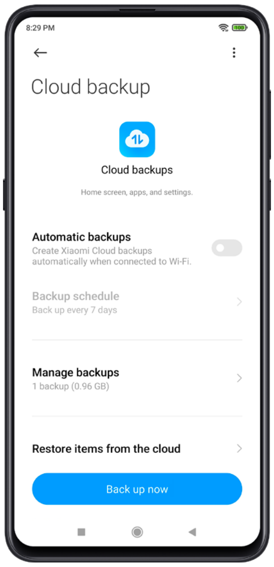
Identify objects on photos — Allow AI algorithm to identify people, places, and objects on your photos so you could find them faster.

Download photos from Xiaomi Cloud automatically

✓ High quality — High quality images look almost identical to the original ones, but take up less storage space

Original — Original images take up more storage space and can only be downloaded via Wi-Fi

Figure 4–3 Gallery Sync Settings



8:29 PM

Cloud backup

Cloud backups

Home screen, apps, and settings.

Automatic backups — Create Xiaomi Cloud backups automatically when connected to Wi-Fi.

Backup schedule — Back up every 7 days

Manage backups — 1 backup (0.96 GB)

Restore items from the cloud

Back up now

Figure 4–4 Cloud Backup Settings

3) Delete Data

① Messages, Contacts, Call History, Notes, Recordings, and Calendar data. You can delete the data in the app. The cloud server will then synchronize the deletion and move the files to trash. Once the retention period has expired, or you manually delete the files in trash, the data will be permanently deleted.

② Wi–Fi and Frequent Phrase data. When you disable synchronization, the data in the cloud will be permanently deleted.

③ Home Screen backup data. This data can be deleted on the Cloud Backup page. See [Figure 4–4 Cloud Backup Settings].

Conclusion

Privacy and security protections are the primary goals of our product design at Xiaomi. The following privacy principles are deeply integrated into Xiaomi Cloud:

- To give you full control of the data you synchronize to Xiaomi Cloud.
- To securely transmit and store synchronized data.
- A promise not to access and analyze your synchronized data.

4.3 Mi Account

Introduction

Mi Account is a general authentication and authorization service provided by Xiaomi.

With Mi Account, you can log in and access Xiaomi's products and services, such as the MIUI system on your smartphone, Mi Store, Mi Home, Xiaomi Cloud, Mi Pay, etc. Once you log in to a Xiaomi mobile phone with your Mi Account, your device will be associated with your account to provide you with better service and support. Mi Account also supports OAuth 2.0 protocol, which lets you use other companies' apps, e.g. Mi Band and Yeelight devices, which are made by our ecosystem companies.

Mi Account is designed to protect your privacy and security. We work hard to collect only the data we need to make your experience better. We also adopt standard industry practices to protect the security of your account, such as 2-step verification, also known as two-factor authentication.

Mi Account is available in all markets.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality	HTTPS	Plain	Per user's request
	Android ID	Identified	App functionality	HTTPS	SHA-1	Per user's request
Contact Info	Email Address	Identified	App functionality	HTTPS	AES-128	Per user's request
	Phone Number	Identified	App functionality	HTTPS	AES-128	Per user's request
	Country	Identified	App functionality	HTTPS	Plain	Per user's request
Usage Data	Product Interaction	Pseudonymized[1]	App functionality	HTTPS	Not stored	N/A
Other Data	Profile Data (nickname, profile photo, gender)	Identified	App functionality	HTTPS	Plain	Per user's request
	Device Model	Identified	App functionality	HTTPS	Plain	Per user's request
	Accelerometer Data and Network Information	Pseudonymized	App functionality	HTTPS	Not stored	N/A
	Account Passwords	Identified	App functionality	HTTPS	Compound encryption with secret password and salt per account	Per user's request

[1] Pseudonymized means that the data is not linked with you. If data is linked with an app instance level identifier or a random identifier, such as Firebase Instance ID, and random ID, it will be classified as pseudonymized. We follow the Best practices for unique identifiers to create and use unique identifiers.

Data Collection and Usage

1) Account Registration and Login

Mi Account can be found and accessed in two ways:

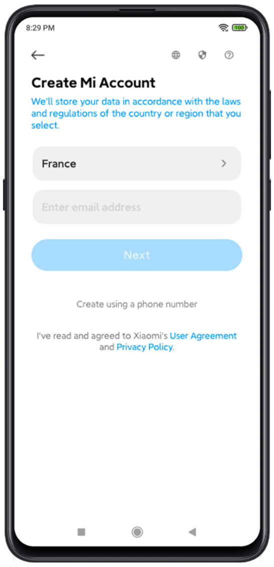
- System settings of the smartphone: Go to: Settings > Account > Mi Account
- Mi Account Website: Go to https://account.xiaomi.com

When you create a new account, we collect your **phone number** or **email address**, and **password**. The data is encrypted on our server. We may also request that you select **your country or region** when creating the account, as it determines where your data in Mi Account is stored. Once you have created a Mi Account, a new **Mi Account ID** is assigned to you. See [Figure 4-5 Create Mi Account]

If you log in on a Xiaomi cell phone with a specific Mi Account ID, the device will be linked with it directly. You can see and manage the smartphones linked to the account on the Manage devices tab.

2) Account Profile

You have the option to add additional personal information to your account profile, including a **nickname**, **profile photo**, and **gender**. You may also need to set up a **recovery phone number or email**, in case you forget your password. See [Figure 4-6 Mi Account Profile]


8:29 PM

Create Mi Account

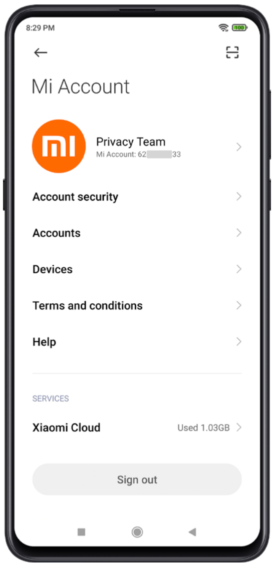
We'll store your data in accordance with the laws and regulations of the country or region that you select.

France

Enter email address

I've read and agreed to Xiaomi's User Agreement and Privacy Policy.

Figure 4-5 Create Mi Account


8:29 PM

Mi Account

Privacy Team
Mi Account: 62[redacted]33

Used 1.03GB

Figure 4-6 Mi Account Profile

3) Security Status Check

We have implemented standard industry practices to help enhance the security level of your account.

- **Login Environment Check**

Every time you log in to MIUI with your Mi Account, we collect **hashed Android ID**, **IP address**, and **device model** to check whether you are in a normal and safe environment. For example, if you log in on a new device or in a new location, that login request would be considered more risky than usual. We will then send a verification code to your phone or mailbox. If you enable 2-step verification, we will push a confirmation dialog to your other devices instead to verify you.

- **Human-Machine Check**

We also collect the **accelerometer data**, as well as the **network environment data** around you to assess whether the login request is from a natural person or a robot. This data is not linked to you and is discarded after the human-machine check is finished. If the result is not positive, we may use Google reCaptcha to conduct further verification. The reCaptcha is subject to the Google Privacy Policy and Terms of Use.

4) OAuth 2.0 Authorization

Mi Account supports the OAuth 2.0 protocol, which is a method to log into other third-party products or services. When you use this method to log in, we generate a **UnionID** to represent you. A UnionID is a string that consists of numbers, letters, and symbols of varying length. We only share your UnionID, profile photo, and nickname with the provider of the product or services. Each service provider will receive a different UnionID from others, which can protect your privacy and avoid further tracking. You can access and manage the authorization on the 'Accounts & Permission' tab.

TIPS
You can learn more about how Mi Account collects and processes your personal information by reviewing the separate Mi Account Privacy Policy.

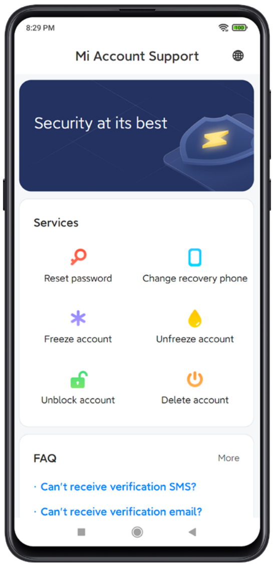
Manage Your Privacy

1) Access and Correct Your Data in Mi Account

Mi Account gives you an easy way to access and correct the data you have provided to Xiaomi:

① You can edit your profile data on the Personal Info tab.

② The Mi Account Help Center lets you: (i) reset your passwords; (ii) change your recovery phone number; (iii) freeze or unfreeze an account; or (iv) block or unblock an account.



Mi Account Support

Security at its best

Services

Reset password

Change recovery phone

Freeze account

Unfreeze account

Unblock account

Delete account

FAQ

More

· Can't receive verification SMS?

· Can't receive verification email?

Figure 4-7 Mi Account Help Center

③ If you want to change the country of your account, you can submit your request in Privacy Support.

2) Delete Your Account

Your Mi Account can be deleted via the Privacy tab.

Once an account is deleted, all the data linked to the account will be deleted or anonymized. In most cases, the data will be deleted. If we choose to anonymize the data, the processed data cannot be re-linked to you, nor will we try to do so.

Conclusion

Privacy and security protections continue to be the primary goals of product design at Xiaomi. The following privacy principles are deeply integrated into Mi Account:

- Provide transparency and control to Mi Account data.
- Consider security when designing Mi Account.
- Minimize the amount of data collected by Mi Account.

4.4 Find Device

Introduction

Find Device is a built-in service in Xiaomi smartphones and can help you locate and track your phone when the phone is marked as lost. At the same time, you can erase data remotely to clear the data from the lost phone, which can help protect your data from unauthorized access.

Security and privacy are fundamental to the design of Find Device. The feature only collects the location information you need, and is fully under your control. You can enable or disable Find Device at any time.

Find Device is available in all markets.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality	HTTPS	AES-128	Per user's request
	MAC Address	Identified	App functionality	HTTPS	AES-128	Per user's request
	Device ID - hashed IMEI or hashed Android ID	Identified	App functionality	HTTPS	Plain	Per user's request
	FID - fixed device level ID	Identified	App functionality	HTTPS	Plain	Per user's request
Contact Info	Phone Number	Identified	App functionality	HTTPS	AES-128	Per user's request
Location	Precise Location	Identified	App functionality	HTTPS	AES-128	Per user's request

Data Collection and Usage

1) Initialization

When you activate Find Phone on your phone, we collect your **Mi Account ID** and the identifiers of your device, including **MAC address**, Device ID (**hashed Android ID/hashed IMEI**, depending on the model type and system version), and **FID**, a fixed device level ID. This enables us to build the solid connection between your phone and your Mi Account. We also collect your current **phone number** to send instructions to your phone when you lose it.

