365mobilesync

User data security in the 365mobilesync application

Whitepaper

Table of Contents

365mobilesync integration with Microsoft Azure 3
Data flow structure | 365mobilesync 3
Additional security features 4
Data compliance with GDPR guidelines 4
Data privacy policies 4

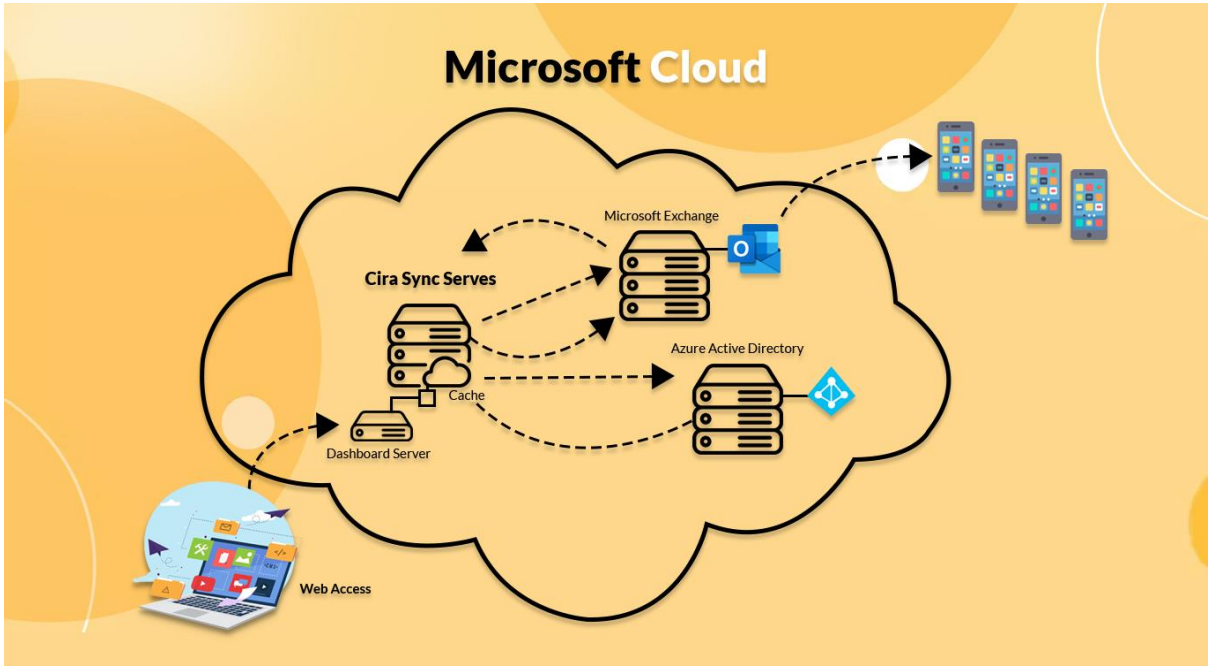
All the user data in the 365mobilesync application is well-secured and compliant with all existing data security laws.

365mobilesync integration with Microsoft Azure

Microsoft Azure ensures world-class security that ensures safe utility for more than 100 million Office 365 active users. 365mobilesync application is registered with Microsoft Azure and uses the Azure Consent framework. The user subscriber data is kept and maintained within the MS cloud.

Data flow structure | 365mobilesync

See how data flows between mobile devices, 365mobilesync, and Microsoft cloud.



1. Sync configuration in 365mobilesync dashboard
2. The system reads sync configurations as a request
3. The system pulls desired contact data from Azure Active Directory using Exchange Web Services (EWS)
4. Compares contact data pulled from Azure Active Directory with MS Exchange data
5. Updates user mailboxes using EWS
6. During the update, the EWS pushes user mailbox data to mobile phones

Additional security features

Dashboard security: Dashboard is the only public internet endpoint and is secured.
Password protection: 365mobilesync does not store any passwords. Log in to the application and redirect to Microsoft login.
EWS protection: HTTPS connection for mailbox updates. There is no flow through the public internet.
Subscription & Licensing data: Stored in Stripe. Accessible from the dashboard and user process.
Cache: The application cache sync configuration data & data from Azure Active Directory into a secure Cloud Database.
Server security: Multi-layer security is available.

Data compliance with GDPR guidelines

365mobilesync is a subscriber-based platform. So, data sync with mailboxes is attached to the subscriber account with encryption.

GDPR compliances followed in 365mobilesync,

A. Delete user data upon user request
B. Data turn over to the user upon request
C. EU user data is to be stored in servers physically located within the EU
D. We inform users how we process data, how it is used, and why it is used

Data privacy policies

Users have complete control over what to share and what not with the application. Users can edit, modify, or delete their accounts. Change subscription plans and choose whether to receive promotional offers & target ads from 365mobilesync.

Learn more about how we handle user data by contacting our team.