XIAOMI IOT PRIVACY WHITE PAPER

June 2021

Statement

This document should be used as a reference guide for users of Xiaomi Inc. and its affiliated companies (hereinafter referred to as “Xiaomi”, “us”, or “we”) products and services to understand the information security and privacy protection of Xiaomi IoT products and services. However, there are certain functions or features only available for some of the devices or regions. Due to the potential problems such as technological upgrading, product iteration, changes in applicable laws and regulations, and consistency of wording, Xiaomi hereby declares that it does not make any express or implied guarantee for the completeness, accuracy, and applicability of the contents hereof.

Due to 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 any errors occur in this document or you have any questions about the contents hereof, please contact us via Xiaomi Privacy Support.

Content

01

Overview

Xiaomi has the world–leading consumer IoT platform – Xiaomi/Mi Home. To date, more than 351[1] million smart devices have been connected to Xiaomi/Mi Home. However, the rapid increase in the use of IoT devices has also caused increasing concern among users over the privacy and security of their personal data.

Respecting users’ privacy has always been among Xiaomi’s core values. Xiaomi frequently insists on the concept of ‘security and privacy by design’ in creating IoT products.

Based on the principle of Transparency (as later defined), we have published this IoT users’ privacy white paper, which aims to demonstrate our privacy protection practices and what we have done to protect your data in each of our products and services. We have included six products and associated three mobile applications in this white paper, and have included details that will enable you to develop a full understanding of how we collect, use, and store data, as well as how you can control your data. Our aim is help you to better understand the Xiaomi IoT privacy protection practices.

Chapter 1 – Overview introduces the basic introduction of xiaomi IoT platform, the purpose and structure of this white paper.

Chapter 2 – Privacy Governance introduces Xiaomi’s privacy governance situation. In this chapter, you can understand that Xiaomi has built mature privacy governance and management system in the company, which lays a solid foundation for privacy protection.

Chapter 3 – Xiaomi IoT Products and Privacy introduce the privacy practice for 6 main types of IoT products and 3 connected mobile applications. You can get all the details of data collections and usages, and specific privacy features for each devices. To provide a simple, clear statement and to improve the understanding of our data collection and usage practice, we refer to most of the concepts from 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 statement, 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 references the standard.

Chapter 4 – International Data Transfer introduces our international data storage and transfer practice. In this chapter, you can learn about our cloud service providers, the storage locations for user data, and our compliance mechanism for international data transfer.

Chapter 5 – Control Your Privacy in IoT Products introduce how you can control your privacy in IoT products via different mobile applications. There are details screenshot or description of different user access right when you connect your device by using different mobile applications.

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

Chapter 7 – Conclusion: an overall summary for the whole white paper to emphasize the privacy protect principles, privacy development integration of our IoT products, and how we improve our technology, process and any other related practice continuously.

We strive for more transparency in this White Paper and hope that all Xiaomi users, developers, partners, and relevant regulatory authorities can better understand the privacy practices in Xiaomi.

[1] Data statistics from Q1 2021 Xiaomi Financial Report.

02

Privacy in Xiaomi

2.1 Privacy Governance

Dating back to 2014, Xiaomi established the Information Security and Privacy Committee and appointed a Chief Privacy Officer to manage and coordinate the 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 teams of Information Security and Privacy, Legal, Internal Audit and Supervision, Cooperates Communications, Human Resources and all the business units in the company, including but not limited to smart phones, 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 assessment, overseeing and managing privacy risks and at all stages of product development and operations, as well as developing and promoting of privacy enhancement technologies.

Following the ISO/IEC 27701 Privacy Information Management System (PIMS), Xiaomi has established the privacy protection framework that covers user communication, 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 product or service of Xiaomi available on the market has undertaken a privacy impact assessment internally, which covers such aspects as data collection, storage, use, and destruction.

We provide users with a copy of our Privacy Policy and ask them for consent when they use our product or service for the first time. We also provide choices and controls for users to manage their data as easy as possible.

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 the concepts and practices of security and privacy protection. Additionally, we provide various professional privacy training courses, covering the topic of privacy laws, management, and technology, for our engineers, specialists, and professionals in different departments. Since 2020, we also host Information Security and Privacy Awareness Month every year in the company to raise security and privacy awareness among our employees and affiliates.

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

We conduct due diligence on business partners and third-party service providers to make sure 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, ISO/IEC 27701, and TRUSTe Enterprise Privacy certifications and carry out yearly third-party audits to maintain these certifications.

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, standard, and process.
Control	We seek to provide you with simple and easy-to-use methods to help you control 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 Privacy Policy explains how Xiaomi collects, uses, processes, discloses, and protects the personal data collected from users. Xiaomi Privacy Policy consists of the General Privacy Policy, and the 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 this Privacy Policy, while the Separate Privacy Policy only applies to the specific product or service. Based on the functions of each model of IoT products, Xiaomi will provides a separate privacy policy for the devices, this separate privacy policy will receive priority application,you can easily get the privacy policy in your connected mobile application(for example, Mi Home plug-in-device-settings). While anything that is not specifically covered shall be subject to the terms of this Privacy Policy.

We review the Privacy Policy periodically and may update it. If we make a material change to this Privacy Policy, we will send the notification via email or publish it on Xiaomi websites or notify you via mobile applications which you connect with your devices. Where required by applicable laws, 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 Technology

Xiaomi established the IoT Security Lab in 2015 to provide the technical testing for the security/privacy vulnerabilities and compliance assessment for our IoT products. All Xiaomi IoT products must pass the privacy impact assessment, privacy testing, security assessment, and security testing to validate the privacy design before they are made available on the market. On-sell products will also be monitored 24/7 hours on the IoT Security and Privacy Platform.

As the world’s leading consumer IoT device platform, we provide to our manufacturers components that have built-in security and privacy features, such as the Mi Home security element and unified module(Wi-Fi, Mesh, BLE), which help improve the privacy protection experience.

We are committed to applying privacy technologies in IoT products, such as Edge Computing. Our MACE Lite framework has been applied to wearable devices, which can reduce data collection and helps keep data more secure.

2.5 User Requests and Complaints

We provide various tools and methods for users to exercise their data rights. Users can request to access, correct, or delete the data collected by visiting Privacy Support. We also receive and respond to the comments, questions, and complaints from users in Privacy Support.

2.6 Transparency Report

We respond to personal information requests for legitimate purposes from government agencies and authorities around. 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 disclose the information about the personal information requests every year.

03

Xiaomi IoT Products and Privacy

3.1 Overview

In this section, we provide additional details on our privacy practices related to the main IoT products and related mobile application, including Mi Smart Band (connected with Mi Fit and Xiaomi Wear), Mi Smart Scale, Mi Robot Vacuum, Mi Scooter, Mi Router, Mi Camera, Xiaomi / Mi Home and Xiaomi Wear.

The content for each application and product normally consists of the following sections:

- **Introduction**, which introduces the general information and functions of each product.
- **Data inventory**, which summarizes the data collection and usage in a table for the application or service. The data inventory includes the data types we collect, the identification qualifier of the data, the purpose for collecting them, the encryption methods when the data is in transit and at rest, and the data retention policy. The concepts of data types, identification qualifier, and purpose are derived from ISO/IEC 19944-1:2020.
- **Data collection and usage**, which details the data collection and usage for each function of a certain application or service. The relevant introduction can be considered as the data use statement defined in ISO/IEC 19944-1:2020.
- **Privacy by design**, which summarizes the privacy features of each product, and how these features can help protect your privacy.

3.2 Mi Smart Band and Privacy

Introduction

The Xiaomi Mi Smart Band is an activity tracker wristband that can be connected to a mobile device and managed via the Mi Fit and/or Xiaomi Wear mobile applications.

The Mi Smart Band can be used to monitor the user’s heart rate, calculate calories burned in different fitness modes, monitor sleep patterns, and receive various notifications from the mobile device it is synced to. Some models also provide NFC function and the SpO_2 tracking. The Mi Smart Band night protection function can monitor your nightly blood oxygen saturation levels and analyze your breathing quality during sleep, so that you can keep track of your own sleep quality.

Based on the principle of data minimization, the Mi Smart Band limits data collection to that which is only necessary from Xiaomi to provide services and a good user experience. There are also certain configurations that provide a ‘control your privacy’ feature which enables users to delete, download or access certain aspects of their data.

Data collection and usage

1) Pairing with device and synchronizing data

When logging into the Mi Fit app through your Mi Smart Band, WeChat, Apple(for iOS), Google or Facebook accounts, we will collect your credentials, avatars, gender, email address as well as time zone, language and region of your phone to provide the Mi Fit account and profile page for you.

When you use Mi Fit to connect to the Mi Smart Band, we will collect the **MAC address, serial number, firmware version of the device, system time, operating system version** and **brand model of your mobile device** to offer firmware or software updates and factory settings. If you add the world clocks function in Mi Fit, we will calculate the local time corresponding to your selected region based on the time of your mobile device, and display this on Mi Fit and the device as part of this function.

2) Calculating exercise results

When you activate Mi Fit, we will collect your **personal body information**, which includes your date of birth, height and weight. When you use the device for exercise, we will collect the **exercise information**, which includes the number of steps taken at any given time, your PAI[1], time of measuring, exercise targets, achieved exercise targets, weight target, stride frequency, stride length, calories burned, stroke times, stroke velocity, stroke length, swimming duration, swim index, stroke speed, resistance value, distance, swimming style, pace and duration of exercise.

We use **personal body information** and **exercise information** to accurately calculate your visceral fat level, and calories burned. Such information helps us provide the exercise functions.

3) Physical analysis

You can use Mi Fit to synchronize **device data**, which includes activity information, sleep patterns, blood oxygen saturation information, information relating to your heart rate at various times of the day, and your weight.

Based on the **personal body information** and the **device data**, we will provide you with an analysis related to your physical condition for your reference. For example, according to your personal data and body composition, we can provide a suggested ideal body weight interval value and present your current/whole-day value and/or tendency to you. Furthermore, we will use **personal body information** and the **device data** to provide you with the sleep function, which will display your sleep score, sleep time, REM, sleep duration distribution and breathing quality during sleep on Mi Fit.

4) Blood oxygen measuring

When you try to use the **blood oxygen measuring** function, we will calculate your **blood oxygen saturation** information and the changes in it to demonstrate you the value or to assist in sleep analysis.

5) Notification display

When you use the phone call, SMS, or application message notification function (**this function is disabled by default**), you will receive an alert relating to your phone calls, SMS or application messages on your device, the **incoming call, text messages and caller information** will be displayed on the device (some devices may not support this feature). **This information will only be displayed on the device screen and will not be stored.**

[1] PAI is a health assessment system that uses an algorithm to transform complex information such as heart rate, activity duration, and other health data into a single numerical value unique to each user.

6) Network usage

We will collect information (such as network type and network signals) relating to certain features of Mi Fit to offer firmware or software updates.