2) Device Location

When you try to locate your phone via the Xiaomi Cloud, the **precise location** of your phone is collected and then made available to you on the map. The location is only uploaded per your request.

3) Remote Control

You can trigger sound, set Lost Mode, and erase data remotely via Xiaomi Cloud. When you turn on Lost Mode, the **precise location** of your lost phone is uploaded at fixed intervals, which helps you locate and track your phone.

Manage Your Privacy

1) Access Your Data in Find Device

You can access and view the location of your devices in Xiaomi Cloud. Go to Xiaomi Cloud > Find Device, and then choose the phone you want to locate.

- You can click the Find Location/Relocate button to see its current location. Once the phone is located successfully, you can see its current location on the map.
- You can also click '…' > View History button to see a list of past locating operations.

2) Turn off Find Device and Delete Data

If you want to revoke the authorization for Find Device and delete the data, go to Settings > Mi Account > Cloud Services > Find Phone, and then disable the Find Device option. You can also disable the option in Xiaomi Cloud.

If Lost Mode is enabled, you need to disable Lost Mode first and then turn off Find Device.

Once Find Device is turned off, we will stop data processing and schedule the deletion of your location data history. When Find Device is turned off for 30 days continuously, the historical location data will be permanently deleted.

Conclusion

Privacy and security protections are the primary goals of product design at Xiaomi. The following privacy principles are deeply integrated into Find Device:

- Designed to safeguard your phone and protect your data.
- Provide full control over functions and data in Find Device.
- Minimize data collection when you find and control your device remotely.

4.5 Themes

Introduction

Themes lets users ‘skin’ their devices. Users can download resources including themes, wallpapers, ringtones, fonts, and more to personalize the appearance of the MIUI system and applications. Themes respects users' privacy and only collects the necessary data when running.

Themes is available in all markets, except for some countries in the Middle East.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality	HTTPS	MD5	Per user's request
	GAID[1]	Identified	App functionality	HTTPS	MD5	180 days
Search History	Search History	Identified	Personalization[2]	HTTPS	Plain	180 days
Usage Data	Product Interaction	Identified	Personalization	HTTPS	Plain	180 days
		Pseudonymized	Analytics[3]	HTTPS	Plain	90 days
	Advertising Data	Identified	Advertising[4]	HTTPS	Plain	180 days
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS	Plain	90 days
Other Data	Locale and Region Settings	Identified	Personalization	HTTPS	Plain	180 days
	Resource Download Record	Identified	App functionality Personalization	HTTPS	Plain	Per user's request
	Favorite Resource List	Identified	App functionality Personalization	HTTPS	Plain	Per user's request

Data Collection and Usage

1) Basic Functions

Themes gives you the resources to personalize your system interface, e.g. using themes, wallpapers, ringtones,

[1] GAID stands for Google Advertising ID. GAID is a unique, user-resettable ID for advertising. Data linked with GAID is classified as Identified. For more information about GAID, go to https://support.google.com/googleplay/android-developer/answer/6048248?hl=en

[2] Personalization means that the data is collected and used to change the selection or presentation of content for different users.

[3] Analytics means that data is collected and used to analyze and improve the existing functional capabilities, and to provide insights for adding new capabilities based on the results of the analysis.

[4] Advertising means that the data is collected and used to provide an advertising service to you, including requesting advertisements, and evaluating the outcome of promotions

and font. You can view, search, download, and apply resources in Themes. Themes collects the **locale and region settings** of your phone to show you the appropriate resources. When you download a resource, Themes collects the **Mi Account ID** and the **resource id** of the items you downloaded.

2) Adding to Favorites

You can add resources to your favorites list. You need to log in with your Mi Account when using this function. We collect the **Mi Account ID** and the **resource id** for the items you added to your Favorites list.

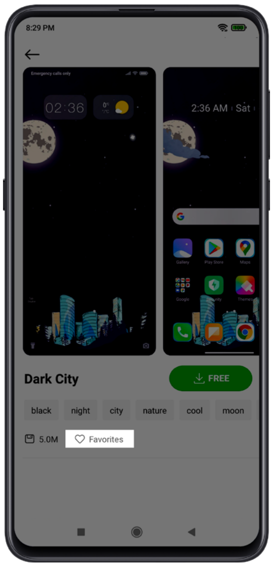


Figure 4-8 Add an Item to Favorites

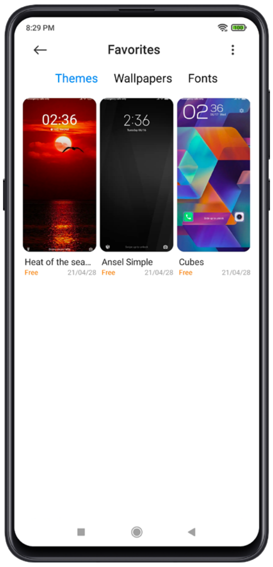


Figure 4-9 Favorites List

3) Personalized Recommendations for Resources

To help you discover more excellent resources, such as wallpapers and themes, Themes presents you with personalized recommendations for resources you may be interested in on the home page, resource detail page, and wallpaper module page.

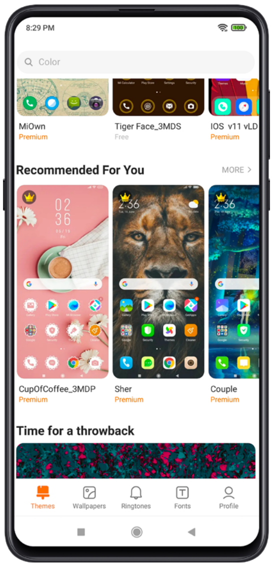


Figure 4-10 Personalized Recommendations

We use the data we collect in Themes, including your download history, favorites list, app interaction data, and search history to provide personalized recommendations.

4) Analytics

Analytical data helps us find issues with the app and improve the user experience. Data collection for analysis purposes is controlled by our MIUI User Experience Program. For details, go to Settings > Password and Security > Privacy > User Experience Program > Learn more about User Experience Program.

Themes collects certain **product interaction data**, such as the number of clicks on each module and page exposure, for analysis and improvement purposes. The data collected for this purpose is used in aggregated form and cannot be associated with a specific user.

Themes also collects **crash data** for troubleshooting and improvement.

5) Advertising

Themes provides you with personalized advertisements. For detailed information regarding ads in MIUI, please refer to 4.11 Advertising and Privacy

Manage Your Privacy

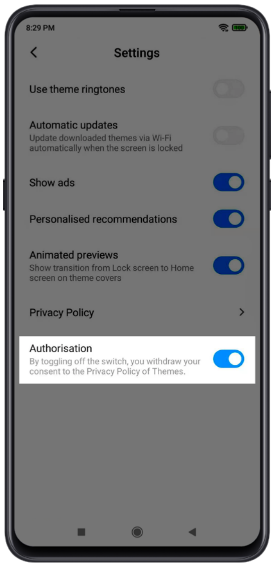
1) Access, Download or Delete User Data in Themes

You can request to access, download, or delete data in Themes by accessing the Privacy Center in Mi Account or by contacting us via Xiaomi Privacy Support.

2) Withdraw Your Consent

You can withdraw your consent in Themes settings. Go to Themes > Settings, and disable the 'Authorization' option. See [Figure 4-11 Withdraw Consent for Themes]

Once the option is disabled, Themes will stop collecting data, and delete your data stored locally and in the cloud.



8:29 PM

Settings

Use theme ringtones ○

Automatic updates ○
Update downloaded themes via Wi-Fi automatically when the screen is locked

Show ads ●

Personalised recommendations ●

Animated previews ●
Show transition from Lock screen to Home screen on theme covers

Privacy Policy >

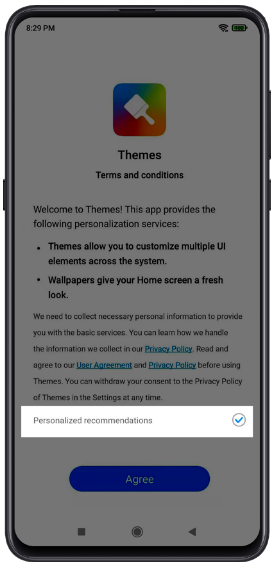
Authorisation ●
By toggling off the switch, you withdraw your consent to the Privacy Policy of Themes.

Figure 4-11 Withdraw Consent for Themes

3) Manage Personalized Recommendations

When you enter the app's Wallpapers homepage for the first time, you will see a pop-up with terms and conditions, a privacy policy, and a check box to manage personalized recommendations. You can unselect the check box if you do not want to see any personalized recommendations in Themes. See [Figure 4-12 Personalization Check Box]

To change your personalized recommendation settings, go to Themes > Settings, and enable or disable the 'Personalized Recommendations' option. See [Figure 4-13 Disable Personalization in Themes]



8:29 PM

Themes

Terms and conditions

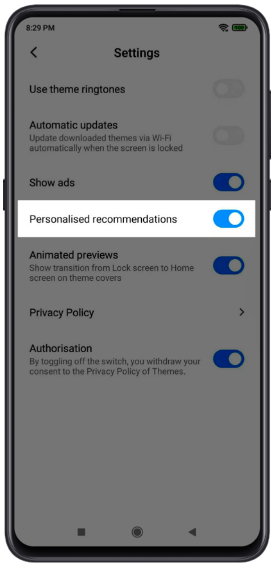
Welcome to Themes! This app provides the following personalization services:

- Themes allow you to customize multiple UI elements across the system.
- Wallpapers give your Home screen a fresh look.

We need to collect necessary personal information to provide you with the basic services. You can learn how we handle the information we collect in our Privacy Policy. Read and agree to our User Agreement and Privacy Policy before using Themes. You can withdraw your consent to the Privacy Policy of Themes in the Settings at any time.

