PRIVACY POLICY

Welcome to **SeeMeeGo**!

At SeeMeeGo App (hereinafter referred as App), we value your privacy and are committed to protecting your personal information. This privacy policy outlines how we collect, use, and protect your information when you use our App.

DEFINITIONS

While U.S. privacy law does not always use the same terminology, we use the following definitions adapted from the General Data Protection Regulation (GDPR) for clarity and consistency in this policy:

1) *Personal information* - any information relating to an identified or identifiable natural person ("data subject"), such as name, email, identification number, location data, or online identifier.

2) *Processing* – any operation or set of operations performed on personal information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure, or destruction.

3) *Data controller* - the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal information. In this case, the organization responsible for handling your personal information is DUBADU CORPORATION, Delaware, USA.

When you use this App, we may collect different types of information to provide services, improve your experience, and keep things running smoothly.

INFORMATION WE COLLECT IN THE APP

1. Information You Provide Directly

- *Account Details***.** When you register or update your profile, we collect information such as your name, email, phone number, and any profile details you choose to share.
- *Content You Upload***.** This includes any photos, videos, voice messages, or documents you upload or share through the App.
- *Messages & Support Requests***.** We collect information when you send messages, leave comments, or contact our support team.

2. Information Collected Automatically

- *Device Details***.** Information such as your device ID, operating system, and App version helps us ensure compatibility and performance.
- *App Usage Data.* We track how you use the App-features you tap, time spent, and preferences-to help us improve the experience.
- *Location (if enabled).* If you allow location access, we may use GPS data for location-based features. *You can turn this off anytime in your device's settings.*
- *Push Notifications.* If enabled, we may send you updates, alerts, or activity-related messages. *You can manage your notification settings in your device preferences.*
- *Tracking Technologies.* We may use cookies or similar tools to analyze usage and improve App functionality.

3. Information from Third-Party Services

- *Social Logins*. If you sign in using Google, Facebook, or similar accounts, we may access basic profile info (like your name and email) from those platforms.
- *Analytics & Advertising Tools*. We may use tools like Google Analytics or Firebase to understand how the App is performing and to show relevant content or ads.

You're always in control. You can manage or disable App permissions such as location access, notifications, or social login via your device's privacy settings at any time.

PURPOSES FOR COLLECTING PERSONAL INFORMATION

We collect and use your personal information for the following purposes:
• To provide and maintain the App and its features;
• To process transactions and deliver requested services;
• To respond to user inquiries and support requests;
• To detect, investigate, and prevent fraud and security incidents;
• To send service-related communications and marketing (with your consent);
• To comply with applicable legal and regulatory obligations.

Where applicable under foreign laws such as the GDPR, processing may be based on legal grounds including contractual necessity, consent, or legitimate interest.

SHARING OF DATA

We do not "sell" or "share" personal information as these terms are defined under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA).

1. Internal Recipients

We may share your data with specific teams within SeeMeeGo App operations:

• *Customer Support Team* - to respond to your inquiries submitted through in-app support channels.

• *Legal and Compliance Teams* - to fulfill legal obligations and enforce your rights.

• *Marketing and Product Development Teams* - based on your consent or our legitimate interests (e.g., to improve App functionality or inform you about new in-app features).

All internal access is strictly controlled and limited to authorized personnel under confidentiality obligations.

2. External Processors (acting on our behalf)

We use trusted service providers under Data Processing Agreements to support key app functionalities:

• *App hosting and infrastructure providers* to ensure App stability and uptime.

• *Content Delivery Networks (CDNs)* for fast and secure delivery of App content.

• *Email communication services* to send system messages, verification codes, or consent-based emails.

• *Payment processors* to handle in-app purchases securely and in compliance with PCI DSS standards.

• *Analytics providers* such as Google Analytics or Firebase, to track in-app performance, crash reports, and user engagement. We minimize data collected and apply measures like IP masking, pseudonymization, and limited data retention. Analytics are enabled only after obtaining user consent when required by law.

• *Anti-spam and App security tools* to detect abuse and protect both users and infrastructure.

All such vendors operate strictly under our instructions and meet data security and privacy requirements defined by GDPR.

3. External Controllers (independent entities)

We may also disclose data to third parties that act as independent data controllers, including:

• *Government agencies or regulators* when required by law or following lawful requests.

• *Auditors, legal advisors, or tax consultants* where disclosure is necessary for compliance or legal defense.

All such disclosures are minimized and legally justified.