7) Music control

When you use the music control functions, we will collect the music information (such as the name of the song, volume level, and the status of the song) from your phone and synchronize it to the device. **This information will only be displayed on the device screen and will not be stored.**

8) Mi Smart Band unlocking

When you use the Mi Smart Band with the off–wrist lock function, the Mi Smart Band will be locked when the device detects that it is not being worn. If the wrong password is entered in the device more than a certain number of times, it will prompt you to change the Mi Smart Band unlock password on Mi Fit or restore the factory settings on Mi Smart Band. We will collect your **Mi Smart Band unlock password** to provide this function.

9) Information from Friends

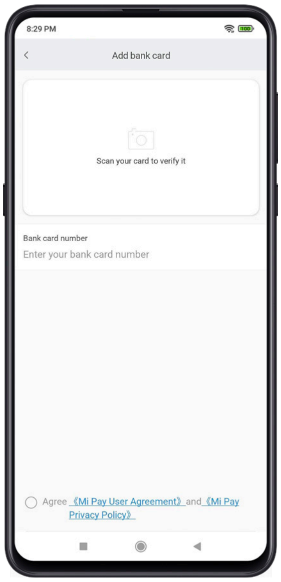
Mi Fit allows you to add friends through the Friends functionality. After receiving permission from your friends, we will collect information regarding the relationship with your friends, as well as the activity and sleep pattern data of your friends.

10) Near Field Communications (NFC)

In some countries or regions, devices with NFC can provide NFC functions for MasterCard payment. You can use MasterCard through the device after you have verified your MasterCard successfully. For verifying the card, the bank (SDK) will collect the **card information** directly (**Mi Fit/Xiaomi Wear will not collect these information**), which includes **card number, name of the card holder, validity date of the card, CVC2** (CVC2 is the last three digits of the number printed on the signature panel on the back of the card)**, bank reserved mobile number, and bank reserved email address.**

The bank will collect your **transaction information** to provide you with services such as topping up your card or completing transactions via NFC. Such **transaction information** includes the **amount, order number, and product description.**

To avoid confusion, the **card information** and **transaction information** are collected by the bank directly. We will only collect the name of your bank, and the last four digits of the physical card number and device card number once the MasterCard authentication has been passed, with this information only being stored on the device (Mi band and phone) securely.



8:29 PM

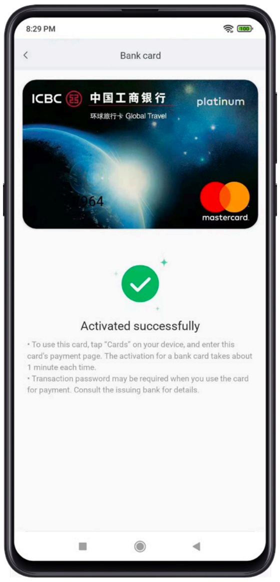
Add bank card

Scan your card to verify it

Bank card number

Enter your bank card number

○ Agree 《Mi Pay User Agreement》 and 《Mi Pay Privacy Policy》

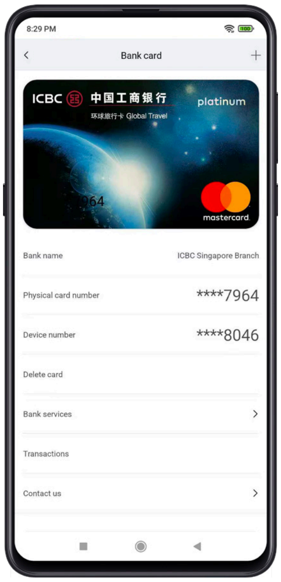


8:29 PM

Bank card

Activated successfully

- To use this card, tap "Cards" on your device, and enter this card's payment page. The activation for a bank card takes about 1 minute each time.
- Transaction password may be required when you use the card for payment. Consult the issuing bank for details.



8:29 PM

Bank card

Bank name	ICBC Singapore Branch
Physical card number	****7964
Device number	****8046
Delete card	
Bank services	>
Transactions	
Contact us	>

11) Female health

You can record certain information relating to your menstrual cycle on Xiaomi devices that support this function or in Mi Fit. If you enable the physiological period intelligent prediction mode (**this function is disabled by default**), we will collect information regarding the **duration of menstruation, menstruation intervals, the start/end date of your menstruation cycle, and your physical condition/mood during your menstruation cycle.** This information will be used to predict your menstrual period and offer you reminders based on the information you fill in. We also offer training courses for you based on your physical condition during menstruation.

12) Location-based services

We will collect location information (based on the mobile phone's GPS) to provide you with specific services (for example, workout trace information recorded by the Mi Fit, location optimization weather function, or map information). You can turn off the location function at any time by changing your app settings.

13) User feedback

We will collect **feedback, user ID, contact information, logs** (including **crash logs** and **performance logs**), **device name, type,** and **time of app or device issues you provide us.** The feedback you provide is extremely valuable in helping us improve our services and offering troubleshooting solutions. To follow up on the feedback provided by you, we may communicate with you using the contact information (e.g., an email address) that you have provided and keep records of such communications.

14) Analytics

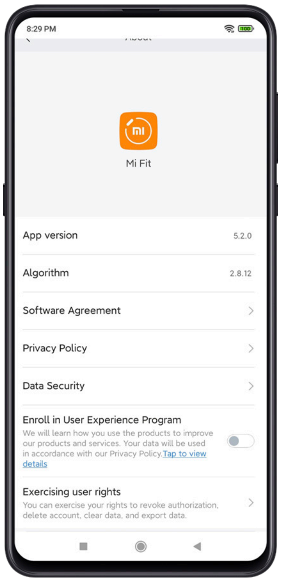
We will collect product interaction data (e.g., number of clicks, failed connections, and viewing activities) on the Mi Fit application. We use such pseudonymized data to help us improve our products and services.

Privacy by design

Mi Smart Band only collects the data which is required to perform its functions. Some of the functions, such as blood oxygen measuring, notification display, and female health functions, are disabled by default to avoid extra data collection. Furthermore, some of the data is processed only on the relevant device and is not sent to a central server. For example, when you use the notification display and music control function, the data will only be displayed on the device screen and we will not store this information.

To maximize the security of your data, all the data in transit is encrypted via HTTPS, while data such as GPS as well as blood oxygen related information and heart rate related information are encrypted at rest.

In addition to providing basic functions for supporting user access rights (such as access, deletion, download, etc.), we will consider the collection of some sensitive data to give users fully control at the early stage of product design, For example, you can change your mobile application settings(refer to below screenshot) of your band to not upload workout trace information to the server, even if the Mi Fit application has obtained location permissions from your phone.



Mi Fit

App version 5.2.0

Algorithm 2.8.12

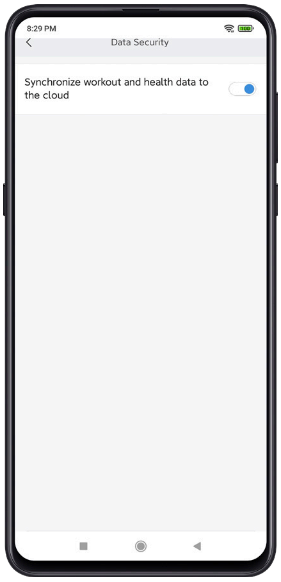
Software Agreement

Privacy Policy

Data Security

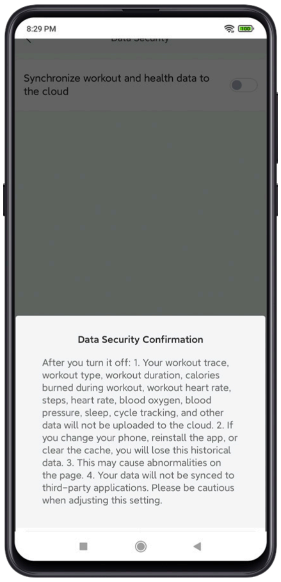
Enroll in User Experience Program ○
We will learn how you use the products to improve our products and services. Your data will be used in accordance with our Privacy Policy.Tap to view details

Exercising user rights
You can exercise your rights to revoke authorization, delete account, clear data, and export data.



Data Security

Synchronize workout and health data to the cloud ●



Synchronize workout and health data to the cloud ○

Data Security Confirmation

After you turn it off: 1. Your workout trace, workout type, workout duration, calories burned during workout, workout heart rate, steps, heart rate, blood oxygen, blood pressure, sleep, cycle tracking, and other data will not be uploaded to the cloud. 2. If you change your phone, reinstall the app, or clear the cache, you will lose this historical data. 3. This may cause abnormalities on the page. 4. Your data will not be synced to third-party applications. Please be cautious when adjusting this setting.

Appendix 1: Data Inventory for Mi Smart Band

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	MAC	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	SN	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
Contact information	Email address	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	Encryption	**App&cloud:** Per user request
	Country	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	City and district	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
Financial information	Card number	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	**Device:** No encryption , only display limited number front and end, others mask with * **Cloud:** Not stored	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Financial information	CVV	For NFC, bank collect directly	App/device functionality	–	–	Depends on bank which user chooses
	Validity date		App/device functionality	–	–	Depends on bank which user chooses
	Transaction record		App/device functionality	–	–	Depends on bank which user chooses
Sensitive information	Personal body information (height, weight)	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	Encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	Sleep information	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		
	Blood oxygen saturation	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		
	Heart rate according to time, resting heart rate, heart rate for whole day	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		
	Duration of menstruation, menstruation intervals, the start/end dates of your menstruation cycles, and physical condition/ mood during menstruation	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS		

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Location	Precise location (workout trace)	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	Rough location	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
User content	Other user content	For caller and message notification, only to display on device	App/device functionality	-	-	**App&cloud:** Not stored
Usage Data	Product interaction	Pseudonymized data	Analytics	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Other usage data	Pseudonymized data	Analytics	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
Diagnostics	Crash data	Identified data	Analytics	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
Other data	Avatars	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Gender	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Date of birth	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Exercise information (number of step, health score, time of measuring, exercise targets, achieved exercise targets, weight target, stride frequency, stride length, calories, stroke times, stroke velocity, stroke length, swimming duration, swim index, stroke speed, resistance value, distance, swimming style, pace and duration of exercise)	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Name of song	Only to display on device	App/device functionality	-	Not stored	-
	Volume	Only to display on device	App/device functionality	-	Not stored	-
	The status of song	Only to display on device	App/device functionality	-	Not stored	-

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Firmware version	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	System time of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Operating system version of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Brand model of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Mi Band unlock password	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	Encryption	**App&cloud:** Per user request
	Activity and sleep records of user's friends	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request

3.3 Mi Smart Scale and Privacy

Introduction

The Mi Smart Scale uses a G-shaped manganese steel sensor and Bluetooth low energy 5.0. It can weigh users and offer an in-depth health analysis. Based on BIA fat measurement, it provides 13 body composition metrics. It is available globally, and is controlled using the Mi Fit application.

Based on the principle of data minimization, the Mi Smart Scale only limits data collection to that which is only necessary for Xiaomi to provide services and a good user experience, with some functions being disabled by default to avoid extra data collection. There are also certain configurations which provide a ‘control your privacy’ feature that enables users to delete, download or access their data more freely.