Personalized recommendations ✓

Agree



8:29 PM

Settings

Use theme ringtones ○

Automatic updates ○
Update downloaded themes via Wi-Fi automatically when the screen is locked

Show ads ●

Personalised recommendations ●

Animated previews ●
Show transition from Lock screen to Home screen on theme covers

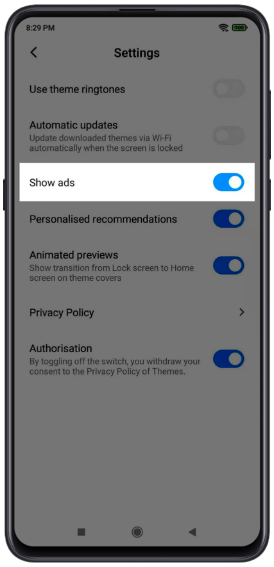
Privacy Policy >

Authorisation ●
By toggling off the switch, you withdraw your consent to the Privacy Policy of Themes.

Figure 4-12 Personalization Check Box Figure 4-13 Disable Personalization in Themes

4) Manage Ads

You can decide whether to show ads in Themes. Go to Themes > Settings, and enable or disable the Show Ads option to change your settings. See [Figure 4-14 Disable Ads in Themes]



8:29 PM

Settings

Use theme ringtones ○

Automatic updates ○
Update downloaded themes via Wi-Fi automatically when the screen is locked

Show ads ●

Personalised recommendations ●

Animated previews ●
Show transition from Lock screen to Home screen on theme covers

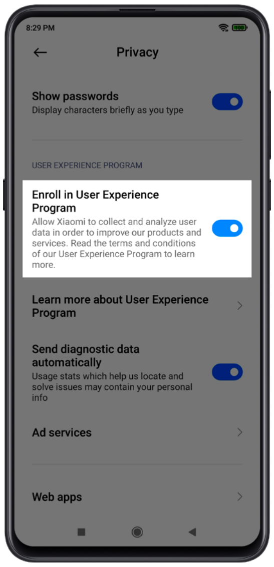
Privacy Policy >

Authorisation ●
By toggling off the switch, you withdraw your consent to the Privacy Policy of Themes.

Figure 4-14 Disable Ads in Themes

5) Manage Data Collection for Analysis Purposes

You can allow or stop data collection for analysis purposes in Themes. Go to Settings > Password & Security > Privacy > User Experience Program, and then enable or disable the 'Enroll in User Experience Program' option. See [Figure 4-15 Opt Out of User Experience Program]



8:29 PM

Privacy

Show passwords
Display characters briefly as you type

USER EXPERIENCE PROGRAM

Enroll in User Experience Program
Allow Xiaomi to collect and analyze user data in order to improve our products and services. Read the terms and conditions of our User Experience Program to learn more.

Learn more about User Experience Program

Send diagnostic data automatically
Usage stats which help us locate and solve issues may contain your personal info

Ad services

Web apps

Figure 4-15 Opt Out of User Experience Program

Conclusion

Privacy and security protections are the primary goals of product design at Xiaomi. The following privacy principles are deeply integrated into the Themes app:

- Provide control over user consent, personalization, and ads.
- Minimize the amount of data collected by Themes.
- Use data to drive the user experience.

4.6 App Vault

Introduction

App Vault is a collection of app cards that make it easy for users to open apps, access useful data, and read the latest news. App Vault is easily accessed by swiping the home screen to the left.

App Vault is designed with user privacy in mind. App Vault only collects the user data necessary to provide services and provides users with the mechanisms to revoke authorization, delete data, and manage personalization.

App Vault is available in all markets.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	GAID	Identified	Personalization	HTTPS	MD5	180 days
Usage Data	Product Interaction	Identified	Personalization	HTTPS	Plain	180 days
		Pseudonymized	Analytics	HTTPS	Plain	90 days
	Advertising Data	Identified	Advertising	HTTPS	Plain	180 days
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS	Plain	90 days
	Performance Data	Pseudonymized	Analytics	HTTPS	Plain	90 days

Data Collection and Usage

1) Shortcuts

Shortcuts is the first card listed in App Vault. Shortcuts lead users to their frequently used apps easily. App Vault collects the name of frequently used apps to decide the display order on this card. The Shortcuts function runs locally on your smartphone, and no data is uploaded to our servers.

2) Application Cards

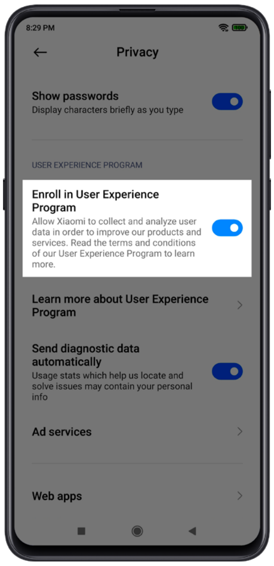
App Vault provides many cards that display information from various apps. Users can view stocks, videos, sports events, schedules, and other information on different cards.

For the Note, Steps, and Calendar cards, App Vault only displays data from the local apps in the device and does not upload the information displayed in the cards to our servers.

3) News Card and Information Personalization

You can see personalized news and information in the News card. The news content in the information stream is provided by either Mail.ru or MSN.com. See [Figure 4-16 Personalized Services by Third Parties]

When the personalized content recommendation function is enabled, the third-party service provider collects the **Google Advertising ID** and the information feed's **interaction data** for analysis and personalization. App Vault does not use usage data from other cards or modules for personalized recommendations.



8:29 PM

Privacy

Show passwords
Display characters briefly as you type

USER EXPERIENCE PROGRAM

Enroll in User Experience Program
Allow Xiaomi to collect and analyze user data in order to improve our products and services. Read the terms and conditions of our User Experience Program to learn more.

Learn more about User Experience Program

Send diagnostic data automatically
Usage stats which help us locate and solve issues may contain your personal info

Ad services

Web apps

Figure 4-16 Personalized Services by Third Parties

4) Analytics

Analytical data helps us find issues with the app and improve the user experience. Data collection for analysis purposes is controlled by our MIUI User Experience Program. For details, go to Settings > Password and Security > Privacy > User Experience Program > Learn more about User Experience Program.

App Vault collects certain **product interaction data**, such as the number of clicks on each module and page exposure, for analysis and improvement purposes. The data collected for this purpose is used in aggregated form and cannot be associated with a specific user.

App Vault also collects **crash data** and **performance data** for troubleshooting and improvement.

5) Advertising

App Vault provides you with personalized advertisements. For detailed information regarding ads in MIUI, please refer to 4.11 Advertising and Privacy

Manage Your Privacy

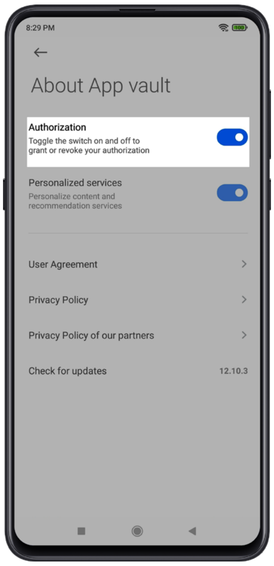
1) Withdraw Your Consent

You can withdraw your consent by revoking the App Vault authorization at any time. Go to App Vault > '⚙' > About App vault, and then enable or disable the 'Authorization' option. See [Figure 4-17 Withdraw Consent in App Vault]

When authorization is revoked, App Vault will immediately stop all data collection, delete data, and cancel the granted permissions.

2) Manage Personalized Recommendations

App Vault can provide users with personalized content and ad recommendation services. The content personalization service is provided by content partners, including Mail.ru and MSN.com, with the user's consent. Go to App Vault > '⚙' > About App vault, and then enable or disable the 'Personalized services' option. See [Figure 4-18 Disable Personalization in App Vault]



8:29 PM

About App vault

Authorization
Toggle the switch on and off to grant or revoke your authorization

Personalized services
Personalize content and recommendation services

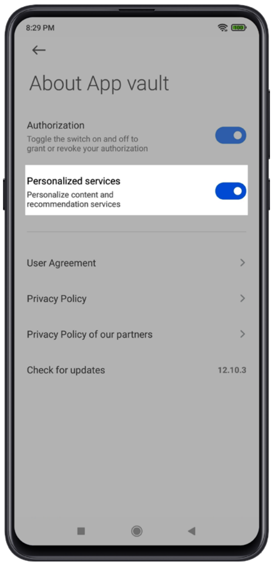
User Agreement

Privacy Policy

Privacy Policy of our partners

Check for updates 12.10.3

Figure 4-17 Withdraw Consent in App Vault



8:29 PM

About App vault

Authorization
Toggle the switch on and off to grant or revoke your authorization

Personalized services
Personalize content and recommendation services

User Agreement

Privacy Policy

Privacy Policy of our partners

Check for updates 12.10.3

Figure 4-18 Disable Personalization in App Vault

3) Manage Data Collection for Analysis Purposes

You can allow or stop data collection for analysis purposes in Themes. Go to Settings > Password & Security > Privacy > User Experience Program, and then enable or disable the 'Enroll in User Experience Program' option.

4) Manage Personalized Ads

Personalized ads in this application are controlled by the 'Personalized Ads' option in the system settings. For details, refer to 4.11 Advertising and Privacy

Conclusion

At Xiaomi, we are committed to protecting user information security and privacy. App Vault is built with this commitment in mind and is designed to respect user privacy.

The following Xiaomi privacy principles are deeply integrated into App Vault:

- Minimize data collection
- All information collected aims to empower user experience
- Provide options for users to withdraw consent and exercise their data rights

4.7 Get Apps

Introduction

Get Apps provides a platform for users of Xiaomi mobile phones to browse, download, install, and update applications. Get Apps only collects the data we need to power your experience.

Get Apps conducts security audits on all connected applications to minimize security risks around applications downloaded by users on the Get Apps platform.

