acolad.

Acolad Live Mobile Application Privacy Policy

Effective Date: 28.04.2025

At NIKITA (“we,” “our,” or “us”), your privacy is a top priority. This Privacy Policy outlines how we collect, use, store, and protect your personal data when you use our mobile application (the "App") for audio calling, VOIP calling, and related services (the "Services"). We are committed to ensuring that your personal information is handled in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR).

By using the App, you agree to the terms of this Privacy Policy.

We might collect, store, use, and/or share ("process") your information when you use our Services, such as when you:

Visit our website at https://www.acolad.com or any of our linked websites that reference this privacy notice.

Use our application, which requires a signed contract; thereafter, you can register and download the Acolad Live iOS or Android application from the Apple Store or Google Play Store.

This policy pertains to our mobile applications, Acolad Live for both iOS and Android, which offers audio and VOIP calling services within the European Union (EU), in compliance with the General Data Protection Regulation (GDPR) and the EU AI Act. Below is the updated privacy policy tailored to our app, ensuring alignment with these regulations.

Section 1. Information We Collect

We collect the following types of personal data when you use our Services:

a. Account Information

- First Name and Surname: To identify you within the App.
- Company Email Address: For account management and communication.
- Phone Number: For verification, contacting you, and providing calling services.
- Company Name: For account management and communication.
- Country of Origin: For account management and communication.
- Postal Address: For account management and communication.
- The legal basis for processing this data is Acolad's legitimate interest in managing its contractual relationship with its customers.

b. Communication Data

- Call Logs: We store information about the calls you make, including the phone number or ID of the person called, duration, and timestamp of the call.
- Voice Data: Voice data transmitted during calls (only during active calls and is typically not stored unless required for service improvements or legal purposes).

c. Device and Usage Information

- Device Information: Information about your device, such as device type, operating system version, and unique device identifiers.
- Usage Information: Data regarding how you interact with the App, including features you use, settings preferences, and error logs.
- IP Address: For call routing, troubleshooting, and ensuring the quality of your service.

Section 2. How We Use Your Information

We use the collected information for the following purposes:

- Provide and Improve Our Services: To facilitate audio and VOIP calls, optimize performance, and enhance the user experience.
- Account Management: To create and manage your account, authenticate users, and recover account access.

- Customer Support: To respond to inquiries, provide support, and resolve issues related to your use of our Services.
- Legal Obligations: To comply with applicable laws, regulations, or legal processes, including fraud prevention and security.

Section 3. Legal Basis for Data Processing (GDPR and AI Act Compliance)

We process your personal data based on the following legal grounds:

- Performance of a Contract: Processing necessary for the provision of our Services, including making calls, managing your account.
- Consent: For certain activities, such as sharing data with third-party service providers for analytics or marketing purposes, explicit consent will be obtained. If you do not provide full consent, certain functionalities of the App may not operate correctly or may be limited.
- Legitimate Interests: Processing data for security, fraud prevention, improving user experience.
- Compliance with Legal Obligations: If required by law (e.g., responding to law enforcement requests).

Section 4. Opt-Out Options

You have the right to opt out of certain data processing activities. If you wish to withdraw your consent for any purpose, you can do so at any time by contacting us at at data-protection-team@acolad.com Please be aware that opting out may affect the functionality and performance of our Services, and without full consent, some features may not work properly.

Section 5. Data Sharing and Transfers

We may share your personal data with the following third parties:

- Service Providers: Third-party companies are utilized for hosting, data analysis, customer support, and communications. These service providers only have access to the personal data necessary to perform their functions.

- Legal Authorities: We may disclose your personal data if legally required or in response to valid requests from law enforcement or other authorities.
- Business Transfers: In the event of a merger, acquisition, or sale of assets, your personal data may be transferred as part of that transaction; we will notify you of such changes.
- If you reside in the EU, your data may be transferred outside of the European Economic Area (EEA) to countries that may not offer the same level of data protection. We will take necessary measures to ensure your data is handled according to GDPR and any other applicable Data Privacy law like, but not limited to UK GDPR, PIPEDA.

Section 6. Data Retention

We will retain your personal data as long as necessary to fulfill the purposes outlined in this Privacy Policy. This includes:

- Retaining call logs and communication data for the duration required by applicable laws or regulations.
- Retaining account data as long as your account is active or needed to provide services and support.
- If you wish to delete your account or request the removal of your personal data, you may do so by contacting us at Acolad's DPO via e-mail at data-protection-team@acolad.com

Section 7. Your Rights Under the GDPR and AI Act

As a user in the EU, you have the following rights regarding your personal data:

- Right to Access: Request a copy of your personal data held by us.
- Right to Rectification: Correct inaccurate or incomplete data.
- Right to Erasure: Request deletion of your data, subject to certain conditions.
- Right to Restrict Processing: Request limitations on the processing of your data.
- Right to Object: Object to certain processing activities, such as direct marketing or the use of AI features.

- Right to Data Portability: Request transfer of your data to another service provider in a structured, commonly used, and machine-readable format.