4. Transfers to Other Countries

Some of our trusted service providers or infrastructure partners may be located in countries that have different data protection laws than those in your region. If your personal information is transferred to another country, including outside of the United States, we take appropriate steps to ensure that your data is handled securely and in accordance with this Privacy Policy.

These safeguards may include:

- Contractual commitments with the receiving party to uphold strong privacy and security standards.
- Technical measures such as data encryption, access controls, and audit procedures.
- Limiting access to your personal information only to those who need it to perform services on our behalf.

We regularly assess the privacy risks of cross-border data transfers and update our practices as needed to protect your information.

DATA RETENTION

We retain your information in accordance with applicable U.S. federal and state regulations, including relevant statutes of limitation, tax laws, and consumer protection rules.

Retention varies depending on the type of data and your activity in the App:

1. *Active Accounts with Obligations*. If you have purchased in-app services, subscriptions, or made transactions, your account and related data will be retained while those obligations are active.

2. *Inactive or Empty Accounts*. If you have not used the App, made purchases, or engaged with content for 24 consecutive months, and no financial or contractual relationship exists, your account may be deleted. You will receive an in-app or email notification beforehand with the option to reactivate.

3. *Financial and Transaction Data*. Stored for at least 7 years after your last purchase or payment activity.

4. *Support Requests and Communication*. Retained only as long as needed to resolve your issue, typically not more than 2 years, unless further interaction occurs.

5. *Legal Hold or Disputes*. We may retain data longer if needed to comply with litigation, investigations, or government requests.

We conduct regular reviews of all stored personal information. Where retention is no longer necessary for the original purpose and no legal basis for further storage exists, we will either:

• securely delete the data, or

• anonymize it to prevent any further identification of the individual.

YOUR PRIVACY RIGHTS

As a user of the App, you have the following rights:

• **Right to Access**: You can request a copy of the personal information we have collected about you.

• **Right to Correct**: If any of the information we hold is inaccurate, you may request a correction.

• **Right to Delete**: You may request the deletion of your personal information, unless retention is required by law or necessary for legal claims or obligations.

• **Right to Restrict Processing**: You can request limitations on how your data is used.

• **Right to Object**: You may object to the processing of your personal information, especially when it's based on our legitimate interests.

• **Right to Data Portability**: You can request your data in a machine-readable format or ask us to transfer it to another controller.

• **Right to Lodge a Complaint**: You have the right to file a complaint with a supervisory authority (e.g., your local Data Protection Authority).

If you wish to exercise any of these rights, please contact us at info@seemeego.com or through the "Help" or "Support" section in the App.

Your privacy rights may vary depending on your state of residence. For example, if you are a California resident, you may have specific rights under the California Consumer Privacy Act (CCPA), including the right to access, delete, or opt-out of the sale or sharing of your personal information.

USE OF AUTOMATED SYSTEMS FOR SECURITY

We do not use your personal information for automated decision-making that produces legal or similarly significant effects.

Any automated systems used within the App (e.g., for spam detection or fraud prevention) are strictly limited to technical filtering. They do not involve profiling or behavioral scoring that could impact your legal status, access, or individual rights.

FTC COMPLIANCE

We are committed to complying with the Federal Trade Commission's **(**FTC) privacy and data protection standards. This means we take necessary precautions to protect your personal information from unauthorized access, use, or disclosure, and ensure transparency in our data collection practices.

DATA SECURITY AND BREACH NOTIFICATION

We take the security of your personal information seriously and implement appropriate safeguards to protect it. In the unlikely event of a data breach involving your personal information, we will comply with applicable data breach notification laws and promptly notify affected users if required by law.

COMPLIANCE WITH GLOBAL DATA PROTECTION LAWS

While our company is registered and operates under the laws of the United States, we understand that our users may reside in different countries and jurisdictions. Therefore, we take

steps to ensure that our data handling practices comply not only with applicable U.S. regulations, but also with international data protection standards where relevant.

We currently implement and align with the following frameworks:

1. United States:

We comply with federal and state-level privacy laws, including:

• Children's Online Privacy Protection Act (COPPA) for users under the age of 13
• California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
• Applicable consumer protection and data breach notification laws in other U.S. states

2. European Union:

For users located in the EU, we process personal information in accordance with the General Data Protection Regulation (GDPR), including the principles of transparency, minimization, and lawfulness (Art. 3 GDPR – extraterritorial scope).

3. United Kingdom:

We follow the UK GDPR and Data Protection Act 2018 for data processing involving users in the UK.