Get Apps is available in India, Russia, Spain, and Indonesia.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality Analytics	HTTPS	Plain	Per user's request
	GAID	Identified	App functionality Personalization Analytics Advertising	HTTPS	Plain	Per user's request
Search History	Search History	Identified	App functionality Personalization Analytics	HTTPS	Plain	Per user's request
User Content Data	Comments	Identified	App functionality	HTTPS	Plain	Per user's request
Usage Data	Product Interaction	Identified	App functionality Personalization Analytics Advertising	HTTPS	Plain	Per user's request
	Advertising Data	Identified	Advertising	HTTPS	Plain	180 days
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS	Plain	90 days
Other Data	App List	Identified	App functionality Personalization	HTTPS	Plain	Per user's request
	Points and Redeem Records	Identified	App functionality	HTTPS	Plain	Per user's request
	Network Type	Identified	App functionality Analytics Advertising	HTTPS	Plain	Per user's request
	Locale and Region Settings	Identified	App functionality Personalization Analytics Advertising	HTTPS	Plain	Per user's request

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Other Data	Device and System Specs	Identified	App functionality Personalization Analytics Advertising	HTTPS	Plain	Per user's request

Data Collection and Usage

1) Application Browsing and Searching

You can find any application you want in Get Apps. When you browse in Get Apps, we collect your **device and system specs**, and **locale and region settings** to provide the most suitable applications for you. When you search applications in Get Apps, we collect the **Google Advertising ID** and retain your **search history**.

2) Application Downloading and Updating

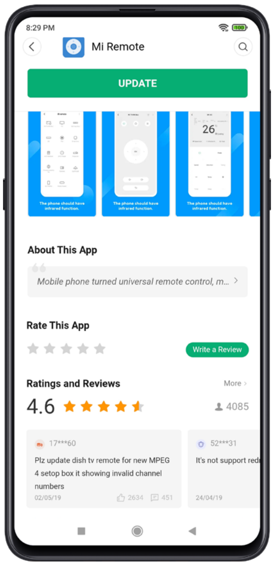
To provide the application download and update function, we collect the **Google Advertising ID** and **application name** to retain a record. We also collect and check the **network type** of your phone to enhance your downloading experience. To check whether the applications on your phone need updates, we collect the **application list** on your phone and the **application version**.

3) Application Ratings and Reviews

You can interact with Get Apps by adding reviews or ratings for an application.

When you publish a review for a certain application, we collect your **Mi Account ID**, **nickname**, **photo**, **application name**, and **comments**. The comments you publish can be read by other users for reference but your nickname will be masked to protect your privacy.

When you rate an app, we collect your **Mi Account ID**, the **application name**, and your **rating score**.



8:29 PM
Mi Remote
UPDATE
26
The phone should have infrared function.
The phone should have infrared function.
The phone should have infrared function.
About This App
Rate This App
Write a Review
Ratings and Reviews
More
4.6
4085
17***60
2634
451
52***31

Mobile phone turned universal remote control, m...

Plz update dish tv remote for new MPEG 4 setop box it showing invalid channel numbers

02/05/19

It's not support red

24/04/19

Figure 4-19 Get Apps Reviews and Ratings

4) Points Mall[1]

In Points Mall, you can earn points by completing tasks and then redeem the points for prizes. When you use Points Mall, we record the **points** with your **Mi Account ID**. We also retain the **redeem records** when a redemption occurs.

5) Personalized Recommendations[2]

Get Apps provides you with personalized recommendations to help you find more applications you may be interested in. We use Google Advertising ID, as well as the data collected in Get Apps, in other functions, such as device and system specs, application download records, search history, and application list, for personalized recommendations.

6) Analytics

Analytical data helps us find issues with the app and improve the user experience. Data collection for analysis purposes is controlled by our MIUI User Experience Program. For details, go to Settings > Password and Security > Privacy > User Experience Program > Learn more about User Experience Program.

Get Apps collects the **Google Advertising ID**, **system and device specs**, **locale and region settings**, **network type**, and certain **product interaction data** within the app. This data includes the number of clicks on each module and button; page exposure; browsing path; and app downloads, installation, and activation for analysis and improvement purposes.

Get Apps also collects **crash data** and **performance data** for troubleshooting and improvement.

6) Advertising

Get Apps provides you with personalized advertisements. For detailed information regarding ads in MIUI, please See [4.11 Advertising and Privacy]

Manage Your Privacy

1) Access, Download or Delete User Data in Get Apps

You can request to access, download, or delete the data in Get Apps by accessing the Privacy Center in Mi Account or by contacting us via Xiaomi Privacy Support.

2) Withdraw Your Consent

You can withdraw your consent for Get Apps in the system settings. Go to Settings > Password & Security > Authorization & Revocation, and then disable the option beside the Get Apps icon.

Once the option is enabled, Get Apps will stop collecting data and delete your data stored locally and in the cloud.

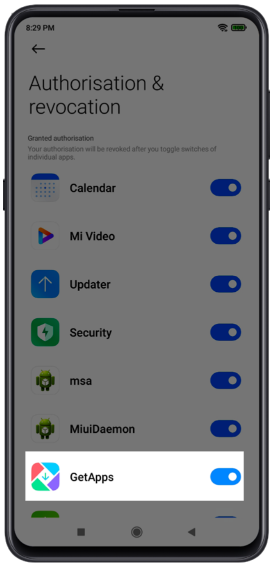
3) Manage Personalized Recommendations

You can disable personalized services at any time. Go to Get Apps > My > Privacy, and then disable the

[1] Points Mall is only available in India.

[2] Personalized Recommendations is not available in Spain

'Personalized Recommendations' option.



8:29 PM

Authorisation & revocation

Granted authorisation

Your authorisation will be revoked after you toggle switches of individual apps.

Calendar

Mi Video

Updater

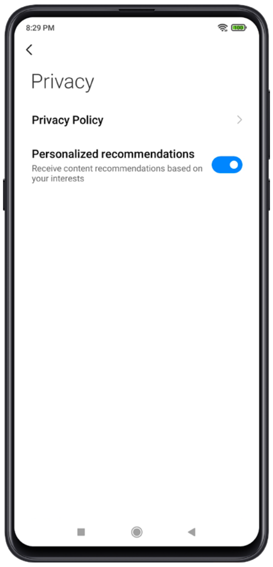
Security

msa

MiuiDaemon

GetApps

Figure 4-20 Withdraw Consent in Get Apps



8:29 PM

Privacy

Privacy Policy

Personalized recommendations

Receive content recommendations based on your interests

Figure 4-21 Disable Personalization in Get Apps

4) Manage Data Collection for Analysis Purposes

You can allow or stop data collection for analysis purposes in Get Apps. Go to Settings > Password & Security > Privacy > User Experience Program, and then enable or disable the 'Enroll in User Experience Program' option.

5) Manage Ads

Personalized ads in this application are controlled by the 'Personalized Ads' option in the system settings. For details, please See [4.11 Advertising and Privacy]

Conclusion

At Xiaomi, user information security and privacy remain at the core of our operations. We are committed to protecting user data security and privacy.

The following Xiaomi privacy principles are deeply integrated into Get Apps:

- Use technical security audits to ensure the apps in Get Apps are secure.
- Provide controls for users to manage their data.
- Users can disable personalized ads, revoke authorization, and delete data at any time.

4.8 Mi Browser

Introduction

Mi Browser is a chromium-based web browser, which is pre-installed in MIUI system. Users can visit websites or stream news, videos, or other content in Mi Browser.

Mi Browser is easy-to-use and is designed to protect users' security and privacy. Mi Browser only collects the user data necessary to provide basic functions, personalized services, and user experience improvements. Mi Browser provides users with many privacy-friendly features described in Section 3.5, including incognito mode, Do Not Track, and browsing history clearing, which can help users to manage and protect their privacy.

Mi Browser is available in all markets, except for India.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	GAID	Identified	Personalization Advertising	HTTPS	Plain	180 days
Usage Data	Product Interaction	Pseudonymized	Analytics	HTTPS	Plain	90 days
	Advertising Data	Identified	Advertising	HTTPS	Plain	180 days
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS	Plain	90 days
	Performance Data	Pseudonymized	Analytics	HTTPS	Plain	90 days
Other Data	Content Consumption Data	Identified	Personalization	HTTPS	Plain	180 days

Data Collection and Usage

1) Browsing Websites

You can open any web page on the Internet with Mi Browser. Mi Browser does NOT collect the URLs of the web pages you visit.

2) Smart Address Bar

The search bar at the top of Mi Browser - the Smart Address Bar - provides a search function where users can enter website names, URLs, and keywords for searches. Mi Browser provides search suggestions to make searching easier. After you type in the search box, Mi Browser sends the search query keywords to the third-party search engine Bing.com to request the search suggestions. For example, if you type ‘Xiaom’ in the search box, the suggested keyword ‘Xiaomi’ will be listed under the search box for you, as it is probably the term you want to search for. See [Figure 4–22 Search Suggestions]

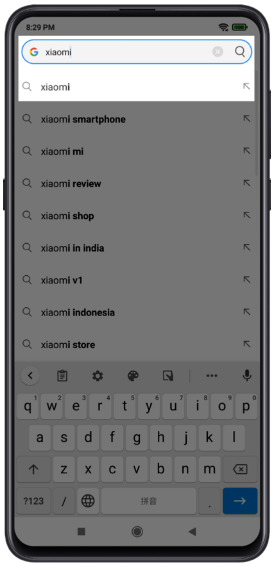


Figure 4–22 Search Suggestions

The search suggestion service is powered by Bing.com. Mi Browser does not keep any information during the process.

3) Data Synchronization

As described in 4.2 Xiaomi Cloud and Privacy, if synchronization for Mi Browser is enabled in Xiaomi Cloud, certain content, including the browsing history, bookmarks, and current tabs will be stored in the Xiaomi Cloud. We do not analyze this data or use it for any other purposes, including personalized recommendations.

4) Information Feeds and Personalization

Mi Browser provides users with personalized content in Information Feeds.

Mi Browser collects the **GAID**, **content consumption data**, and **information feed interaction data** for personalization purposes.

5) Analytics

Analytical data helps us find issues with the app and improve the user experience. Data collection for analysis purposes is controlled by our MIUI User Experience Program. For details, go to Settings > Password and Security > Privacy > User Experience Program > Learn more about User Experience Program.

Mi Browser collects certain **product interaction data**, such as the number of clicks on each module and page exposure, for analysis and improvement purposes. The data collected for this purpose is used in aggregated form and cannot be associated with a specific user.

6) Advertising

Mi Browser provides you with personalized ads. For detailed information regarding ads in MIUI, please refer to 4.11 Advertising and Privacy

Manage Your Privacy

1) Withdraw Your Consent

You can withdraw your Mi Browser consent by revoking the authorization at any time. Go to Mi Browser > My > Settings > Privacy and Security, and then disable the 'Authorization' option to withdraw your consent. See [Figure 4–23 Withdraw Consent]

Once the authorization option is disabled, Mi Browser will stop collecting data, and delete your data stored locally and in the cloud.