Data collection and usage

1) Pairing with device and synchronizing data

When logging into the Mi Fit app through your Mi, WeChat, Apple(for iOS), Google or Facebook accounts, we will collect your credentials, avatars, gender, email address as well as time zone, languages and regions of your phone to provide the Mi Fit account and profile page for you.

When you use Mi Fit to connect to the Mi Smart Scale, we will collect the **MAC address, serial number, firmware version of the device, system time, operating system version,** and **brand model of your mobile device** to offer firmware or software updates and factory settings. If you add the world clocks function in Mi Fit, we will calculate the local time corresponding to your selected region based on the time of your mobile phone, and display this on Mi Fit and the device as part of this function.

2) Calculating body fit results

When you activate Mi Fit, we will collect your **personal body information**, which includes your date of birth, height and weight. This information is used to accurately calculate the body fit result, such as **BMI, muscle mass, body fat percentage, moisture content, protein, basal metabolism, visceral fat level, bone mass content, body shape, body age, and calories burned.**

3) Physical analysis

You can use Mi Fit to synchronize **data collected by the device** (“**device data**”). This includes weight information and bioelectrical impedance data.

Based on the **personal body information** and the **device data**, we will provide you with a physical analysis related to your physical condition for your reference. For example, according to your personal data and body composition, we can provide you with a suggested ideal body weight interval value for your reference and present to you your current weight.

4) Network usage

We will collect information such as network type and network signals, relating to certain features of the Mi Fit to offer firmware or software updates.

5) Guest information

When using the guest function, a guest is able to experience the device and certain limited services. The data of the guest (such as gender, height, and date of birth) will be collected and used to calculate and present the results of certain services experienced by the guest. The user can choose whether to save such information in Mi Fit. If the user decides to save the information, an account will be set up for the guest and that information will be uploaded to our server.

6) Crash information

If you choose to upload debug logs to help troubleshooting, your application debug log file will be sent to the server.

7) Analytics

We will collect product interaction (clicks, failed connection, viewing activities) on the Mi Fit application(home page, sports, settings, my profile). We use such pseudonymized data to help us improve our products and services.

Privacy by design

To ensure the security of your data, all the data in transit is encrypted via HTTPS, while user’s **body fit results** and **physical analysis** are encrypted at rest.

In addition to providing basic functions for supporting user access rights (such as access, deletion, download, etc.), we will consider the collection of some sensitive data to give users fully control at the early stage of product design, For example, you can change your mobile application settings of your band to not upload **body fit results** and **physical analysis information** to the server, even if the Mi Fit application has obtained location permissions from your phone.

Appendix 2: Data Inventory for Mi Smart Scale

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**App&cloud:** Per user request
	MAC	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	SN	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
Contact information	Email address	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Country	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
Sensitive information	Personal body information (weight)	Identified data	App/device functionality	**Device:** BLE **App<-->Cloud:** HTTPS	No encryption	**Device:** Unpair or restore the factory-released binding with the user

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Sensitive information	Body fit results (height, weight, BMI, muscle mass, body fat percentage, moisture content, protein, basal metabolism, visceral fat level, bone mass content, body shape, body age, and calories burned)	Identified data	App/device functionality,	**App<-->Cloud:** HTTPS	No encryption	**Device:** Unpair or restore the factory-released binding with the user
Usage data	Product interaction	Pseudonymized data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	No encryption, statistical data	**App&cloud:** Per user request
	Other usage data	Pseudonymized data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	No encryption, statistical data	**App&cloud:** Per user request
Diagnostics	Crash data	Identified data	Analytics	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
Other data	Avatars	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Gender	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Date of birth	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Firmware version	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	System time of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Operating system version of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request
	Brand and model of user's phone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	No encryption	**App&cloud:** Per user request

3.4 Mi Robot Vacuum and Privacy

Introduction

The Mi Robot Vacuum is a smart device that helps you to clean your floor. It supports multiple functionalities in terms of cleaning tasks, such as: i) enabling you to manage device operations, ii) selecting a desired cleaning mode, iii) managing room cleaning tasks, iv) customizing a cleaning layout/plan and v) designating specific cleaning areas.

In order to make the robot cleaning more intelligent, we have added extra vision sensor besides the laser sensor system. We are very cautious about the involvement of camera. In order to collect minimal user data, we have involved device computing capabilities. With device computing, we only extract image patten and match with the patten database locally, instead of comparing the image itself. In addition ,we do not store the image on local storage, and NOT upload the image to the server, either, and we delete the image once the image patten extracted.

Data collection and usage

1) Pairing with device and synchronizing data

We collect the **Xiaomi account ID, MAC address** and **SN** of the device to validate your device ownership.

2) Network connection

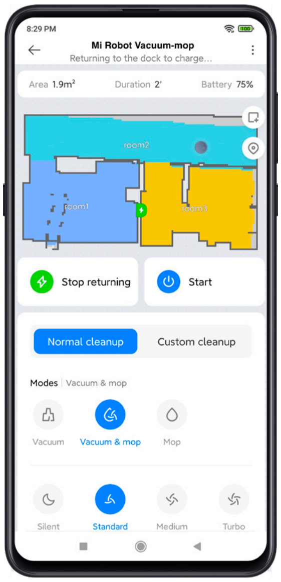
We collect network-related information (when your device is connected to a network) in order to set up and maintain the connection to the device. This includes the **current Wi-Fi connection mode** (LAN or remote), **IP address, the name of the connected Wi-Fi network, Wi-Fi signal strength** (i.e. RSSI) and the **MAC address of the device.**

3) Basic information

We collect the **device name, battery level, location in which the device is installed** (e.g. living room)**, operation status, firmware version** and **cleaning area**, to display the status of the robot in the Mi Home/Xiaomi Home app.

4) Status record

We will collect related parameters such as **cleaning mode, gear position, water volume and voice alert sound volume** to provide your settings and confirm the status of your robot.



8:29 PM

Mi Robot Vacuum-mop

Returning to the dock to charge...

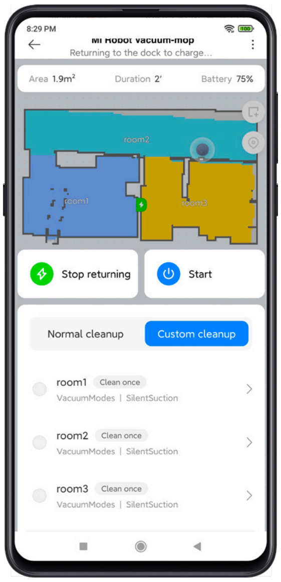
Area 1.9m² Duration 2' Battery 75%

Modes | Vacuum & mop

5) Cleaning Layout

Your device needs to know its position in the house in order to create accurate cleaning paths and avoid missing anything out or repeated cleaning. The device will scan the fuzzy contour layout of the room and upload it to the server and Xiaomi/Mi Home app to display the room layout and provide the layout function. Such layout information includes:

- **Floor layout:** We will collect information about the **floor layout** generated by the device after each cleaning task, and information about the **zone coverage** and **zone name, restricted areas** (areas not allowed for cleaning) and **virtual walls** (i.e., locations where the device is unable to pass) which have been set by you.
- **Ceiling features:** We will collect information about the **ceiling** and any objects attached to it (i.e., suspended ceilings and light fixtures). Information about ceiling features is collected on models using visual navigation technology (such as Mi Robot Vacuum-Mop 1C and Mi Robot Vacuum-Mop 2 Pro+). **Such information will only be processed on the local device and will not be uploaded to our server.**



8:29 PM

Mi Robot Vacuum-mop

Returning to the dock to charge...

Area 1.9m² Duration 2' Battery 75%

room1 Clean once
VacuumModes | SilentSuction

room2 Clean once
VacuumModes | SilentSuction

room3 Clean once
VacuumModes | SilentSuction

6) Cleaning records

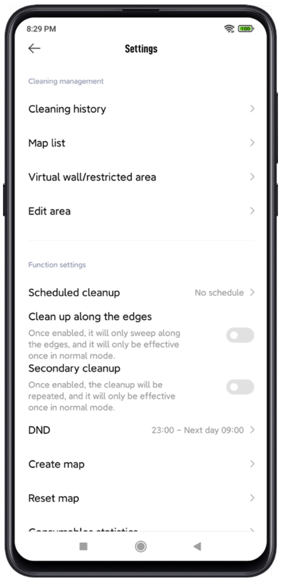
We will collect cleaning process records, which include **cleaning paths, cleaning zones, modes, time, duration,** and **coverage.** Such records are used to display usage records and to help you learn about the area, duration, zone of each cleaning task, as well as the accumulated time and area, and the total number of clean-ups.

7) Information about consumables

We will collect information relating to consumables, including **usage time and remaining life of consumables, with such information being used** to notify you of your usage of consumables.

8) Scheduled cleaning and DND

We will collect scheduled cleaning time, DND time, and **time zone settings** to provide the timing activation of related functions.



8:29 PM

Settings

Cleaning management

Cleaning history

Map list

Virtual wall/restricted area

Edit area

Function settings

Scheduled cleanup No schedule

Clean up along the edges

Once enabled, it will only sweep along the edges, and it will only be effective once in normal mode.

Secondary cleanup

Once enabled, the cleanup will be repeated, and it will only be effective once in normal mode.

DND 23:00 – Next day 09:00

Create map

Reset map

Consumables statistics

9) Data analysis

We collect product interaction data(e.g., clicks, failed connections, viewing activities) from the Mi/Xiaomi Home application plug-in for a statistical analysis of the usage and status of these functions. Such data is collected only if you have previously agreed to join the User Experience Improvement Plan.

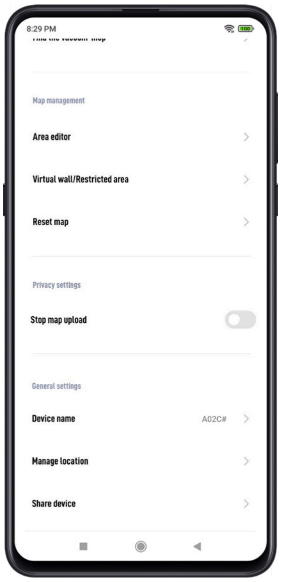
Privacy by design

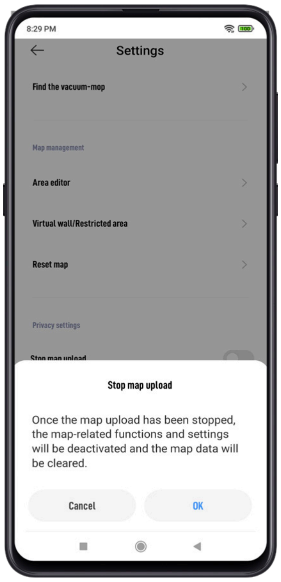
Mi Robot Vacuum only collects the data which is required to provide its functions. For example, functions which rely on the cleaning layout, such as: i) selected rooms cleaning, ii) designated area cleaning, iii) spot cleaning, and iv) cleaning record viewing. The relevant algorithms required for the Mi Robot Vacuum to perform obstacle avoidance and route planning are completely deployed and executed **locally on the device**. The surrounding environment information temporarily collected during the process will be used and discarded in real time, and will not be saved or uploaded to the server. In addition, some of Mi robot vacuum models such as the Mi Robot

Vacuum-mop 1C and Mi Robot Vacuum-mop 2 Pro+ use their top camera to collect ceiling images, and then immediately run the recognition algorithm deployed on the device to recognize and save the feature points such as the ceiling edge. After only milliseconds of processing time, the ceiling images are discarded and the original image is not saved or uploaded. The robot then draws an outline layout of the family rooms based on the feature points to support navigation and cleaning layout functions.