4. Canada:

We align with the Personal Information Protection and Electronic Documents Act (PIPEDA) for transparency and accountability in data handling.

5. Australia:

We observe the requirements of the Privacy Act 1988, including individual access and correction rights.

6. Other Jurisdictions:

Where applicable, we take reasonable steps to adhere to local data protection laws, ensuring secure and lawful handling of your personal information regardless of location.

MINORS' DATA PROTECTION

We comply with laws governing children's privacy, including the U.S. Children's Online Privacy Protection Act (COPPA). We do not knowingly collect personal information from children under 13 without verified parental consent.

Parents or guardians may review, delete, or manage their child's information by contacting us at the email provided in the "Contact Us" section.

CHANGES TO CONSENT

You may withdraw your consent for data processing at any time by contacting us or adjusting your cookie preferences.

MANDATORY VS. OPTIONAL DATA PROVISION

Some data fields are required for contractual purposes-for example, payment details for in-app purchases. If you choose not to provide this information, we may be unable to grant access to certain features or services within the App.

Other fields are optional and used only with your consent. Not providing optional data will not affect your ability to use the App's core features.

CHANGES TO THIS PRIVACY POLICY

We've updated our Privacy Policy to better reflect how we handle your data and protect your privacy within the App.

The updated Privacy Policy will take effect either five (5) business days after we notify you in the App, or immediately upon its publication inside the App, depending on the nature of the changes.

You can always access and review the latest version of the Privacy Policy in the "Settings" or "Privacy" section of the App.

It is your responsibility to review the updated policy. By continuing to use the App after the changes take effect, you confirm your acceptance of the revised Privacy Policy. If you do not agree with any part of the updated policy, please discontinue using the App.

PRIVACY BY DESIGN AND BY DEFAULT

At SeeMeeGo, we are deeply committed to the principles of Privacy by Design and Privacy by Default. This means that data protection is not an afterthought - it's an integral part of every stage of our App's development, from initial concept to release and beyond.

Our approach includes:

• *Data Minimization by Default*. We only collect and process the personal information necessary to deliver core functionalities. Any additional data is gathered strictly on an opt-in basis, with your explicit consent.

• *Default Privacy Settings*. Your personal information is protected by default. Visibility and data-sharing settings are turned off unless you actively choose to enable them.

• *Built-in Security Measures*. We implement robust technical and organizational safeguards including encryption, role-based access controls, and regular audits - to ensure your data remains safe at all times.

• *Early Integration of Data Protection*. Privacy risks are assessed during the earliest planning stages of any new App feature. This allows us to proactively mitigate risks before launch.

• *Continuous Review and Improvement*. Our systems and practices are routinely evaluated and updated to stay aligned with evolving privacy standards and legal requirements.

By embedding privacy directly into the DNA of our App, we aim to offer you a secure, respectful, and transparent data experience - every time you use SeeMeeGo.

In-App Cookie-Like Technologies & Transparency

We use in-app technologies that function similarly to cookies in order to support essential features and improve your overall experience within the App. These technologies may include local device storage, analytics tools, and event tracking systems.

They help us:

- Maintain secure and stable operation of the App;
- Understand how users interact with different features;
- Customize content and functionality based on your preferences;
- Deliver relevant in-app marketing messages (only with your permission).

Your choices matter, You can accept, reject, or adjust your preferences via the in-app privacy or settings panel.

We do not access or store non-essential information on your device unless you've given us permission through in-app prompts.

We respect your privacy settings and give you full control over tracking and personalization preferences.

Electronic Communications and Marketing

We comply with applicable U.S. laws and regulations regarding marketing communications and user consent:

• We send electronic marketing messages (e.g., push notifications, emails, SMS) only after receiving your clear opt-in consent.

• You may withdraw consent or unsubscribe at any time via in-app settings, message links, or by contacting support.

• We do not share your contact details with third parties for marketing without your explicit permission.

• No unsolicited promotional communications will be sent.

Device Access and Privacy Preferences

We respect your device-level and in-app privacy settings regarding tracking and communications. While universal standards (like "Do Not Track") may vary in support across devices, you can always control your data preferences directly through the privacy or cookie settings in the App.

WHO IS RESPONSIBLE FOR YOUR DATA?

DUBADU CORPORATION
254 Chapman RD STE 208 Unit 16795 Newark, De 19702
EIN 99-1804493

CONTACT US

If you have questions, comments or concerns regarding our privacy practices or the privacy policy, or wish to update your data, please contact our support team.

Effective Date: July 23, 2025