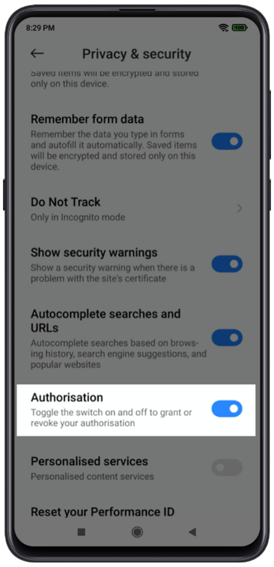
2) Disabling the Smart Address Bar

Go to Mi Browser > My > Settings > Privacy and Security, and then disable the 'Autofill Search Terms and URLs' option. See [Figure 4–24 Disable Smart Address Bar]

Once turned off, Mi Browser does not send any information to the search engine until the user initiates a search. Mi Browser does not provide search suggestions in incognito mode.

4) Manage Personalized Recommendations

You can disable personalized services at any time. Go to Mi Browser > My > Settings > Privacy and Security, and then disable the 'Personalized Services' option. See [Figure 4–25 Disable Personalization]



8:29 PM

Privacy & security

Saved items will be encrypted and stored only on this device.

Remember form data
Remember the data you type in forms and autofill it automatically. Saved items will be encrypted and stored only on this device.

Do Not Track
Only in Incognito mode

Show security warnings
Show a security warning when there is a problem with the site's certificate

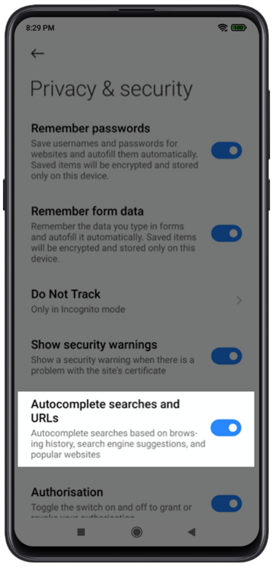
Autocomplete searches and URLs
Autocomplete searches based on browsing history, search engine suggestions, and popular websites

Authorisation
Toggle the switch on and off to grant or revoke your authorisation

Personalised services
Personalised content services

Reset your Performance ID

Figure 4–23 Withdraw Consent



8:29 PM

Privacy & security

Remember passwords
Save usernames and passwords for websites and autofill them automatically. Saved items will be encrypted and stored only on this device.

Remember form data
Remember the data you type in forms and autofill it automatically. Saved items will be encrypted and stored only on this device.

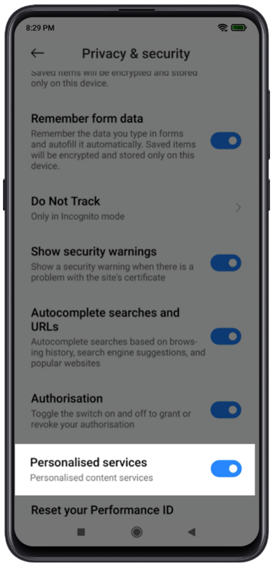
Do Not Track
Only in Incognito mode

Show security warnings
Show a security warning when there is a problem with the site's certificate

Autocomplete searches and URLs
Autocomplete searches based on browsing history, search engine suggestions, and popular websites

Authorisation
Toggle the switch on and off to grant or

Figure 4–24 Disable Smart Address Bar



8:29 PM

Privacy & security

Saved items will be encrypted and stored only on this device.

Remember form data
Remember the data you type in forms and autofill it automatically. Saved items will be encrypted and stored only on this device.

Do Not Track
Only in Incognito mode

Show security warnings
Show a security warning when there is a problem with the site's certificate

Autocomplete searches and URLs
Autocomplete searches based on browsing history, search engine suggestions, and popular websites

Authorisation
Toggle the switch on and off to grant or revoke your authorisation

Personalised services
Personalised content services

Reset your Performance ID

Figure 4–25 Disable Personalization

5) Manage Data Collection for Analysis Purposes

You can allow or stop data collection for analysis purposes in Themes. Go to Settings > Password & Security > Privacy > User Experience Program, and then enable or disable the 'Enroll in User Experience Program' option.

6) Manage Personalized Ads

Personalized ads in this application are controlled by the 'Personalized Ads' option in the system settings. For details, refer to 4.11 Advertising and Privacy

Conclusion

Mi Browser is committed the security and privacy of users' information and incorporates security and privacy design into the browser's features. Mi Browser also complies with the following rules:

- Follow data minimization principles.
- All information collected is subject to user consent.
- Users may revoke authorization at any time.
- Users can request to delete their data.

4.9 Mi Video

Introduction

Mi Video provides users with an easy way to watch videos on their smartphone. Mi Video offers local video management and an online video service. Users can search, watch, comment on, and share the online videos freely in the app.

Mi Video protects your privacy by default. Mi Video minimizes the amount of data needed to provide and optimize the services, and includes many features to help manage your data and protect your privacy.

Mi Video is available in all markets, except for India, United Kingdom, United States, Japan, and South Korea.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality	HTTPS, AES-128	Plain	Per user's request
	GAID	Identified	Advertising	HTTPS, AES-128	Plain	Per user's request
Search History	Search Keywords	Identified	App functionality	HTTPS, AES-128	Plain	Per user's request
User Content Data	Comments	Identified	App functionality Personalization	HTTPS, AES-128	Plain	Per user's request
Usage Data	Product Interaction	Pseudonymized	Analytics	HTTPS, AES-128	Plain	90 days
	Advertising Data	Identified	Advertising	HTTPS, AES-128	Plain	180 days
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS, AES-128	Plain	90 days
Others	Country or Region Setting	Identified	App functionality Personalization Analytics	HTTPS, AES-128	Plain	Per user's request
	Video Usage Data	Identified	App functionality Personalization	HTTPS, AES-128	Plain	Per user's request
	Channel Subscription	Identified	App functionality Personalization	HTTPS, AES-128	Plain	Per user's request
	Network Type	Pseudonymized	App functionality	HTTPS, AES-128	Plain	Per user's request
	Device and System Specs	Pseudonymized	App functionality	HTTPS, AES-128	Plain	Per user's request

Data Collection and Usage

1) Local Video File Management

Mi Video provides the basic functions for local video file management. When you only use the local Mi Video functions, we just collect the analytical data described in paragraph 6) Analytic. The local video viewing history is kept locally.

2) Trending and Video

When you use Mi Video to watch online videos and TV shows, Mi Video collects your **country or region settings**, **network type**, and **device and system specs** to match and provide suitable video content for you. See [Figure 4-26 Video Tab]

You can click the 'Like' icon, publish **comments** on videos, and add **channels** to your subscription list. Mi Video also collects your **video usage data** so that you can review your video viewing history.

Please note that if you are located in Russia, we may use the data collected in this function to provide a personalized recommendation service.

3) Video Search

To provide you with the most appropriate video recommendations and the search history function, Mi Video collects your **search keywords**. See [Figure 4-27 Video Search]

We may analyze these keywords to choose suitable, popular videos for recommendation.

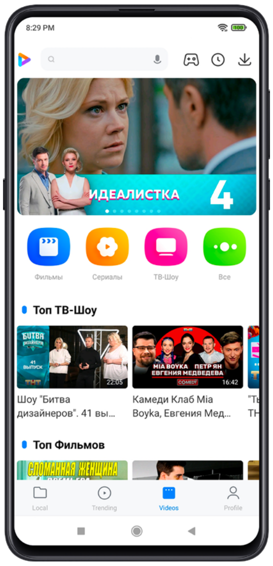


Figure 4-26 Video Tab

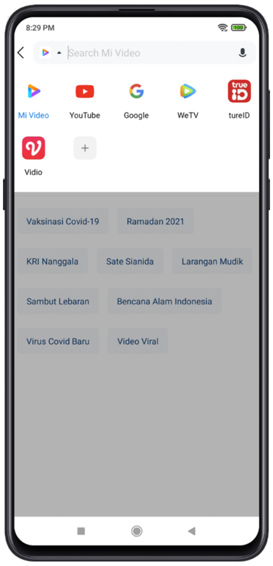


Figure 4-27 Video Search

4) Short Videos Provided by Third Parties

Short Video is a popular Internet service where users can watch short, looping video clips. The Short Video function in Mi Video is provided by third-party video content providers, including YouTube, Facebook, Instagram, and Twitter. The **hashed Google Advertisement ID** and the **video interaction data** are collected and shared with third parties during your use.

Depending on your choice of service, one of following privacy policies may apply.

- YouTube's Privacy Policy
- Facebook's Privacy Policy
- Instagram's Privacy Policy
- Twitter's Privacy Policy

5) Analytics

Analytical data helps us find issues with the app and improve the user experience. Data collection for analysis purposes is controlled by our MIUI User Experience Program. For details, go to Settings > Password and Security > Privacy > User Experience Program > Learn more about User Experience Program.

Mi Video collects the **network type**, **locale and region settings**, and certain **product interaction data** within the app, such as the number of clicks on each module and page exposure for analysis and improvement purposes.

Mi Video also collects **crash data** for troubleshooting and improvement.

6) Advertising

Mi Video provides you with personalized ads. For detailed information regarding ads in MIUI, please refer to 4.11 Advertising and Privacy

TIPS
You can learn more about how Mi Video collects and processes your personal information by reviewing the separate Mi Video Privacy Policy.

Manage Your Privacy

1) Access, Download, or Delete User Data in Mi Video

You can request to access, download, or delete the data in Mi Video by accessing the Privacy Center in Mi Account or by contacting us via Xiaomi Privacy Support.

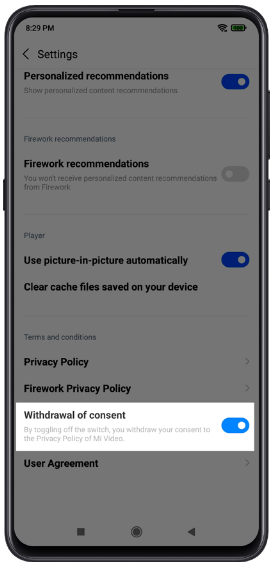
2) Withdraw consent

You can withdraw your consent in Mi Video settings. Go to Mi Video > Settings, and enable the 'Withdrawal of Consent' option. See [Figure 4-28 Withdraw Consent for Mi Video]

Once the option is enabled, Mi Video will stop collecting data, and delete your data stored locally and in the cloud.