To exercise any of these rights, please contact us at data-protection-team@acolad.com

Section 8. Security of Your Data

We take appropriate technical and organizational measures to protect your personal data from unauthorized access, loss, or alteration. These measures include encryption, secure protocols, and regular security audits. However, data transmission over the internet cannot be guaranteed to be 100% secure, and we cannot ensure the absolute security of your data during transmission.

Section 9. Third-Party Links

Our App may contain links to third-party websites or services that are not operated by us. We are not responsible for the content or privacy practices of third-party sites. We encourage you to review the privacy policies of any third-party services you interact with.

Section 10. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal obligations, or the introduction of AI features. When we make changes, we will update the “Last Updated” date at the top of this page. If significant changes are made, we will notify you through the App or via email.

Section 11. Sensitive Information

We do not process sensitive information. When necessary, with your consent or as otherwise permitted by applicable law, we may process the following categories of sensitive information:

- First name and last name

- Company email address
- Device IMEI and model number
- Location data

Section 12. Application Data

If you use our application(s), we may collect the following information if you choose to provide us with access or permission:

- Geolocation Information: We may request access or permission to track location-based information from your mobile device to provide certain location-based services. You may opt to change access permissions in your device's settings.
- Mobile Device Access: Permissions may be requested for certain device features, including Bluetooth, calendar, camera, and VOIP functions. Adjust permissions in your device's settings if desired.
- Mobile Device Data: Device information is automatically collected (e.g., device ID, model, IMEI, manufacturer), along with operating system and version information.
- Push Notifications: We may send you push notifications regarding your account or certain features of the application(s). You can opt out of these notifications in your device's settings.
- User Permissions: Required permissions are outlined for the successful operation of our audio VOIP mobile application.

Section 13. User Permissions

The following user permissions are needed to operate our VOIP audio application effectively:

- POST_NOTIFICATIONS: For showing notifications to the user, Android >= 12
- RECORD_AUDIO: Microphone permission during the phone call
- READ_PHONE_STATE: From the Android docs: "*Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device*.". Needed for managing Connections using ConnectionService.
- MODIFY_AUDIO_SETTINGS: Needed to switch audio device during VoIP calls
- FOREGROUND_SERVICE: Needed to sustain foreground services (of types phoneCall, microphone, connectedDevice and dataSync)

- FOREGROUND_SERVICE_MICROPHONE: Needed to get permission for the microphone in the background during the VoIP call
- FOREGROUND_SERVICE_PHONE_CALL: Needed for the phone call notifications
- FOREGROUND_SERVICE_DATA_SYNC: Needed for refreshing the connection with the VoIP platform (Azure Communication Services). Refreshes every 10 minutes if application is not in Doze.
- FOREGROUND_SERVICE_CONNECTED_DEVICE: Needed for managing Bluetooth audio devices in the background, for example switching from speaker to Bluetooth headset in a full screen activity on the lockscreen
- BLUETOOTH_CONNECT: Needed to connect with Bluetooth devices during the VoIP call for audio input & output.
- MANAGE_OWN_CALLS: Needed to provide a self-managed ConnectionService
- VIBRATE: Needed to enable vibration for incoming call notifications
- USE_FULL_SCREEN_INTENT: Needed to open up Full screen intents with the incoming call notifications
- RUNTIME PERMISSIONS
    - **Required permissions:**

      Requested at login of interpreter/client:

      RECORD_AUDIO

      READ_PHONE_STATE

      MODIFY_AUDIO_SETTINGS

      Requested at app startup:

      POST_NOTIFICATIONS

      See descriptions in previous section, Launch permissions.

    - ·**Optional permissions:**

      Requested at login:

      BLUETOOTH_CONNECT

Section 14. The Runtime Information We Collect

Log and Usage Data: We collect log and usage data, which includes service-related, diagnostic, usage, and performance information that our servers automatically gather when you access or use our Services. This data may be recorded in log files and can include your IP address, device information, browser type, user preferences, and other settings. Additionally, it may consist of information about your activities within the Services, such as date/time stamps associated with your usage, pages and files viewed, searches performed, and features accessed. This processing is necessary for maintaining service functionality and improving our Services.

Device Data: We gather device data, which consists of information about the devices you use to access our Services, including computers, smartphones, tablets, or any other relevant devices. This data may include, but is not limited to, your IP address (or proxy server), device and application identification numbers, hardware model, location, browser type, Internet service provider, mobile carrier, operating system, and system configuration information. This information helps us ensure the compatibility and performance of our Services across different devices.

Location Data: We collect location data, which refers to information regarding your device's location that can be either precise or imprecise. The type and amount of information collected depend on your device settings and the type of device you use to access our Services. For instance, we may utilize GPS and other technologies to collect geolocation data indicating your current location (which may be based on your IP address). You have the right to opt out of allowing us to collect this information by refusing access or disabling the Location permission in your device settings. However, please note that by choosing to opt out, you may lose the ability to use certain features of the Services that require location information.

