Thinfinity Workspace Mobile App Privacy Policy

Last Updated: December 2024

1. Introduction

This Privacy Policy applies to the Thinfinity Workspace mobile applications for Android and iOS ("the App"), developed and provided by Cybele Software, Inc. ("Cybele Software", "we", "our", or "us"). The App is designed for enterprise users to access remote desktops, virtualized applications, and files securely. Cybele Software is committed to protecting your privacy and handling your personal data with transparency and integrity, in full compliance with the EU General Data Protection Regulation (GDPR).

This policy describes how the App collects, processes, and safeguards your information. It also explains your rights as a user. The App is typically used in conjunction with your organization's Thinfinity Workspace environment and identity provider. While this policy focuses on the App's practices, your organization is responsible for the data you access and process through the service.

2. Data Collected and Processed

Minimal Data Collection:

The App is designed with a data minimization philosophy. It does not collect or store personal data on your device, except as strictly necessary for authentication and secure operation:

- **Authentication Token:**
  When logging in, the App integrates with your organization's selected Identity Provider (via OAuth 2.0 or SAML SSO). The only personal data handled by the App is the authentication token or assertion provided by the Identity Provider, which may include a user ID or email. This token is held in memory only for the active session and is not stored persistently. Usernames and passwords are not collected or stored by the App.

- **Device Permissions (User-Initiated Only):**
  The App may request access to device features—such as the camera, microphone, or files—only when you choose to use these features within an authenticated session. Any such data (e.g., camera feed, audio, file upload) is transmitted securely and directly to your organization's Thinfinity Workspace environment, never stored in the App, and never transmitted to third parties.

- **Push Notification Token:**
  If you enable push notifications, the App will register a device push token with the relevant platform (Apple or Google). This token is used solely for delivering notifications and does not contain personal information.

No Local Storage of Sensitive Data:

The App does not store session data, files, or personal information on your mobile device's permanent storage. All caches or temporary data are cleared when you log out. No sensitive information remains after your session ends.

No Third-Party Analytics or Trackers:

The App does not integrate any third-party analytics, advertising SDKs, or social plugins. Your activity is private and not shared for analytics or marketing.

3. Purpose and Use of Data

Cybele Software uses the minimal data processed through the App exclusively to provide the intended service:

- **Authentication & Access:**
  Tokens are used to verify your identity and enable secure login to your remote workspace. No other processing occurs.

- **Feature Enablement:**
  Device data (camera, mic, files) is processed only as needed to provide features you initiate during remote sessions, and not stored or used beyond the immediate session.

- **Notifications:**
  Device tokens are used only to send relevant service notifications that you have consented to receive.

We do not sell, profile, or use your data for advertising. All data use is strictly limited to providing secure remote access as required by you and your organization.

4. Legal Basis for Processing

Our processing activities are based on:

- **Performance of a Contract:**
  Processing authentication and session data is necessary to deliver the service to you as an authorized user of your organization.

- **Legitimate Interests:**
  We have a legitimate interest in providing a secure and efficient enterprise remote access solution, always balancing this interest with your privacy rights.

- **Consent:**
  For features such as camera, microphone, and notifications, we request and rely on your explicit consent. You may withdraw consent at any time via your device or in-app settings.

5. Data Minimization and Storage Limitation

We strictly adhere to the principle of data minimization, collecting only what is necessary for the App to function. All session and authentication data are held only in memory during your active use and are cleared when your session ends. No persistent databases of personal information are created by the App.

Any additional data associated with your account, access, or activities is managed by your organization's Thinfinity Workspace environment according to their policies.

6. Device Permissions and User-Initiated Features

- **Camera & Microphone:**
  Access is requested only if you choose to use these features during an authenticated session. Data is streamed securely and is not stored or accessed by Cybele Software.

- **File Uploads:**
  Files are uploaded only when you select them and are transferred directly and securely to your organization's remote environment. The App retains no copies.

- **Push Notification:**
  If enabled, you will receive only service-related notifications. You may disable notifications at any time.

7. Data Sharing and Transfers

Cybele Software does not share your data with unauthorized third parties. The only data transfers that occur are:

- **To your organization's Thinfinity Workspace environment** (for authentication and service delivery).

- **To identity providers** (for authentication via OAuth or SAML).

- **To platform providers** (for delivery of push notifications).

All such transfers are protected by industry-standard encryption and security measures. Data location and retention are determined by your organization's infrastructure and configuration.

8. International Data Transfers

If your organization's Thinfinity Workspace server or Identity Provider is located outside the European Economic Area (EEA), data may be transferred to that jurisdiction. All transfers are encrypted and protected. Your organization is responsible for ensuring any required safeguards are in place.

9. User Rights Under GDPR

As an App user in the EU, you have the right to:

- **Be informed about data processing (as described in this policy).**
- **Request access to any data processed about you.**
- **Rectify inaccurate or incomplete data.**
- **Request deletion of personal data.**
- **Restrict or object to processing under certain conditions.**
- **Receive data you provided in a portable format.**
- **Withdraw consent at any time for features requiring it.**
- **Lodge complaints with your national Data Protection Authority.**

To exercise these rights, contact Cybele Software or your organization's IT administrator. Many requests can be resolved directly by your organization, who controls your account and access.

10. Security Measures

Cybele Software implements robust technical and organizational measures to protect your data, including:

- **End-to-end encryption** of all communications.
- **No local data storage** on devices.
- **Strict access controls** inherited from your organization's security policies.
- **Secure coding, regular testing, and rapid patching** of vulnerabilities.
- **Support for enterprise mobile security features and compliance requirements.**

11. Changes to This Policy

We may update this policy to reflect new legal requirements or changes in the App's features. Updates will be posted in the App and on our website, and the "Last Updated" date will reflect changes. Continued use of the App constitutes acceptance of the revised policy.

12. Contact Information

If you have questions about this Privacy Policy or wish to exercise your rights, please contact us:



Cybele Software, Inc.
3422 Old Capitol Trail, Wilmington, DE, 19808, USA



International
+1 (302) 892-9625



Email
info@cybelesoft.com

© 2002-2025 Cybele Software Inc. All rights reserved.