3) Manage Personalized Recommendations

You can manage personalized recommendation services. Go to Mi Video > Settings, and then disable or enable the 'Personalized Recommendation' option. See [Figure 4-29 Disable Personalization]



8:29 PM

Settings

Personalized recommendations ●
Show personalized content recommendations

Firework recommendations

Firework recommendations ○
You won't receive personalized content recommendations from Firework

Player

Use picture-in-picture automatically ●

Clear cache files saved on your device

Terms and conditions

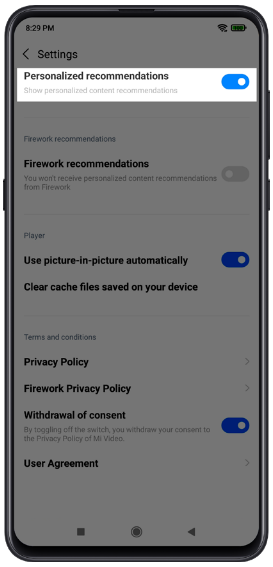
Privacy Policy >

Firework Privacy Policy >

Withdrawal of consent ●
By toggling off the switch, you withdraw your consent to the Privacy Policy of Mi Video.

User Agreement >

Figure 4–28 Withdraw Consent for Mi Video



8:29 PM

Settings

Personalized recommendations ●
Show personalized content recommendations

Firework recommendations

Firework recommendations ○
You won't receive personalized content recommendations from Firework

Player

Use picture-in-picture automatically ●

Clear cache files saved on your device

Terms and conditions

Privacy Policy >

Firework Privacy Policy >

Withdrawal of consent ●
By toggling off the switch, you withdraw your consent to the Privacy Policy of Mi Video.

User Agreement >

Figure 4–29 Disable Personalization

4) Manage Data Collection for Analysis Purposes

You can allow or stop data collection for analysis purposes in Themes. Go to Settings > Password & Security > Privacy > User Experience Program, and then enable or disable the 'Enroll in User Experience Program' option.

5) Manage Personalized Ads

Personalized ads in this application are managed by the 'Personalized Ads' option in the system settings. For details, refer to 4.11 Advertising and Privacy

Conclusion

Xiaomi is committed to helping protect users with leading privacy and security technologies that are designed to safeguard personal information. Mi Video is built with that commitment in mind.

The following Xiaomi privacy principles are deeply integrated into Mi Video:

- Minimize the amount of data collected by Xiaomi and shared with third parties.
- Provide transparency and control of data that is shared.

4.10 Mi Pay

Introduction

Mi Pay is a revolutionary, interoperable, secure, fast, and reliable payment app developed by Xiaomi. You can go on a fast and secured payment journey just by adding your bank account and creating a UPI ID.

Mi Pay is designed with your security and privacy in mind and only collects data necessary to provide services. All the data transmitted and stored in Mi Pay is securely protected.

Mi Pay is only available in India.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	Mi Account ID	Identified	App functionality Personalization Analytic	HTTPS, AES-128	Plain	Per user's request
	IMEI	Identified	App functionality	HTTPS, AES-128	AES-128	Per user's request
Device Info	SIM Card Slot Number	Identified	App functionality	HTTPS, AES-128	AES-128	Per user's request
Contact Info	Name	Identified	App functionality	HTTPS, AES-128	AES-128	Per user's request
	Email Address	Identified	App functionality	HTTPS, AES-128	AES-128	Per user's request
	Phone Number	Identified	App functionality	HTTPS, AES-128	AES-128	Per user's request
Financial Info	Card Number	Identified	App functionality	HTTPS	AES-128	Per user's request
	UPI ID	Identified	App functionality	HTTPS, AES-128	Plain	Per user's request
	Valid to Date	Identified	App functionality	HTTPS	AES-128	Per user's request
	Transaction Record	Identified	App functionality Analytics	HTTPS	Plain	Per user's request
Location	Precise Location	Pseudonymized	App functionality	HTTPS	Not stored	N/A
	Coarse Location	Identified	App functionality	HTTPS	Plain	Per user's request
Usage Data	Product Interaction	Identified	Analytics	HTTPS	Plain	Per user's request
Diagnostics	Crash Data	Pseudonymized	Analytics	HTTPS	Plain	Per user's request
	Performance Data	Pseudonymized	Analytics	HTTPS	Plain	Per user's request

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Other Data	Electricity consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Water consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	DTH consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Gas consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Broadband consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Landline consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Donation consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Education consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	FASTag consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Housing consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Insurance consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Loan consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Municipal services consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Tax consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Hospital consumer number	Identified	App functionality	HTTPS	plain	Per user's request
	Subscription consumer number	Identified	App functionality	HTTPS	plain	Per user's request

Data Collection and Usage

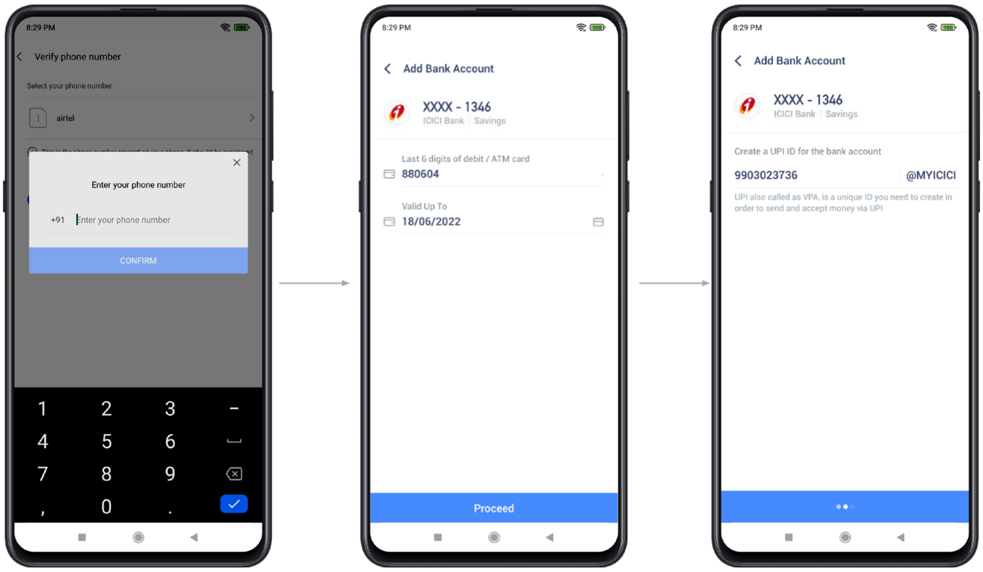
1) Add Bank Card and Create UPI Account

Before using Mi Pay to pay or transfer money, you are required to verify your phone number, add a bank account, and create a UPI account. See [Figure 4-30 Add Bank Card and Create UPI Account]

① When verifying a phone number, Mi Pay collects the **phone number** of the SIM card in your phone.

② When adding a bank account, Mi Pay collects the **card number** and **valid to date of your bank card** and sends them together with your phone number to the issuing bank for verification.

③ When creating a UPI account for the bank account, Mi Pay collects the **UPI ID** set by the user.



Add Bank Account
XXXX - 1346
ICICI Bank | Savings
Last 6 digits of debit / ATM card
880604
Valid Up To
18/06/2022

Add Bank Account
XXXX - 1346
ICICI Bank | Savings
Create a UPI ID for the bank account
9903023736 @MYICICI
UPI also called as VPA, is a unique ID you need to create in order to send and accept money via UPI

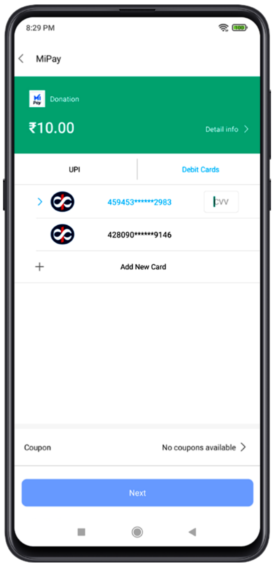
Figure 4-30 Add Bank Card and Create UPI Account

Mi Pay also collects **IMEI** and **slot number** of your SIM card to ensure the transaction security during all the processes above.

2) Payment

There are two ways to pay in Mi Pay: i) using a UPI account, ii) using a bank card

When you use a bank card, the **CVV** (card verification value) of your card is collected and sent to the issuing bank for verification directly. See [Figure 4-31 Bank Card Payments]Mi Pay doesn't collect and store the CVV of your card.



₹10.00
459453******2983
428090******9146
Coupon No coupons available

Figure 4-31 Bank Card Payments

Once the payment is finished, Mi Pay generates and keeps a **transaction record** for the payment, generally including the transaction ID, UPI ID, or pseudonymized card number of the payer and payee, payment amount, remarks, etc.

3) Money Transfer

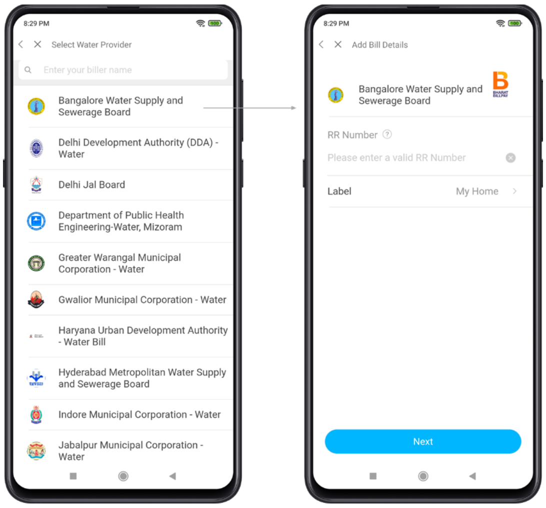
Mi Pay can use its Send Money function to transfer money to the chosen payee or use the Request Money function to receive money from the chosen payer.

When transferring money, Mi Pay collects the **UPI ID** and **name of the payee** if paid with UPI account; otherwise, it collects the **card number** if payment is through a bank account.

When receiving money, Mi Pay collects the **UPI ID** and **name of the payer** and then sends a payment request to the payer.