To ensure the security of your data, all the data in transit is encrypted via HTTPS, and all cleaning historical layouts are encrypted by AES-128 at rest.

We not only provide the functions for your data rights to be met (i.e., by enabling you to access, delete, and download your data), but also support some specific features when we design the functions. For example, Mi Robot Vacuum provides you with a local mode option. After turning the option on, all cleaning layouts and cleaning records are processed and **saved locally on the device only, and are not uploaded to the server**.





Stop map upload

Once the map upload has been stopped, the map-related functions and settings will be deactivated and the map data will be cleared.

Appendix 3: Data Inventory for Mi Robot Vacuum

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	MAC	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	SN	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
Usage data	Product interaction (clicks, browsing, usage time, etc.)	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
Diagnostics	Crash data	Identified data	Analytics	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** AES-128 **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	Performance data	Identified data	Analytics	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** AES-128 **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
Other data	Current Wi-Fi connection mode, IP address, name of the connected Wi-Fi network, Wi-Fi signal strength (i.e. RSSI)	Identified data	App/device functionality	**Device<-->Cloud:** MQTT **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Device name, battery level, installed location (e.g. living room), operation status , firmware version and cleaning area	Identified data	App/device functionality	**Device<-->Cloud:** MQTT **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request
	Cleaning mode, gear position, water volume, and voice alert sound volume	Identified data	App/device functionality	**Device<-->Cloud:** MQTT **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request
	Floor layout, zone coverage and zone name, restricted areas, and virtual walls	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** AES-128 **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	Ceiling features and significant objects	Identified data	App/device functionality	Not transmitted	**Device:** No encryption	**Device:** Discarded after milliseconds of processing time
	Cleaning path, zone, mode, time, duration, and coverage	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** AES-128 **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	Usage time and remaining life of consumables	Identified data	App/device functionality	**Device<-->Cloud:** MQTT **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request
	Scheduled cleaning time, DND time, and time zone setting	Identified data	App/device functionality	**Device<-->Cloud:** MQTT **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request

3.5 Mi Scooter and Privacy

Introduction

The MI scooter provides users with a new means of enjoyment. It has a compact design and is easy to carry, whilst offering power and a fashionable appearance. Users are able to view the scooter's general functions via the display panel, including, speed, gear, on/off light functions and battery BMS system information. It is also possible to check this information in Mi Home app, which allows for the easy management of MI Scooter devices. Additional functions such as tail lights-always-on and kinetic-energy-recovery are also available via the Mi Home App.

The device does not have a GPS function, so the specific location information of the device cannot be obtained. Information such as battery info, speed and mileage during use is only transmitted via the Mi Home app secure protocol between the device and the application end, and will not be uploaded to the server.

Data collection and usage

1) Pairing with device and synchronizing data

When you try to register the device, we will collect the **Xiaomi account ID, MAC address,** and **SN of the device** to record ownership and to connect you to the device.

2) Basic functions

We will collect information such as i) electricity usage, ii) remaining mileage, iii) temperature and iv) battery information in the Mi/Xiaomi Home application, which is used to display the status information of the device on the Mi/Xiaomi Home application plug-in. For the lock function, a user-defined **PIN Code** is stored locally on the device and is **only transmitted between the Mi/Xiaomi Home application** and **the device. Such data is stored on the device and will not be uploaded to the server.**

3) Status record

We will collect the **chosen setting** of the **tail lights-always-on, kinetic energy recovery, constant speed cruise** and other functions to the Mi/Xiaomi Home application to set the above functions on the application side. After disconnecting, the settings information is stored in the device, and the data in the application will be cleared. As with the data used for basic functions, **this data is stored locally and will not be uploaded to the server.**

4) Data analysis

We collect product interaction data (e.g., clicks, failed connections, viewing activities) from the Mi/Xiaomi Home application plug-in for statistical analysis on usage of the product and status of these functions. Such data is only collected if you have previously agreed to join the User Experience Improvement Plan.

Privacy by design

The Mi Scooter only collects the necessary information for displaying the speed calculation, scooter gear and any changes made. The data collected by the Mi/Xiaomi Home application, such as: i) battery information, ii) device information and ii) speed/mileage, is processed, calculated and displayed locally without uploading to the server for storage. In addition, a unique lock function switch is also provided. The PIN code required to lock the device is defined by the user and is also stored **locally** on the device.

Appendix 4: Data Inventory for Mi Scooter

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	**Device:** No encryption **App&cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	MAC	Identified data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	**Device:** No encryption **App&cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	SN	Identified data	App/device functionality, analytics	**App<-->Cloud:** HTTPS	**Device:** No encryption **App&cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
Usage data	Product interaction (clicks, browsing, usage time, etc.)	Identified data	Analytics	**App<-->Cloud:** HTTPS	**App&cloud:** AES-128	**App&cloud:** Per user request
Diagnostics	Crash data	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Device:** AES-128 **App&cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	Performance data	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Device:** AES-128 **App&cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	PIN code	Anonymized data	App/device functionality, analytics	**Device<-->App:** BLE	**Device:** No encryption	**Device:** Factory reset
	chosen setting of the tail lights-always-on, kinetic energy recovery, constant speed cruise	Anonymized data	App/device functionality, analytics	**Device<-->App:** BLE	**Device:** No encryption	**Device:** Factory reset
	Electricity, remaining mileage, temperature and battery information	Anonymized data	App/device functionality, analytics	**Device<-->App:** BLE	**Device:** No encryption	**Device:** Factory reset

3.6 Mi Router and Privacy

Introduction

The Mi Router aims to provide fast wired and wireless network connection services. This includes basic router functions such as wireless access and LAN access, web management and Wi-Fi settings. With a high-performance processor, outstanding throughput and strong load capacity, it can fully guarantee the quality of real-time applications on the network.

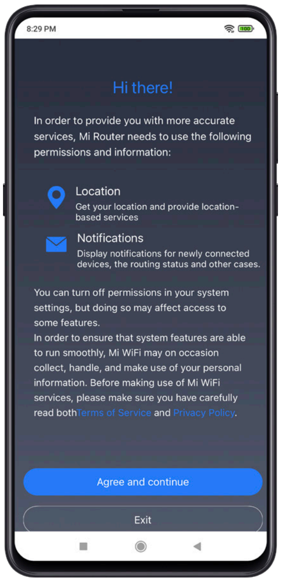
You can control your routers conveniently via the Mi WiFi app.

Data collection and usage

1) Pairing with device and synchronising data

In order to configure the Mi Router to provide you with Xiaomi Wi-Fi services, we will collect the following information:

- **Mi Account information:** Mi Account ID.
- **Location information:** Used to obtain Wi-Fi info[2] and identify the server to which the device is connected and the default language.
- **Device identification information:** MAC address, Android ID and IP.
- **Configured Mi Router information:** Information related to your Mi Router. This includes Mi Router activation status, binding status, active status, sharing status, model, system version, MAC address, device SN, device ID, country code, and router location.
- **Hardware and system information:** LED light on/off status, USB 3.0 on/off status, default time zone, default



8:29 PM

Hi there!

In order to provide you with more accurate services, Mi Router needs to use the following permissions and information:

Location
Get your location and provide location-based services

Notifications
Display notifications for newly connected devices, the routing status and other cases.

You can turn off permissions in your system settings, but doing so may affect access to some features.
In order to ensure that system features are able to run smoothly, Mi WiFi may on occasion collect, handle, and make use of your personal information. Before making use of Mi WiFi services, please make sure you have carefully read bothTerms of Service and Privacy Policy.

Agree and continue

Exit

[2] Android 6.0 and above, must have location permissions enabled in order to obtain Wi-Fi info and Bluetooth usage permissions

date, default time, firmware version number and default language.

2) Identify and display devices connected to the Mi Router

In order to provide management functions of the Mi Router, we will collect information including **network information, device information, location information** and **hard drive information.** Such information is used to identify the device and provide corresponding functions and processes for each network device. Network SSID and encrypted passwords in the network information, as well as index information in the hard drive, may be used to provide remote access services. During remote access to your router, data may be transmitted via our servers to your device. **Such data is encrypted and not stored on our servers.**

The above various information types are listed in detail as follows:

- **Network information:** Includes network SSID, access mode, gateway address, upload and download speed of WAN port, encryption mode, Wi-Fi channel, password, MU-MIMO on/off status, 2.4GHz/5GHz band on/off status and VPN configuration information (if the relevant information has been configured by the user).
- **Device information:** Includes device connection status and timing, device name, IP address, MAC address, device type, device brand, connection type, signal strength, noise strength, upload and download speeds and throughput, maximum upload and download speeds, guest Wi-Fi ID information, guest network connect and disconnect time, operating system, device online duration and frequency of Wi-Fi connections made; in addition, bandwidth usage ratio and duration will be collected when the device exceeds a certain threshold.
- **Location information:** Includes country code, GPS (if permission has been enabled), default time zone, default date, default time and default language.
- **Hard disk information:** If your Mi Router is connected to a hard drive, or has a self-contained hard disk, we will collect information related to the hard drive, which includes a summary of stored files, specifically the total size, file count and index information.

3) Push notifications

Push services cover terminal device online alerts, new software update alerts, backup action alerts, channel switch alerts, permission sharing alerts, system error alerts, device report alerts, and function recommendations.

In order to provide push notifications for your Mi Router, we may collect your **Mi Account, device information, disk information** and **network information** to provide you with message push services.

4) Firewall settings

We will collect your **firewall level settings, network blacklist** and **whitelist** and the **MAC address** of devices that have been blocked and experienced access failure, in order to provide firewall services. **Please be assured that this information is stored locally on the Mi Router and will not be stored on our servers.**

5) Wi-Fi optimisation

We will collect **Wi-Fi channel status, noise strength, channel throughput, download task status, upload status and signal strength** to assess and display Wi-Fi quality, download status, upload status, and signal strength. **Please be assured that this information will not be stored on our servers.**

6) Quality of service (QoS)

We provide QoS functions. When you enable or disable the QoS functions, we will collect information such as **bandwidth information, upload and download speeds, the type of speed limit you set** (such as game priority) and **the upload and download speed limit you set**. Such information will be used for intelligent speed distribution and speed limits.