Compliance Note

All data collected is processed in accordance with the principles laid out in the GDPR and the EU AI Act, ensuring that your personal data is handled lawfully, transparently, and securely. You reserve the right to access, rectify, and erase your personal data, as well as to withdraw your consent at any time.

Section 15. How We Process Your Information

We process your personal information for various purposes, depending on how you interact with our Services. This processing is based on your consent, the performance of a contract, our legitimate interests, or compliance with legal obligations. The following outlines the specific purposes for which we may process your personal information:

- Account Management: To facilitate account creation and authenticate user accounts, enabling you to create, log into, and maintain your account in good working order.
- Service Delivery: To provide and effectively manage the Services you have requested, ensuring that they meet your requirements and expectations.
- Customer Support: To respond to inquiries and provide support. We may process your information to address any questions or issues you may encounter with our Services.
- Administrative Communications: To send you administrative information related to our Services, such as details about our products and services, important updates, changes to our terms and policies, and other similar communications.
- Service Fulfillment: To fulfill and manage your transactions and services, including processing payments and exchanges made through our Services.
- User Communications: To enable communication between users when you choose to use features that allow interactions with other users.
- Feedback Solicitation: To request feedback on our Services, allowing us to contact you regarding your experience and suggestions.
- Security and Fraud Prevention: To protect our Services and users by monitoring for fraud and security threats. We may process your information as part of our security measures.
- Usage Analysis: To analyze how you use our Services to identify issues, improve functionality, and enhance user experience.
- Vital Interests: To process your information when necessary to protect or save an individual's vital interests, such as preventing harm.

Sharing of Personal Information

We may share your personal information in the following circumstances:

- Business Transfers: In connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.
- Google Location Matrix API: When using Google Maps Platform APIs (e.g., Google Maps API, Places API), we may share your information for location-specific services. You can find out more about Google's Privacy Policy through their website. We may process the following location-related data:
    - Origins and destinations in the form of place IDs, addresses, or latitude/longitude coordinates.
    - Distance and travel time between various origins and destinations.
    - Duration in traffic based on your specified driving mode and departure time.
    - We may cache your location on your device for 30 consecutive calendar days. After this period, we will delete the cached Google Matrix content. You may revoke your consent at any time by contacting us through the details provided at the end of this document.
    - We do not use cookies in our mobile apps and when we accessing google maps we do not store or retain any
- Affiliates: We may share your information with our affiliates (parent company, subsidiaries, joint ventures, or other companies within our control), which will be expected to comply with this privacy notice.
- Suppliers and Service Providers: We may share your information with our partners to facilitate the Services, including platforms like Google Firebase for notifications.

Compliance with GDPR and EU AI Act

We will ensure that any processing of your personal data, including AI technologies, when and if applicable, complies with the principles established by the GDPR, UK GDPR and the EU AI Act, ensuring transparency, accountability, and respect for your rights. You are encouraged to exercise your rights detailed in our privacy policy, such as the right to access, rectification, erasure, and objection to processing.

Section 16. Verification and Authentication Process

Upon receiving your request, we verify your identity to ensure you are the individual associated with the information in our application. Verification may involve a PIN code or biometric information. We do not store this sensitive data on our servers.

Section 17. Contact Us

The persons concerned by the processing of their data are informed that they may submit a complaint to the competent data protection authorities:

- **Austria**: Österreichische Datenschutzbehörde
- **Belgium**: Gegevensbeschermingsautoriteit
- **Bulgaria**: Комисия за защита на личните данни
- **Croatia**: Agencija za zaštitu osobnih podataka
- **Cyprus**: Επιτροπή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- **Czech Republic**: Úřad na ochranu osobních údajů
- **Denmark**: Datatilsynet
- **Estonia**: Andmekaitse Inspektsioon
- **Finland**: Tietosuojavaltuutetun toimisto
- **France**: Commission Nationale de l'Informatique et des Libertés (CNIL)
- **Germany**: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- **Greece**: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- **Hungary**: Nemzeti Adatvédelmi és Információszabadság Hatóság
- **Ireland**: Data Protection Commission
- **Italy**: Garante per la protezione dei dati personali
- **Latvia**: Datu valsts inspekcija

- **Lithuania**: Valstybinė duomenų apsaugos inspekcija
- **Luxembourg**: Commission nationale pour la protection des données
- **Malta**: Information and Data Protection Commissioner
- **Netherlands**: Autoriteit Persoonsgegevens
- **Poland**: Urząd Ochrony Danych Osobowych
- **Portugal**: Comissão Nacional de Proteção de Dados
- **Romania**: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
- **Slovakia**: Úrad na ochranu osobných údajov
- **Slovenia**: Informacijski pooblaščenec
- **Spain**: Agencia Española de Protección de Datos
- **Sweden**: Datainspektionen
- **United Kingdom**: Information Commissioner's Office (ICO)

For any inquiries, please contact Acolad's Data Protection Officer via email at data-protection-team@acolad.com