4) Utility Bill Payment

Users living in India can also pay their utility charges in Mi Pay, including landline bills, electricity bills, gas bills, water bills, broadband bills, and prepaid DTH connection accounts. To complete the payment, Mi Pay collects the **consumer number of the bill** to be paid, and sends it together with the phone number to the relevant service providers. The customer number may vary across different municipal agencies.



Bangalore Water Supply and Sewerage Board
Delhi Development Authority (DDA) - Water
Delhi Jal Board
Department of Public Health Engineering-Water, Mizoram
Greater Warangal Municipal Corporation - Water
Gwalior Municipal Corporation - Water
Haryana Urban Development Authority - Water Bill
Hyderabad Metropolitan Water Supply and Sewerage Board
Indore Municipal Corporation - Water
Jabalpur Municipal Corporation - Water

Bangalore Water Supply and Sewerage Board
RR Number
Please enter a valid RR Number
Label My Home

Figure 4–32 Utility Bill Payment

5) Analytics

Mi Pay may collect certain **product interaction data**, such as the number of clicks on each module and page exposure, **event data**, **performance data**, and **crash data** for analysis, troubleshooting, and improvement purposes.

TIPS
You can learn more about how Mi Account collects and processes your personal information by reviewing the separate Mi Pay Privacy Policy.

Manage Your Privacy

1) Access and Correct Data

- You can access the banded bank account through 'Bank accounts' in Mi Pay.
- You can access the UPI account through 'My UPI ID' in Mi Pay.
- You can access the transaction record through 'Transaction' in Mi Pay.
- You can access the consumer number and purchase history through functions such as 'DTH', 'Water', etc.
- You can correct your information by submitting a request to the Mi Pay team at mipayofficial@xiaomi.com.

2) Download Data Copy

You can download a copy of your personal information by submitting a request to us at mipayofficial@xiaomi.com. The copy collected and processed by us will be provided to you upon request free of charge.

3) Delete Bank Account

- You can delete the banded bank account using the 'Unbind' function in Mi Pay.
- You can delete all your UPI-related information from Mi Pay through the 'De-register' function.

4) Withdraw Consent or Delete Account

You can withdraw your consent for the collection, use, and/or disclosure of your personal information by submitting a request to the Mi Pay team at mipayofficial@xiaomi.com.

Conclusion

Xiaomi makes privacy and transparency a core component of the user experience. Mi Pay has prioritized its privacy default design from day one.

The following Xiaomi privacy principles are deeply integrated into Mi Pay:

- Follow data minimization principles.
- Provide transparency and control of data that is shared.
- All data processing procedures use the necessary security measures.
- Data protection complies with laws and regulations.

4.11 App Usage Data

App Usage

Introduction

‘App usage data’ refers to the data collected through the use of apps in the MIUI system. This data includes information on when and how you use MIUI apps on your device including: initial installation, first app launch, app usage, app updates, and app uninstallation.

This data enables Xiaomi to improve and enhance their services to ensure they continue to provide you with products of a high quality. Xiaomi uses the App usage data for various purposes, including analysis and app improvement, personalization, and advertisements.

Although app usage data will enhance your experience, should you wish not to share this data with Xiaomi, Xiaomi provides you with a method to turn off the collection of app usage data.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	GAID	Identified	Advertising	HTTPS	Plain	180 days
Usage Data	App Usage Data	Identified	Advertising	HTTPS	Plain	180 days
Other Data	Device and System Specs	Identified	Advertising	HTTPS	Plain	180 days
	Locale and Region Settings	Identified	Advertising	HTTPS	Plain	180 days
	Operator and network type	Identified	Advertising	HTTPS	Plain	180 days

Data Collection and Usage

1) The collection of app usage data

We use the following data to provide basic advertising services

The app usage data includes the following data elements:

- Identifier: **Google Advertising ID (‘GAID’)**.
- Device and Network Information: **device type**, **device specifications**, **operating system version**, **mobile operator**, and **connection type**.
- Event Data: this includes **data related to how you use the MIUI Apps**. The data collected is dependent on how you use the apps. In particular,

  △ Type 1: App usage sequence:

- App package name and version type.
- How you use the app including the opening and closing of the app, duration of use and your mobile operator and network type.
- This data is may be collected each several times a day you use an MIUI app.

△ Type 2: App status:

- App package name and version type.
- Language preferences.
- App status including initial download and installation (including download and installation source), first launch, updates and uninstallation.
- This data is collected when the relevant event occurs.

△ Type 3: Snapshot of installed apps:

- App package name and version.
- Installation (including installation source) and any recent updates.
- This data is generally collected once a day.

We don’t share any original app usage event data collected from your device with any other third parties .

2) The usage use of app usage data

We use the app usage data for the following purposes, including:

- Analysis and improvement of the MIUI Apps

We use app usage data to help us improve and analyze our products and services.

For this purpose, we aggregate and analyze relevant data to help us provide you with more useful products and services and understand the overall development trend of the industry.

Individuals cannot be identified through aggregated data, therefore it is treated as non-personal information.

- Personalization and advertisement

App usage data is also used to provide personalized services and advertisements to you.

For these purposes, we link the GAID with your relevant user data. This data is used to analyze your preferences and create personalized advertisements for you. We additionally use this data to recommend apps you may wish to install on your device.

As described in other sections of this white paper, you can control and prevent this type of data collection including the personalization of recommendations and personalized advertisement in the privacy settings of in our apps (see below).

Control Your Privacy

Control the collection of app usage data

You can turn off the collection of app usage data in the MIUI system settings. Please go to Settings > Passwords & security > Privacy > Usage and Diagnostics, and turn off the ‘Usage and Diagnostics’ switch;

You can also turn off the ‘Usage and Diagnostics’ switch during the out-of-box experience (OOBE).

Please note that turning off app usage data will not prevent your device from sending necessary telemetry data to Xiaomi which is needed for essential services such as system updates and security.

Conclusion

Respecting users’ privacy is one of Xiaomi’s core values. We strive to provide you with better products and services while protecting your privacy rights by:

- Providing transparency to our use of App Usage Data.
- Providing convenient controls for the collection for App Usage Data both in the OOBE and system settings.

4.12 Advertisement

Introduction

We provide app recommendation ads in our apps and system interfaces to help you discover more apps that you may be interested in. These ads allow us to provide you with most of our high-quality apps and services free of charge. These advertisements include non-personalized advertisements and personalized advertisements and may be provided directly by Xiaomi, or by third-party advertising platforms including Google and Facebook.

The information below is to help you to understand the types of data we collect and how your data is used, securely stored and retained for majority of advertisements you see in our apps and system interfaces as listed below. Xiaomi never uses your photos, recordings, and other files that you store in Xiaomi Cloud for advertising purposes. We also provide you with methods to turn off personalized advertisements, you will continue to receive non-personalized advertisements.

Data Inventory

Category	Type	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention
Identifiers	GAID	Identified	Advertising	HTTPS	Plain	180 days
Usage Data	Advertising Data	Identified	Advertising	HTTPS	Plain	180 days
	App Usage Data	Identified	Advertising	HTTPS	Plain	180 days
Other Data	Device and System Specs	Identified	Advertising	HTTPS	Plain	180 days
	Locale and Region Settings	Identified	Advertising	HTTPS	Plain	180 days
	Operator and network type	Identified	Advertising	HTTPS	Plain	180 days

Data Collection and Usage

1) Basic Advertising Services in MIUI

We use the following data to provide basic advertising services

- Identifier: **Google Advertising ID (‘GAID’).**
- Device and network information: **device type**, **operating system version**, **mobile operator**, and **network type**.
- **Advertisement interaction data**: how you interact with the advertisement, including click-rate and browsing history.

We collect this data to provide you with personalized advertising content, optimize how you view the ads and perform statistics and analysis on advertising effects.

2) Mi Ads Service and User Segments

Xiaomi's Mi Advertising Service uses personalized advertising content to create advertising recommendations. We do this by creating user segments based on individual characteristics, these segments are then used to deliver personalized advertisement. We may use the following information for user segmentation:

- **App usage data**: this includes how you use the apps on your smartphone, and initial download and installation (including download and installation source), first launch, updates and uninstallation.
- **Advertising interaction data**: this includes how you interact with advertisements, including click-rate and browsing history.

Our advertising services do not use the data stored in Xiaomi Cloud and Mi Pay.

3) Third-party Advertisement

When personalized advertisements are provided by third-party advertisement platforms, including Google and Facebook, the advertising content you receive is determined solely by the provider. Further information around how third-party advertising platforms collect and use your personal information can be found in their privacy notices. A detailed list of the third parties advertising platforms and providers can be found in the Section 8 of Xiaomi Privacy Policy.

Manage Your Privacy

Manage Personalized Ads

There are two ways to enable or disable personalized ads in MIUI.

① Go to Settings > Passwords & Security > Privacy > Ad Services > Personalized Ad Recommendations, and then disable the 'Personalized Ad Recommendations' option.

② Go to Settings > Google > Ads, and then enable the 'Opt out of Ads Personalization' option.

Conclusion

Privacy and security are fundamental to providing ad services at Xiaomi. We strive to provide you with better products and services while protecting your privacy rights by:

- Providing transparency to our advertisement services.
- Providing controls to personalized advertisement.
- Prohibiting the use of user content data for personalizing advertisement.

4.13 AI Technology

Introduction

In an era of intelligent interconnectedness, Xiaomi is committed to developing trustworthy artificial intelligence (AI) technologies to benefit and empower every user. We center on ‘human subjectivity’ and ensure that AI technologies are always used to enhance and enrich the user experience of consumer electronics products.

During the course of developing and implementing AI technologies, Xiaomi follows the internationally recognized values in the EU's Ethics Guidelines for Trustworthy Artificial Intelligence. We have also implemented the basic principles of trustworthy AI at Xiaomi, covering four aspects: **Security and Safety**, **Privacy**, **Fairness**, and **Explainability**.

We are dedicated to protecting our users' privacy and personal data in line with high standards throughout the AI life cycle and aim to achieve best practice, rather than mere compliance with laws and regulations. For instance:

- We guarantee that our AI technology products and services comply with the principle of data minimization and only collect the data necessary to provide relevant services.
- **We never use users' data to train AI systems.** All training data comes from legitimate sources and has been reviewed for compliance.
- We try our utmost to avoid any risks during the transmission of user data by deploying AI algorithms on the local device.
- We use multiple encryption technologies to ensure the security of the algorithm operating environment as well as the storage of user data.