7) Regular guest Wi-Fi

We support the set-up of a Wi-Fi subnet that is specifically for guests. If you set up guest Wi-Fi, the supported device will connect to the subnet as a guest, thereby distinguishing it from the primary network. In order to enable this function, we may collect the **function on/off status, network SSID, encryption status, encrypted passwords and network terminal information** that you have set. Such information will be used to provide guest Wi-Fi and network device display functions.

8) Wi-Fi timer, scheduled reboot

For better Xiaomi Wi-Fi service, we will collect your **Wi-Fi reboot time** in order to enable you to set the Wi-Fi timer and/or reboot.

9) Router sharing

When this function is turned on (this is disabled by default), we will collect the **sharing status** and **shared account information** from your Mi Router to provide you with sharing functions while also giving you the ability to control your sharing and view the sharing status of your router.

10) Router backup

When this function is enabled(this is disabled in default), we will collect your router configuration information(**network SSID and password**) to the server to provide a backup for your router configuration.

Privacy by design

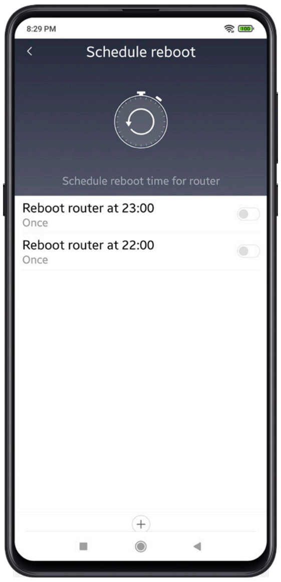
The Mi WiFi app only collects data which is required to provide functions, some of which are disabled by default to avoid extra data collection. For example, we will collect the configuration of your router information to backup only when you enable the automatic backup function.

To ensure the security of your data, all data in transit is encrypted through HTTPS and encrypted through AES-128 at rest.

We not only provide the functions for your data rights to be met (i.e., by enabling you to access, delete, and download your data), but also support some specific features when we design the functions. For example, we will not use GPS information even though the Mi WiFi application has access to it from your mobile device. GPS is only used to find nearby Wi-Fi devices on the Mi WiFi app. We also provide you with functions such as Wi-Fi timer, scheduled reboot, router backup, router sharing, which you are free to enable/disable according to your preference.

1) Wi-Fi timer, scheduled reboot

To provide smooth network connection, our Mi Router support automatic reboot function for Routers. Users can activate this function in Mi WiFi app. After setting time and frequency(i.e., once a week, once a month, everyday, etc.). The routers will automatic reboot at scheduled time.



Schedule reboot

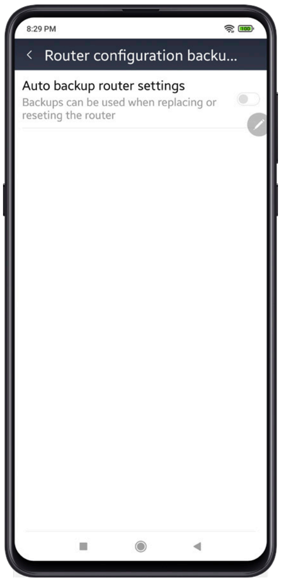
Schedule reboot time for router

Reboot router at 23:00
Once

Reboot router at 22:00
Once

2) Router backup

The user can choose whether to enable the router backup function on the Router configuration backup page. This function is disabled by default and when it is enabled, we will collect your router configuration information to the server.

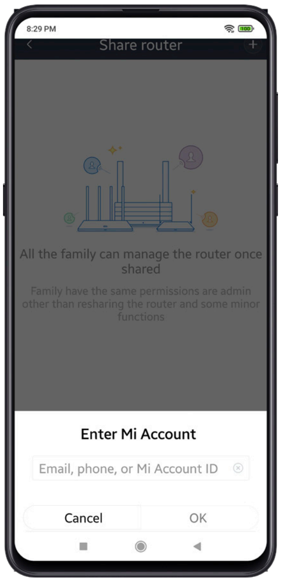


Router configuration backu...

Auto backup router settings
Backups can be used when replacing or reseting the router

3) Router sharing

The user can use Router sharing function in this page, and the user is required to actively enter the user account information that is allowed to receive.



All the family can manage the router once shared

Family have the same permissions are admin other than resharing the router and some minor functions

Enter Mi Account

Email, phone, or Mi Account ID

Appendix 5: Data inventory of Mi Router

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	MAC	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	SN	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Android ID	Identified data	App/device functionality	–	–	–
	IP	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Contact information	Email address (this is optional for users to provide user feedback)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Country	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
Location	Rough Location	Identified data	App/device functionality	Location information is only obtained when required by a function, and is neither saved nor uploaded	-	-
	Country code, default time zone, default date, default time, and default language	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
Customer Support	Description of the issue, attached screenshots, email address, the model of your router and phone, system versions, Mi Wi-Fi app version, your region	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
Other data	Configured Mi Router information (Mi Router activation status, binding status, active status, sharing status, model, system version, device ID and router location)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Hardware and system information （LED light on/off status, USB 3.0 on/off status, default time zone, default date, default time, firmware version number, and default language）	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Network information (network SSID, access mode, gateway address, upload and download speed of WAN port, encryption mode, Wi-Fi channel, password, MU-MIMO on/off status, 2.4GHz/5GHz band on/off status and VPN configuration information (if the user has configured relevant information), Wi-Fi reboot time and network password)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Device information (device connection status and timing, device name, device type, device brand, connection type, signal strength, noise strength, upload and download speeds and throughput, maximum upload and download speeds, guest Wi-Fi ID information, guest network connect and disconnect time, operating system, device online duration and frequency of Wi-Fi connections made, bandwidth usage ratio, duration, the type of speed limit you set (such as game priority), sharing status, and shared account information)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Hard disk information (summary of stored files, specifically the total size, file count, and index information)	Identified data	App/device functionality	When the user chooses to download a file, the phone/computer accesses the hardware inserted into the router through the Samba protocol, reads the file to be downloaded and stores the file on the mobile phone or computer, instead of uploading it to the Xiaomi server.	AES 128+Base64	Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Firewall settings information (firewall level settings, network blacklist, whitelist)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Wi-Fi optimisation information (Wi-Fi channel status, noise strength, channel throughput, download task status, upload status, and signal strength)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request
	Regular guest Wi-Fi information (function on/off status, encryption status, encrypted passwords, and network terminal information)	Identified data	App/device functionality	HTTPS	AES 128+Base64	Per user request

3.7 Mi Camera and Privacy

Introduction

The Mi Home Security Camera is a device which provides monitoring functions and solutions for homes with detection needs. It supports remote viewing on multiple devices, two-way real-time voice calling, and human detection to help users live with peace of mind. It offers functions such as three storage methods for backup, quick playback and easy browsing, and standard/inverted mounting with 180° screen rotation.

We fully understand your concerns about the security and privacy of information such as the video captured by the camera. To address these concerns, we have ensured that the Mi Camera adopts a combined secure encryption method for encrypted videos in transit and rest. For example, we provide the end-to-end encrypted transmission for the streamed images to protect against unauthorized access.

Data collection and usage

1) Pairing with device and synchronising data

We will collect below information to pair your device with your account.

- **Account information:** Includes your Mi account ID and Mi accounts you share the device with.
- **Device Information:** Includes the device name, device ID, firmware version, installed location (such as in the living room), time zone, security code (if you have already set it up) for viewing the device, screen information (such as sharpness, scaling), recording mode(Continuous recording mode, human detection detect recording mode) as well as memory card information (errors relating to record storage, used/remaining storage of memory card).
- **Device settings:** Includes the status indicator on/off, data usage prevention on/off, smart frame on/off, flow protection switches, physical obstruction settings, image settings, night vision settings.
- **Network information:** When your device is connected to a network, this information includes current Wi-Fi connection mode (LAN or remote), **assigned IP address, Wi-Fi signal intensity, RSSI, MAC address,** and the **Wi-Fi network name (SSID) and password.**

2) Viewing real-time image

We will collect **information on the current image time, playback speed, image quality option** and **volume** to provide you with real-time image viewing functionality. In addition, you can take a screenshot or record the current live image. Real-time image screenshot/video recordings will be saved on your phone instead of being uploaded to any server.

3) human detection

You can enable or disable the Home Surveillance Assistant function (**this function is disabled by default**). If this function is enabled, we will collect the following information:

- Mobile-human detection switch,
- Sensitivity(the ability to sense human movement in high or low sensitivity),
- Home surveillance periods(users can set surveillance periods, like all day tracking, or 8:00-18:00 scheduled time tracking),
- Shooting interval, (To reduce pushing notification, shooting interval can be raised),
- Image change push notification on/off(receive push notifications when an image changes).

In addition, video recording will only be triggered when the image changes within the detection range of the camera. You can set the distance (in meters) away from the door to trigger video recording, the start and end time of home surveillance, and to shoot in interval for more seamless viewing.

4) Baby crying detection

When baby crying sound detection is enabled (**this function is disabled by default**), you will receive a push notification if a baby crying sound is detected. We will collect the status of **notification settings of this function (on/off)** to provide this service. This information is processed locally and only the videos of triggering events instead of whole videos are uploaded to the server.

5) Video playback

You can view various types of videos in the Xiaomi/Mi Home app plug-in. We will collect and encrypt the **videos triggered by Home Surveillance Assistant** and **baby crying**, as well as the **triggering events**, and save this encrypted data on a secure server for 7 days. We will also collect information related to the recording and network, which includes **recording date, recording time, trigger event, recorded video duration, sound settings,** and **playback speed** to provide this service.

6) Two-way talkback

You can view information on the live image in the application plug-in and talk with others using the two-way talkback function. We will not collect information on your conversation, unless you select to record current real-time image before using the two-way talkback. **However, under no circumstances will we try to access or identify your conversation.**

7) Notification

The device will send you corresponding notifications according to triggering events. For example, you can set the device to send a notification to your phone when the monitored image changes. We will collect **information on your notification settings** to provide this service.

8) Data analysis

We collect product interaction (clicks, failed connections, viewing activities) from the Mi/Xiaomi Home application plug-in for statistical analysis of your usage and status of these functions. Such data is collected only if you have previously agreed to join the User Experience Improvement Plan.

Privacy by design

Mi Camera only collects data which is required to provide its functions, some of which are disabled by default to avoid unnecessary data collection. For example: for users who enable functions such as human detection and baby crying detection, **videos triggered by these options**, as well as the **triggering events**, will be stored in rest only for 7 days, while the algorithms for these two functions are processed locally.

Note:

Human detection algorithms is very different from normal motion detection because it will be trigger **only when a human body is detected**. The detection algorithm analyzes the body moves, so it is able to detect even intruders that are wearing a mask.

