

Xiaomi Cloud Service Data Migration Guidance

1. Product Introduction

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

2. Cloud Service Migration Application Process

2.1 User Application

Users can visit the platform <http://dataact.mi.com/> to submit specific cloud service migration requests, which include three aspects: migrating data (downloading data to a local device and no longer using Xiaomi cloud services — in this case, the data download link will remain valid for 30 days), backing up data (users adopting a multi-cloud strategy and using services from multiple cloud providers. Downloading data to a local device and subsequently uploading and backing it up to cloud services provided by other suppliers while retaining Xiaomi cloud services. The data download link will remain valid for 30 days), and deleting data (requesting Xiaomi to delete the data on the cloud service).

2.2 Xiaomi Response Process

- Notice Period

According to the requirements of the Data Act, users must first notify the cloud service provider that they have submitted a migration application. The maximum duration of the notice period is 2 months. During these 2 months, the cloud service provider (such as Xiaomi) will prepare for the user's migration (for example, exporting relevant data, obtaining contact information of the intended cloud service provider).

- Transitional period

Cloud service providers should generally complete cloud service migration within 30 days.

Where the mandatory maximum transitional period is technically unfeasible, the provider of data processing services shall notify the customer within 14 working days of the making of

the switching request, and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months.

- The period for data retrieval

The original cloud service provider (such as Xiaomi) must reserve a 30-day period for data retrieval.

3. User Self-Service Download, Backup Path and Technology

Support data download for users on the desktop version of the cloud service.

Specific path: Settings -> User Rights -> Get Data Copy -> Apply for Download

- After clicking to request the download, the system will enter the status of preparing a data copy.
- After the data copy is ready, the button will change to "Get Data Copy," at which point you can download the corresponding file.
- The download link for the file will be sent to the user's email in the form of an email. After downloading, use the password provided in the email to decrypt the file, and you will be able to access the exportable copy of the cloud data.

4. Data Format and Structure

The user data download service provides a function for exporting all user data, with the results displayed in JSON format.

The exported data structure is tableName: tableRecords.

Where tableName represents the name of the data table, and tableRecords represents the specific records of the table as a JSON array.

5. Key Business Data that Can Be Exported

Service Name	Exportable primary data about the file
Recorder	<ul style="list-style-type: none">• The type, sizes, names, and URLs of documents.• Create time, upload time, delete time, ID, purge time, recover

	time of documents.
Contact List Service	Contents, create time, status (deleted or not), types and update time
Find device	Lock content, phone information, status, and contents, update time
SMS service	Contents, creator, deleter, last update time
Call Record Service	Creator, modifier, contents, status
Sticky Note	<ul style="list-style-type: none"> • Contents, history, folder name, status, types • Create time, update time, status, orders
Micard	Card content, record status, the status of data synchronization
Browser	Contents, status
Cloud Card	contents
Application Backup Service	User device id, product, IMEI, backup time, backup size, clear time, pkgName, label, version name, version code, whether icons are active, APK size, delete time, oldest backup time, URL
Music	playlist Online Id, song Online Id, status, type, create time, update time, size and asset
Calendar	Status, types, and contents
Lending Model	loan information, credit information, status, type, create time, update time, content, size, asset
App search	record, type, search time, status, create time, update time, size and asset

Common Phrases	phrase, type, status, create time, update time, size, asset
Clipboard	text, type, status, create time, update time, size, asset

6. Key Metadata that can be Exported

	Field Name
User Quota	Create time
	Expire time
	size
	status
	type
Service Quota Usage	type
	used status and volume
Gift Membership Data	amount
	channel
	Create time
	level
	type

7. Data that cannot be exported

Micloud user id mapping data

The file of Membership sharing

The file of Micloud sharing

Vip operation stats/vip operation information/vip gift

Bill and user profile

activity data such as tickets, activation codes

Users' status data

8. Is cloud migration charged?

In general, it is free.

9. Location of Cloud Server

The data center cloud server is located in Amsterdam, Netherlands.

10. Protection Measures for Cloud Storage Content

10.1 Technical Measures

Xiaomi Cloud is built to protect your privacy. The data synchronized and stored in Xiaomi Cloud is strictly encrypted. We will not access, view, or analyze the data you store in Xiaomi Cloud.

10.2 Organizational Measures

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

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

We are committed to ensuring the confidentiality and protection of our users' personal information. To prevent unauthorized access, disclosure, or similar risks, we have established industry-recognized physical, electronic, and managerial procedures to safeguard and secure the information.

10.3 Contractual Measures

We will conclude a Xiaomi Cloud Terms of Service <https://i.mi.com/useragreement?> with our users and promise that we will prevent unlawful access to or transfer of non-personal data held in the European Union where such access or transfer would create a conflict with Union law or the national law of the relevant Member States.