Xiaomi applies AI technology to the following services in our smartphones:

Voice Call Noise Reduction	Camera Image Optimization
Face Unlock	Fingerprint Unlock

Voice Call Noise Reduction

Voice call noise reduction aims to enhance voice information between callers by suppressing ambient noise. This ensures clearness and the effectiveness of every call, and enhances the user's remote phonic communication experience. Voice call noise reduction AI algorithms are applied to calling scenarios and are available on all Xiaomi smartphones.

Xiaomi does not collect or upload any user data through voice call noise reduction. The noise reduction AI algorithm only operates on the device and outputs results in real-time without preserving any data locally or transmitting it to our servers.

Camera Image Optimization

The camera image optimization AI algorithm is mainly used in the following camera features: Super Moon, AI Camera, Document Mode, Front Portrait Mode with Background Blurring, and Beautify. These features enable users to easily take amazing photos without complicated post-processing.

Xiaomi does not collect or upload any user data through camera image optimization. The algorithm only runs on the device. When the photo is being processed by the algorithm, the photo also stays on the device. Xiaomi has built a framework for the image optimization algorithm to minimize the security risks in the algorithm's operating environment.

Face Unlock

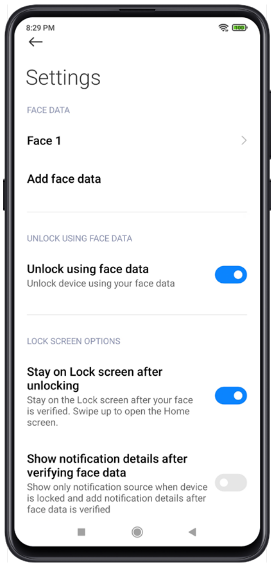
Face Unlock is based on biometric authentication technology, which is powered by the facial recognition AI algorithm. The algorithm intelligently detects facial features and performs high-precision matching, allowing users to quickly unlock and access their devices simply by looking at the device screen. This function is an optional function for users. Because passwords are the basis for users protecting their personal data through encryption, users need to enter a password before turning the Face Unlock function on or off.

The facial recognition AI algorithm is integrated and runs locally on the device. The algorithm only runs on the device. We will not upload any user's facial images or facial feature information to our servers, thereby largely avoiding any security and privacy risks during the data transfer process. The facial recognition AI algorithm irreversibly extracts the facial feature information from the face image, and the original face image will not be saved afterward. The facial feature information is only used for the face unlock function and is not used for personalization, analysis, or advertising purposes.

Users have full control of the face unlock function. Users can manage the face unlock function. Go to Settings > Passwords and Security > Face Unlock. Password verification is needed before entering the Face Unlock settings. See [Figure 4-34 Face Unlock]

- The Face Unlock function can be turned on or off at any time.
- Facial feature information can be added, renamed, and deleted.
- When adding facial feature information, the user's identity authorization and express consent are also required.
- After the Face Unlock function is turned off, the facial feature information will not be deleted automatically. Users need to delete it manually.

- When factory settings are restored, facial feature information is deleted automatically.



8:29 PM

Settings

FACE DATA

Face 1

Add face data

UNLOCK USING FACE DATA

Unlock using face data
Unlock device using your face data

LOCK SCREEN OPTIONS

Stay on Lock screen after unlocking
Stay on the Lock screen after your face is verified. Swipe up to open the Home screen.

Show notification details after verifying face data
Show only notification source when device is locked and add notification details after face data is verified

Figure 4-34 Face Unlock

Fingerprint Unlock

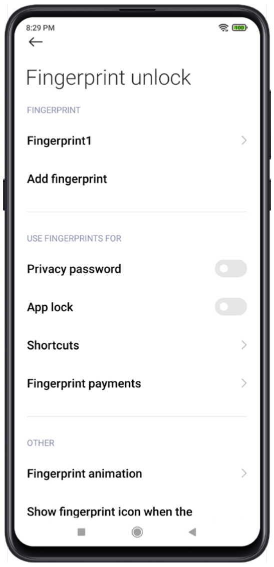
Fingerprint Unlock is based on biometric authentication technology. After users turn this function on, they only need to place their fingers on the fingerprint sensor to quickly unlock their device without needing to enter a long and complex numeric or graphical password each time. This function is an optional function for users. To protect user security and privacy, the Fingerprint Unlock service is restricted in the following scenarios:

- When the user's device has just been turned on.
- If the device has not been unlocked using a password for more than 72 hours.
- If the Fingerprint Unlock function fails to unlock the user's device five times in a row.

The fingerprint recognition AI algorithm is integrated and runs locally on the device. While in use, the user's fingerprint data will not leave the device, nor will it ever be backed up or uploaded to our servers. When adding a fingerprint template, the device only saves the extracted fingerprint feature information, not the original fingerprint biometric information. The fingerprint recognition algorithm operates on the Fingerprint TA in a TEE environment. Applications that support fingerprint authentication can only initiate fingerprint authentication requests and receive authentication results from the Fingerprint TA in the TEE environment through the external fingerprint framework. These applications cannot directly access the fingerprint templates.

Users have full control of the Fingerprint Unlock function. Users can manage the Fingerprint Unlock function. Go to Settings > Passwords and Security > Fingerprint Unlock. Password verification is needed before entering the Fingerprint Unlock settings. See [Figure 4-35 Fingerprint Unlock]

- The Fingerprint Unlock function can be turned on or off at any time.
- Fingerprint template information can be added, renamed, and deleted.
- When factory settings are restored, fingerprint template information is deleted automatically.



8:29 PM

Fingerprint unlock

FINGERPRINT

Fingerprint1

Add fingerprint

USE FINGERPRINTS FOR

Privacy password

App lock

Shortcuts

Fingerprint payments

OTHER

Fingerprint animation

Show fingerprint icon when the

Figure 4-35 Fingerprint Unlock

Conclusion

Xiaomi is committed to privacy and security in the design phase of its products. The following privacy principles are deeply integrated into Xiaomi AI Technologies:

- Provide transparency of and control over data collected through Xiaomi AI.
- Minimize the amount of data collected by AI technologies.
- Only use data for the functions users actually need.
- Consider security when designing Xiaomi AI.

05

International Data Transfer

International Data Transfer

Xiaomi processes and backs up personal information through a globally operated and controlled infrastructure. Your data is transmitted by encrypted communication channels and stored by global top−tier cloud service providers. For the purposes described in our Privacy Policy, your information may be transferred to these data centers in accordance with the applicable laws.

The table below provides detailed information about cloud service providers and data storage locations for users in different regions.

Region	Cloud Service Providers	Data Storage Locations
European Union	Amazon Web Services	Germany, United States
	Alibaba Cloud	Singapore
India	Amazon Web Services	India
	Microsoft Azure	India
Russia Federation	Kingsoft Cloud	Russia
United Kingdom	Amazon Web Services	Germany, United States
	Alibaba Cloud	Singapore
Mainland China	Kingsoft Cloud Alibaba Cloud 21ViaNet	Mainland China
Others	Amazon Web Services	United States
	Alibaba Cloud	Singapore

If you use our products and services in the EEA, Xiaomi Technology Netherlands B.V. will act as the data controller, and Xiaomi Singapore Pte. Ltd. is responsible for the data processing. Xiaomi's international transfer of personal data collected in the EEA is governed by EU Standard Contractual Clauses.

06

Security and Privacy Certifications

Security and Privacy Certifications

Xiaomi has been widely recognized by globally recognized third-party information security and privacy protection agencies. The information security and privacy certifications we have obtained are the best embodiment of our leadership on and commitment to internationally recognized privacy and security standards.

ISO/IEC 27001:2013 Certification

ISO/IEC 27001 has developed into the most authoritative, rigorous, and most widely accepted information security management standard in the world. This certification means that Xiaomi has met the requirements of international standards and fulfilled our commitment to users.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED

ISO/IEC 27018:2019 Certification

ISO/IEC 27018 is the first international code of conduct focusing on the protection of personal information in the cloud. This certification indicates that Xiaomi has effectively established a cloud data security and privacy management system aimed at protecting users' data stored in the cloud.

bsi
ISO/IEC
27018
Personal Data in the
Cloud
CERTIFIED

ISO/IEC 27701:2019 Certification

ISO/IEC 27701:2019 is the latest international standard designed solely for privacy protection. It effectively integrates privacy protection practices into the information security management system. This certification illustrates that Xiaomi maintains privacy protection best practices.

bsi
ISO/IEC
27701
Privacy Information
Management
CERTIFIED

TRUSTe Enterprise Privacy Certification

TRUSTe certification is a privacy and data governance framework created by TrustArc, a certification organization specializing in privacy protection. This certification shows that Xiaomi has established an internationally recognized privacy compliance management system.

TRUSTe
Certified Privacy
Powered by TrustArc

You can learn more about our security and privacy certifications in Xiaomi Trust Center.

07

Overall Conclusion

Overall Conclusion

Respect for user privacy has always been among Xiaomi's core values. As the core component of Xiaomi smartphones, MIUI takes the responsibility of building a foundation of trust seriously. MIUI gives priority to protecting user privacy. This White Paper is a comprehensive presentation of MIUI's privacy features and practices. We hope that this White Paper can help you better understand our privacy practices.

As mentioned in this White Paper, Xiaomi has adopted the concept of privacy by design in our product development process, and is consistently trying to use more innovative technologies and methods to protect privacy. Xiaomi strives to put security and privacy protection awareness at the heart of every one of its business departments, employees, and business partners.

Xiaomi will continuously strengthen its privacy practices, refine the security and privacy protection features of its products and services, and optimize its security and privacy management system. This will be continually demonstrated through certifications, white papers, privacy policies, and other means so that Xiaomi can build user confidence in Xiaomi's products and services, allowing users to choose and use Xiaomi products and services with even greater peace of mind.

In an era driven by big data and artificial intelligence, there will always be contradictions between corporate development and user privacy. However, Xiaomi firmly believes that by respecting and protecting user information security and privacy, it can build long-term trust in Xiaomi products. Xiaomi insists on putting information security and privacy protection above all else, and continually increasing its investment in security and privacy. Xiaomi is committed to sharing its standardized methods, best practices, and technical capabilities relating to information security and privacy protection with its partners, so that we can grow and protect user privacy together.

To learn more about the security and privacy practices of Xiaomi, go to trust.mi.com