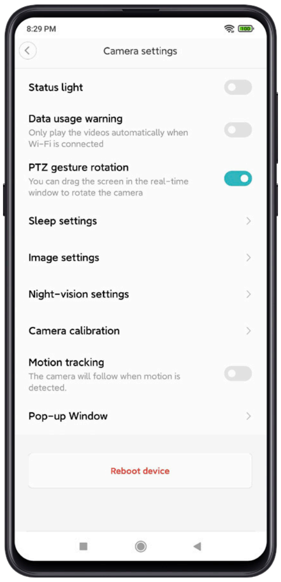
Baby crying detection algorithms

For human detection, the camera will capture the image at different frame rates to calculate and compare by the CPU in accordance with certain algorithms. When there is a change in the picture, such as someone walking by or an object movement, the calculation and comparison results in the number will exceed the threshold and adjust the camera a certain angle through the motor, so that the moving object can be recorded in the centre of the video.

For baby crying detection, a certain number of statistical samples are used to establish the eigenvalues. The signals are collected locally and compared with the eigenvalues through some data processing such as noise reduction, cleaning, Fourier transform, and then the baby’s crying is determined.

To ensure the security of your data, Mi Camera adopts a combined secure encryption method for encrypted transmission and storage of your video. The video uploaded by the camera to the cloud is encrypted for transmission and storage via HTTPS+AES128. Furthermore, we support end-to-end encrypted transmission to ensure that nobody is able to access your video data in the camera’s real-time video stream.

We not only provide the functions for your data rights to be met (i.e., by enabling you to access, delete, and download your data), but also support some specific features when we design the functions. For example, Mi Camera supports human detection and baby crying detection. These functions are disabled by default, and users are free to enable/disable them according to their preference.



Camera settings

Status light ○

Data usage warning ○
Only play the videos automatically when Wi-Fi is connected

PTZ gesture rotation ●
You can drag the screen in the real-time window to rotate the camera

Sleep settings >

Image settings >

Night-vision settings >

Camera calibration >

Motion tracking ○
The camera will follow when motion is detected.

Pop-up Window >

Reboot device

Appendix 6: Data Inventory for Mi Camera

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App functionality	HTTPS	AES-128 with encryption SDK	Per user request
	MAC	Identified data	App functionality	HTTPS	AES-128 with encryption SDK	Per user request
	SN	Identified data	App functionality	HTTPS	AES-128 with encryption SDK	Per user request
	Device ID	Identified data	App functionality, analytics	**Device:** Wi-Fi **APP<-->Cloud:** HTTPS	No encryption	Per user request
User content	Photos or videos	Identified data	App functionality	HTTPS	AES-128 with encryption SDK	Per user request
	Audio data	Identified data	App functionality	**Device:** WiFi **APP<-->Cloud:** HTTPS	Not stored	-
User data	Product interaction	Anonymized data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
Diagnostics	Crash data	Anonymized data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Performance data	Anonymized data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
Other data	Firmware version	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Memory card information (errors, remaining storage, recording mode)	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Device settings, including status indicator on/off	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Data usage prevention on/off	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Assigned IP address	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Wi-Fi signal intensity	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	RSSI	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request
	Wi-Fi network name (SSID) and password	Identified data	App functionality, analytics	HTTPS	AES-128 with encryption SDK	Per user request

3.8 Xiaomi/Mi Home

Introduction

Xiaomi/Mi Home is the smart device management platform for your home. Xiaomi/Mi Home enables you to interact with smart devices conveniently through your mobile phone, and enables you to control your smart devices under one platform.

1) Linkage control, easy to use

Even users without previous experience of smart devices can quickly master the connection and operation of smart devices, allowing for such devices to become interconnected.

2) Customize as you wish

Set up smart scenes according to your own habits.

3) Device sharing, fun delivery

Sharing devices with family and friends lets everyone experience the fun of technology together.

Data collection and usage

1) Smart device connections

In order to provide you with Mi Home/Xiaomi Home services and to enable you to securely connect to and manage your smart devices, we will collect your Wi-Fi information, location information, account login information, information related to your mobile phone and smart device, and information associated with your Mi account and smart device.

This information will be used to provide you with various functionalities, including pairing with and connecting to smart devices, discovering nearby devices, and device management. Specific examples involving the above information are set out below:

- **Account login information:** Mi account (the account ID may be the Xiaomi ID, phone number or email address), nickname, and profile picture information, as well as cookies (including Mi account, ServiceToken, country code, app store channel, and time zone) to log in to your account.
- **Mobile phone related information:** Hardware-based identifiers (MAC address, Android ID), phone model, OS version, OS language, country or region, App Store version, screen size and resolution, CPU, and display device related information. Based on the type of smart device you wish to connect to, we will collect the following information:
    - **Smart devices connected via Wi-Fi: Wi-Fi information (SSID, BSSID, MAC address of Wi-Fi, Wi-Fi password), MAC address of the device,** and **device ID.**
    - After establishing a local connection via Bluetooth, smart devices connected via Wi-Fi: Wi-Fi information

(**SSID, BSSID, MAC address of Wi-Fi, Wi-Fi password**), **MAC address of the device,** and **MAC address of Bluetooth on the device.**

- Smart devices connected via Bluetooth: **MAC address of Bluetooth on the device,** and **device ID.**
- Smart devices connected via Zigbee: **MAC address of the device,** and **device ID.**

2) Using smart devices for home management

We will collect **information that you provide relating to room settings for smart devices** in order to facilitate smart home management. This will allow you to enjoy greater convenience when using smart devices (for example, when using multiple smart lights, being able to quickly identify that a light is in a bedroom instead of the living room).

3) Device sharing

We provide support for you to share smart devices with others through Mi accounts. Sharing a smart device with others allows them to also control the device. In order to provide this service, we will collect your **Mi account ID, the Mi account ID which you use to share**, and shared device information (including the **device ID, device name, device verification key, and sharing status of device**). Such information equips us with the ability to enable you to share device control and usage with the accounts of other Mi users as well as to display the device's sharing status on the My Devices page in the Mi Home/Xiaomi Home application.

4) App and smart device updates

To ensure you are able to continue enjoying the latest Mi Home/Xiaomi Home services, we will use your **Mi Home/Xiaomi Home app version** and **phone model** in order to provide you with updates to the Mi Home/Xiaomi Home app. We will also collect **a list of your connected smart devices and associated firmware version information** in order to provide you with smart device updates so that you can use the latest version of the service.

5) Smart linkage scenes

We provide support for you to configure certain rules to establish smart connections between devices under specific conditions. In order to enjoy this feature, we may collect your **location information, smart scene rule settings,** and **designated device status** so as to enable specific device functions to be executed according to the commands you give. For example, enabling a light to turn on whenever a sensor detects someone passing by. This functionality cannot be enabled without your explicit consent and configured rules.

6) Provision of content-related support

We provide support for content-related services. For example, articles and audio content playback are available in certain regions only. To help you make better use of smart devices, we will provide you with selected articles on such devices. When you view these articles, we will not collect any information from you.

If you have connected a smart device (such as the Mi AI Smart Speaker) that plays media content to Mi Home/Xiaomi Home, you can select and control the music or content to be played on the corresponding support page. We will collect the **smart device type registered with your account** to make corresponding smart device control functions available to you.

7) Data analysis

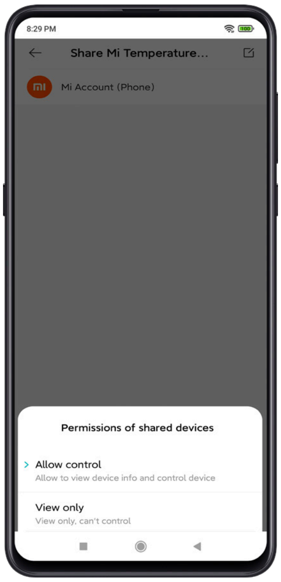
We collect the **usage time and frequency of each function in Xiaomi/Mi Home and product plug-ins** for statistical analysis of your usage and status of these functions. Such data is collected only if the user has previously agreed to join the User Experience Improvement Plan.

Privacy by design

Xiaomi/Mi Home supports the sharing of smart devices, and strictly controls device sharing permissions. When you share a device with others in Xiaomi/Mi Home, the shared party will only be granted viewing permissions and permissions to control basic functions. You remain the sole device owner at all times, and have the ability to cancel the sharing at any time.

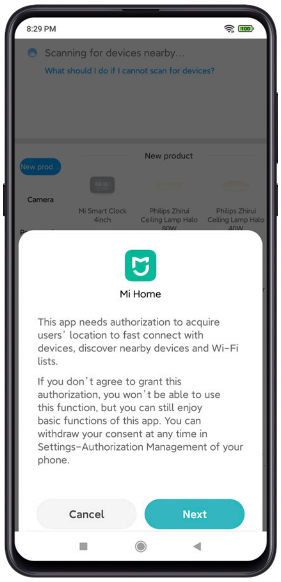
You can also create your device's smart linkage function in the Xiaomi/Mi Home app. For example, when the door and window sensors recognise that someone has returned home, the smart light at home will light up. These functions are implemented by Xiaomi/Mi Home, so even if you link smart devices from different manufacturers, you do not have to worry about your personal information being shared with different manufacturers.

Due to security restrictions of the Android and iOS system, Xiaomi/Mi Home needs to obtain mobile phone location permission when scanning and connecting to Bluetooth and Wi-Fi smart IoT devices. Xiaomi/Mi Home will only ask the user for location permissions when the user is using such scanning or connecting functions in relevant pages. If the user does not agree to enable location permissions, they are still able to use the basic functions of Xiaomi/Mi Home other than those of scanning and connecting to smart devices.



Permissions of shared devices

- Allow control
  Allow to view device info and control device
- View only
  View only, can't control


8:29 PM
Scanning for devices nearby...
What should I do if I cannot scan for devices?
New product
New prod...
Camera
Mi Smart Clock 4inch
Philips Zhirui Ceiling Lamp Halo 80W
Philips Zhirui Ceiling Lamp Halo 40W
Mi Home

This app needs authorization to acquire users' location to fast connect with devices, discover nearby devices and Wi-Fi lists.

If you don't agree to grant this authorization, you won't be able to use this function, but you can still enjoy basic functions of this app. You can withdraw your consent at any time in Settings-Authorization Management of your phone.

Appendix 7: Data Inventory for Xiaomi/Mi Home

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
	MAC	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	SN	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
	Android ID	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
	Facebook ID	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
	Device ID	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Device:** No encryption **Cloud:** AES-128	**Device:** Factory reset **App&cloud:** Per user request
Contact information	Country	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request
User content	User information that may be recorded by the smart device (such information may include camera videos or home temperature that varies from different devices)	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
Usage data	Product interaction	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Diagnostics	Crash data	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
	Performance data	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
User feedback	Feedback, contact information, logs (including crash log, performance log), error code, type and time of app or device issues you provide to us	Identified data	Analytics	**App<-->Cloud:** HTTPS	**Cloud:** AES-128	**App&cloud:** Per user request
Other data	Nickname, profile photo, device model	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request
	Phone model, system version, system language, application store version, phone screen size and resolution, CPU model, and installed phone applications	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request
	Wireless router MAC address and SSID, Wi-Fi lists	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request
	1. Wi-Fi list of current user device 2. The smart device list, device attributes 3. Operation instructions of the user's smart device (such as turning on/off of the smart device)	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	1. The token, user name, shared user name, device name of the corresponding user ID of the shared device 2. Device sharing status	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**Cloud:** No encryption	**App&cloud:** Per user request
	Information triggered by smart devices (e.g. information triggered by sensors)	Identified data	App/device functionality	**Device<-->Cloud:** HTTPS **App<-->Cloud:** HTTPS	**Cloud:** No encryption	**Device:** Factory reset **App&cloud:** Per user request
	Cookies including Mi account, ServiceToken, country code, channel (app channel such as Mi app store, GooglePlay), time zone	Identified data	App/device functionality	**App<-->Cloud:** HTTPS	**App:** No encryption	**App:** Uninstall

3.9 Xiaomi Wear and Privacy

Introduction

The Xiaomi Wear application is a platform used to connect your Xiaomi smart wearable devices, allowing you to manage them and view the data measured by these devices, such as your sleep data, exercise records, calories consumed, and steps walked per day.

Data collection and usage

1) Smart wearables registration

To facilitate the registration of your smart wearables in the app, we will collect the information relating to your **Mi Account, identification of the smart wearable, country,** identification of your devices such as **MAC, SN, Android ID, and Bluetooth information** of smart wearables and your **phone model, OS version.**

2) User login

When you try to log in to the app, we will collect the account information. The account ID may be the **Xiaomi ID, phone number or email address.**

3) Weather

You can view the weather information in your corresponding city on the device after pairing. We need to collect your **rough location information** (GPS is accurate to approximately 1km), or else you will need to select the city manually. Such data will not be stored in the server and will only be used to provide the weather information in your city.

4) Workouts

You can use the ‘workouts’ function in your app to record your route during outdoor exercises. While using workouts, we need to collect your **precise location information**. You may disable the function to stop uploading the workout trace information to our servers.

5) Recording and display of exercise and health data

Your exercise and health information will be recorded and displayed on the smart wearable device and in the app. You may check it at any time to ensure that your body is in perfect working order. We will collect and record information relating to your activity, including the **number of steps you take, standing activity and duration, exercise mode, cadence, distance covered, exercise duration, elevation, heart rate, swimming strokes, stroke rate, number of laps, and heartbeat information**. In addition, we will collect your personal information, including your **nickname, gender, date of birth, height,** and **weight**. This information will be used to calculate and display your heart rate, number of steps you take, calories you burn from exercise, and sleep time, which is to help you better understand the state of your health.

6) Notification Display

You may enable the notification alert function in the app (**disabled by default**). Once turned on, you will receive alerts for your calls, SMS, and application notification messages on your device (certain types of devices may not support this feature). The name of your contact, text messages, and the app notifications may show on the device as a reminder. **Such data will only be used for displaying and will not be stored.**

7) Analytics

We collect the **usage time and frequency of each function in the Xiaomi Wear app** for statistical analysis of your usage and status of these functions. Such data is collected only if the user has previously agreed to join the User Experience Improvement Plan.

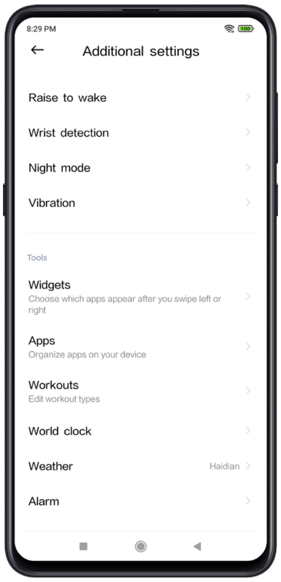
Privacy by design

GPS permission access only applies for permissions required from you by the app function, such as **search and connect devices, outdoor sports** and **weather positioning.**

The transmission of data between the app and server is based on HTTPS. In addition, all sensitive data is encrypted at rest with varying degrees, such as with AES-256 and AES-128.

We not only provide the functions for your data rights to be met (i.e., by enabling you to access, delete, and download your data), but also support some specific features when we design the functions. For example,workout trace data cannot be uploaded to the server even if the app has obtained location permissions from your smartphone.

You may also choose to enable or disable the weather positioning function according to your preference in order to prevent GPS information being collected. This can be disabled via the "**My Profile > Settings > Additional settings > Weather**" page. Once disabled, the rough location data **will no longer** be collected.



8:29 PM

Additional settings

Raise to wake

Wrist detection

Night mode

Vibration

Tools

Widgets
Choose which apps appear after you swipe left or right

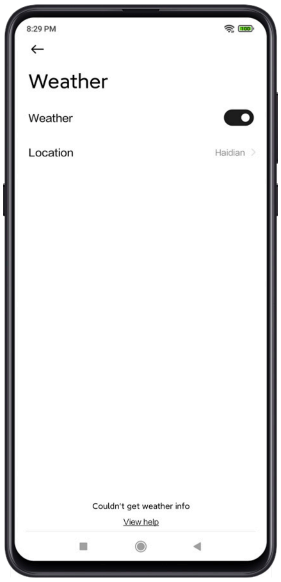
Apps
Organize apps on your device

Workouts
Edit workout types

World clock

Weather Haidian

Alarm



8:29 PM

Weather

Weather ●

Location Haidian

Couldn't get weather info

View help

Appendix 8: Data Inventory for Xiaomi Wear

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Identifiers	Mi Account ID	Identified data	App/device functionality	HTTPS	**Device:** No encryption **App&cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	MAC	Identified data	App/device functionality	HTTPS	**Device:** No encryption **App&cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	SN	Identified data	App/device functionality	HTTPS	**Device:** No encryption **App&cloud:** No encryption	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	Android ID	Identified data	App/device functionality	HTTPS	**App&cloud:** No encryption	**App&cloud:** Per user request
Contact information	Country	Identified data	App/device functionality	HTTPS	**App&cloud:** keycenter AES-128	**App&cloud:** Per user request
Sensitive information	Nickname, gender, date of birth, height, weight	Identified data	Analytics	HTTPS	**App&cloud:** keycenter AES-128	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
	Health data (heart rate, heartbeat information)	Identified data	Analytics	HTTPS	**Device:** No encryption **App&cloud**: keycenter AES-128	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request
Location	Precise location	Identified data	App/device functionality	HTTPS	**App&cloud:** AES-128 with encrption SDK	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Location	Rough location	Identified data	App/device functionality	BLE	**Device:** No encryption	**Device:** Factory reset
User content	Photos	Identified data	App/device functionality	BLE	**Device:** No encryption	**Device:** Factory reset
	Watch settings (alarm, timer, do not disturb mode, brightness, theme, etc.)	Identified data	App/device functionality	BLE	**Device:** No encryption	**Device:** Unpair or restore the factory-released binding with the user
	Watch face store	Identified data	App/device functionality	BLE	**Device:** No encryption	**Device:** Unpair or restore the factory-released binding with the user
Usage data	Product interaction	Pseudonymized data	Analytics	HTTPS	**App&cloud:** keycenter AES-128	**App&cloud:** Per user request
Diagnostics	Crash data(logs on system and device errors, country/region, model, firmware version, and name of the device)	Pseudonymized data	Analytics	HTTPS	**App&cloud:** No encryption	**App&cloud:** Per user request
	Performance data(device connection result, battery level, watch face, and NFC information)	Pseudonymized data	Analytics	HTTPS	**App&cloud:** No encryption	**App&cloud:** Per user request

Type	Type of data	Identification Qualifier	Purpose	Data Transmission Encryption Measures	Data Storage Encryption Measures	Data Retention Policy
Other data	Phone model, OS version , firmware version	Identified data	App/device functionality, analytics	HTTPS	**App&cloud:** No encryption	**App&cloud:** Per user request
	Calls, text messages, app notifications	Identified data	App/device functionality, analytics	BLE	**Device:** No encryption	**Device:** Unpair or restore the factory-released binding with the user
	Feedback: phone number, email address, log information	Identified data	Analytics	HTTPS	**App&cloud:** User identify info: keycenter AES-128 Logs: AES-256	**App&cloud:** Per user request
	Workout data (number of steps you take, standing activity and duration, exercise mode, cadence, distance covered, exercise duration, elevation, swimming strokes, stroke rate, number of laps)	Identified data	Analytics	HTTPS	**Device:** No encryption **App&cloud:** keycenter AES-128	**Device:** Unpair or restore the factory-released binding with the user **App&cloud:** Per user request

04

International Data Transfer

Xiaomi processes and backs up personal information through a globally operating and controlled infrastructure. Your data is transmitted by encrypted communication channels and stored in 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 applicable laws.

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

Below is the table which outlines the geographic location of data stored by Xiaomi applications and devices:

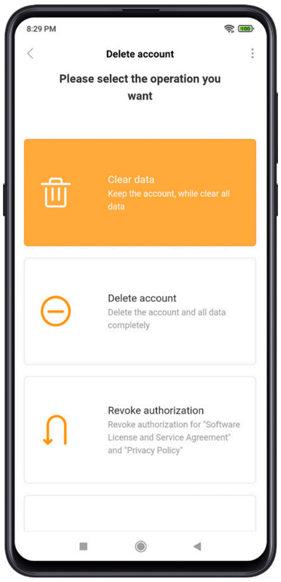
Region	Cloud service providers	Data storage locations	Device & app
EEA	Amazon web services	Germany	Mi Fit/Mi Home/Xiaomi Home/Xiaomi Wear
	Amazon web services	Germany	Mi WiFi
	Alibaba cloud	Singapore	Mi WiFi
United Kingdom	Amazon web services	Germany	Mi Fit/Mi Home/Xiaomi Home/Xiaomi Wear
	Amazon web services	Germany	Mi WiFi
	Alibaba cloud	Singapore	Mi WiFi
India	Amazon web services Microsoft azure	India	Mi Fit/Mi Home/Xiaomi Home/Xiaomi Wear/ Mi WiFi
Russia Federation	Kingsoft cloud	Russia	Mi Fit/Mi Home/Xiaomi Home/Xiaomi Wear/ Mi WiFi
United States	Amazon web services	United States	Mi Fit/Mi Home/Xiaomi Home/Xiaomi Wear
	Alibaba cloud	Singapore	Mi WiFi
Mainland China	Kingsoft cloud Alibaba cloud 21ViaNet	Mainland China	Mi Home/Xiaomi Home/Xiaomi Wear
	Amazon web services		Mi Fit
Other	Alibaba cloud	Singapore	Mi Home/Xiaomi Home/Xiaomi Wear/Mi WiFi
	Amazon web services	Singapore	Mi Fit

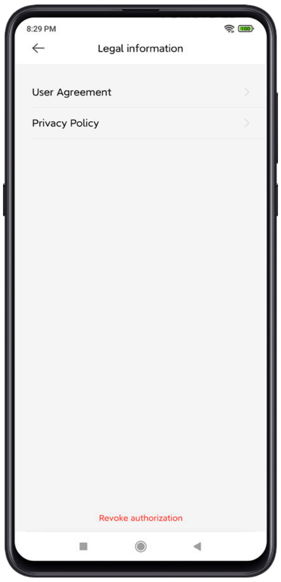
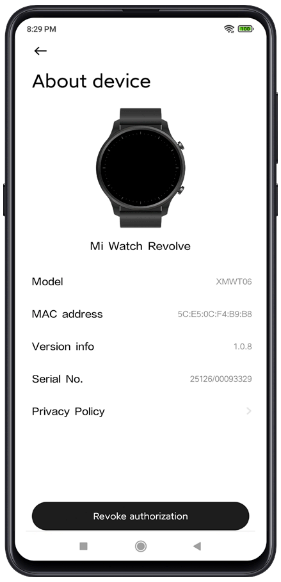
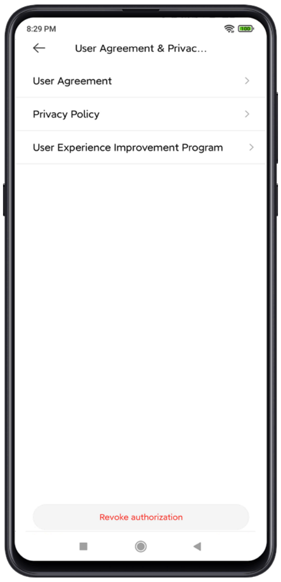
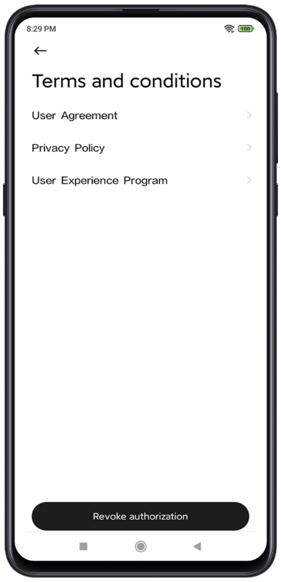
If you use our products and services in the area of the European Economic Area (EEA), Xiaomi Technology Netherlands B.V. will act as the data controller, and Xiaomi Singapore Pte. Ltd. will be responsible for the data processing. Xiaomi’s international transfer of personal data collected in the European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

05

Control Your Privacy in IoT Products

We provide you full control for your privacy in IoT products, it is easy for you to view, correct, delete, download and withdraw consent in your mobile application which your device connected with. Below is a table which sets out instructions on how users can manage data stored by Xiaomi:

Device Connected to App	Controls	How
Mi Fit	View Correction	Mi Fit – Profile
	Delete	Mi Fit – Profile – Settings – Account – Delete account  8:29 PM Delete account Please select the operation you want Clear data Keep the account, while clear all data Delete account Delete the account and all data completely Revoke authorization Revoke authorization for "Software License and Service Agreement" and "Privacy Policy"
	Download	Mi Fit – Profile – Settings – Account – Export Data
	Withdraw Consent	Mi Fit–Profile–Settings–Account–Revoke authorization
	Others	Send email to privacy@huami.com or DPO@huami.com (EU only)
Mi Home/ Xiaomi Home/ Xiaomi Wear	View Correction	· You may edit your profile data or sign in/out of your account via the "**Profile – Personal Info**" page (Xiaomi/Mi home/Automation), or in "**Profile – My profile**" page (Xiaomi Wear). · You can manage your devices, rooms/homes and related automation scenarios in the "**Xiaomi/ Mi home/Automation**" tabs, or manage your smart wearable devices function and settings in the "**Profile – device"** tab. · You can Reset password, Change recovery phone in the Mi Account Help Center (https://account.xiaomi.com/helpcenter).
	Delete	· You can go to Mi account privacy center – app to delete data on the Xiaomi/Mi home app/Xiaomi Wear servers and all bound devices. · You can delete data stored locally in your device by factory resetting, please check user manual for factory resetting steps.
	Download	· You can go to Mi account privacy center – app to download a copy of the Xiaomi/Mi home/Xiaomi Wear data.

Device Connected to App	Controls	How
Mi Home/ Xiaomi Home/ Xiaomi Wear	Withdraw consent	· If you want to withdraw your consent to the single Product Privacy Policy and delete all personal data on servers related to that product, you can go to "**Xiaomi/Mi home – Your device icon – Settings – Additional settings – Legal information – Revoke authorization**" for Xiaomi/Mi home, or go to "**Profile – Additional settings – About device – Revoke authorization**" for Xiaomi Wear.  8:29 PM Legal information User Agreement Privacy Policy Revoke authorization  8:29 PM About device Mi Watch Revolve Model XMWT06 MAC address 5C:E5:0C:F4:B9:B8 Version info 1.0.8 Serial No. 25126/00093329 Privacy Policy Revoke authorization · If you want to withdraw your consent to the Privacy Policy of the Xiaomi/Mi home/Xiaomi Wear app and all bound products, and delete all your personal data, including data related to your devices on servers and data generated during your use of the Xiaomi/Mi home/Xiaomi wear app on both our servers and on your phone, you can go to "**Xiaomi/Mi home – Profile – User Agreement & Privacy Policy – Revoke authorization**" for Xiaomi/Mi home, or go to "**Profile – More – Settings – Terms and conditions – Revoke authorization**" for Xiaomi Wear.  8:29 PM User Agreement & Privac... User Agreement Privacy Policy User Experience Improvement Program Revoke authorization  8:29 PM Terms and conditions User Agreement Privacy Policy User Experience Program Revoke authorization

Device Connected to App	Controls	How
Mi Home/ Xiaomi Home/ Xiaomi Wear	Others	· If you have any concerns, complaints, or questions regarding privacy, please click the "Xiaomi Privacy Support" for further help. · Xiaomi/Mi home/Xiaomi wear offers an opt-in User Experience Improvement Plan. If you wish to provide your usage data from the Xiaomi/Mi home/Xiaomi Wear app or device plug-in page, you can choose to give your consent on the User Experience Improvement Plan pop-up dialogue when opening the Xiaomi/Mi home app or Xiaomi/Mi home device plug-in page for the first time. For the Xiaomi Wear app, you can check the checkbox in Privacy and permissions page when opening the app for the first time. You can quit the User Experience Improvement Plan in "**Xiaomi/Mi home - Profile - Settings - Privacy settings - Join User Experience Program**" for Xiaomi/Mi home, or "**Profile - More - Settings - Enroll in User Experience Program**" for Xiaomi Wear.
Mi WiFi	View correction	· You can edit your profile data or sign in/out of your account via the "**Profile - Personal Info**" page. · You can manage your devices, rooms/homes and related automation scenarios in the "**Xiaomi/Mi Home/Automation**" tabs. · You can Reset password, Change recovery phone in the Mi Account Help Center.
	Delete	· You can go to Mi account privacy center - app to delete data on the Mi WiFi app server and all bound devices. · You can delete data stored locally in your device by factory resetting, please check user manual for factory resetting steps. · If you want to withdraw your consent to single Product Privacy Policy and delete all personal data on server related to that product.
	Download	· You can go to Mi account privacy center - app to download Mi WiFi data copy.
	Others	· If you have any concerns, complaints, or questions regarding privacy, please click the "Xiaomi Privacy Support" for further help.

06

Security and Privacy Certifications

Xiaomi has been widely recognized by global third-party agencies in the field of information security and privacy protection. The authoritative information security and privacy certifications we obtained are the best embodiment of our leading position.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED

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. The certification presents that Xiaomi has met the requirements of international standards and fulfilled our commitment to users, which puts Xiaomi in a leading position in the information security management area.

bsi
ISO/IEC
27701
Privacy Information
Management
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 proves that Xiaomi has satisfied the strict requirements of privacy protection.

Xiaomi is also a corporate member of the IoT Security Foundation (“IoTSF”). We implement the security assessment framework of IoTSF in our practices, and have built our internal IoT security and privacy management system and testing cases in accordance with IoTSF principles.

You can learn more about the information security and privacy certifications of Xiaomi by visiting Xiaomi Trust Center – Compliance.

07

Conclusion

Xiaomi is committed to providing fully functional, secure and easy-to-use digital hardware and software products to personal, home and industrial users worldwide. In the process of research, design, manufacturing, operation and service of IoT technology, Xiaomi consciously abides by the security specifications of IoT technology and always insists on achieving fairness, security and privacy protection to enhance and enrich the user experience of Xiaomi's consumer IoT products. This white paper is a comprehensive presentation of Xiaomi's IoT product design and implementation.

Xiaomi seeks to root the principles of IoT security and privacy in the hearts of every business unit, every employee, and every partner. As proposed earlier, Xiaomi continuously improves its security and privacy management system and integrates security and privacy strategies into all aspects of IoT product development and application. We also conduct strict security and privacy audits of our partners and actively monitor and address new security issues and threats to ensure that user data is protected throughout its lifecycle. To address the evolving security posture, Xiaomi will continue to improve its IoT technology and security capabilities, improve the security and privacy protection features of its products and services, optimize its security and privacy management system, and continue to demonstrate them through authoritative certifications, white papers, and privacy policies to build users' confidence in Xiaomi's products and services and make them more confident in choosing and using Xiaomi's products and services.

Xiaomi firmly believes that only by respecting and protecting users' information security and privacy can users trust Xiaomi IoT products in the long run. Therefore, Xiaomi continues to increase its investment in security and privacy, and is committed to delivering Xiaomi's normative practices, best practices, and technical capabilities in IoT security and privacy technologies to its partners to provide users with trusted and secure IoT products and services.

08

Glossary

English Abbreviations	Full name	Definition
DND	Do not disturb	Users can switch the DND mode on to silence the voice reporting of Mi Robot Vacuum.
SN	Serial Number	The SN is a unique identifier assigned incrementally or sequentially to an item, to uniquely identify it.
IMEI	International Mobile Equipment Identity	IMEI is a unique number to identify mobile phones.
MAC	Media Access Control	A unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.
BLE	Bluetooth Low Energy	BLE is a wireless personal area network technology.
HTTPS	Hyper Text Transfer Protocol over SecureSocket Layer	HTTPS is an HTTP channel with security as its goal; on the basis of HTTP, the security of the transmission process is guaranteed through transmission encryption and identity authentication.
Wi-Fi	Wireless Fidelity	Wi-Fi is a wireless local area network technology created in the IEEE 802.11 standard.
GPS	Global Positioning System	GPS is a high-precision radio navigation positioning system based on artificial earth satellites.
AES	Advanced Encryption Standard	AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
ECDH	Elliptic Curve Diffie - Hellman	Elliptic-curve Diffie - Hellman (ECDH) is a key agreement protocol that allows two parties, each having an elliptic-curve public - private key pair, to establish a shared secret over an insecure channel.
PAI	Personal Activity Intelligence	PAI is a health assessment system that uses an algorithm to transform complex information such as heart rate, activity duration, and other health data into a single numerical value unique to each user.