PRIVACY NOTICE FOR invAIte

BACKGROUND

MORROWLINE GLOBAL (Registration No. 202603116289 (NS0322389-P)), as operator of the application known as invAIte ("invAIte", "we", "our" or "us") sets out this Privacy Notice to explain the purposes, types, sources, uses, disclosures, retention, security measures, choices and rights relating to personal data processed in connection with invAIte.

For the avoidance of doubt, MORROWLINE GLOBAL is a sole proprietorship registered in Malaysia. This public Privacy Notice identifies the registered business name and registration number only, and does not publish owner identity details or residential address details.

This Privacy Notice applies to our mobile applications, hosted web RSVP flows, event pages, notification systems, calendar subscription tools, support channels, account deletion request pages, privacy-choice pages and related services. It also applies where another User provides your details to invite or identify you in connection with an Event.

The purpose of this Privacy Notice is to explain to you:

- the type of personal data we collect and how we collect it;
- how we use personal data;
- the parties to whom personal data may be disclosed;
- how personal data may be stored, transferred, retained and protected; and
- how we intend to deliver the rights and choices available to you under Applicable Laws.

1.0 Personal Data Confidentiality and Key Roles

1.1 We strive to protect the confidentiality and security of personal data provided to, collected by or processed through invAIte ("Data").

1.2 For the purposes of this Privacy Notice, "Data Controller" means the person or organization that determines the purposes and means of processing Data. For invAIte, the Data Controller is MORROWLINE GLOBAL (Registration No. 202603116289 (NS0322389-P)), as operator of the application known as invAIte, unless and until a different operator is formally identified in an updated notice or policy.

1.3 “Data Processor” means a service provider or other party that processes Data on behalf of the Data Controller. “Data Subject” means the identifiable individual to whom Data relates.

1.4 This Privacy Notice is intended for Account holders, Hosts, co-hosts, Invitees, Web RSVP guests, persons whose details are uploaded or selected by another User, support requesters, persons submitting reports, and any individual whose Data may be processed in connection with the Service.

1.5 Any service provider that we engage to process Data on our behalf is expected to process Data in accordance with applicable contractual, operational and legal obligations. Please understand that we may share Data with service providers and certain third parties as described in this Privacy Notice.

1.6 If Applicable Laws require us to appoint a Data Protection Officer, or if we choose to appoint one, we may publish or provide those contact details separately.

2.0 Choice to Supply Personal Data and No Sale of Data

2.1 Certain Data is needed to enable us to provide the Service, process account creation, verify phone numbers, secure invite-gated access, operate Web RSVP flows, deliver notifications, administer subscriptions, respond to support requests, investigate abuse and comply with Applicable Laws.

2.2 If you decline to supply Data that is required for a particular feature, we may not be able to provide that feature or the Service to you. For example, without a verified phone number and certain account information, we may not be able to create or secure your Account or permit access to invite-only Event details.

2.3 Other Data is optional and tied to particular features, such as contact access, location access, camera access, photo-library access, media-library access and document access. If you choose not to grant such permissions, some parts of the Service may not work or may be limited.

2.4 invAIte does not sell personal data. invAIte does not disclose Data to third parties for their own unrelated advertising purposes. We disclose Data only as described in this Privacy Notice, including to service providers, to other Users where Service functionality requires it, for legal and safety purposes, and in limited business-transfer situations.

3.0 Types of Personal Data Collected

3.1 Personal data generally refers to information that relates directly or indirectly to an individual who is identified or identifiable from that information. The types of Data we collect may vary according to the relationship, feature or Event context involved.

Type of Data	Examples
Account and profile data	Name, phone number, email address, avatar or profile image, account creation and update timestamps, settings, notification preferences and event-related counts or capability status tied to the Account.
Authentication and security data	Firebase phone-verification data, OTP workflow records, phone hashes, PIN hashes, trusted-device records, failed-attempt counters, lock states, recovery flags, audit logs, session controls and tokenized calendar subscription security metadata.
Host-uploaded invitee and contact data	Invitee names, phone numbers, phone hashes, contact labels, host-supplied display names, invitation routing metadata and related access-control data.
Event and guest data	Event titles, dates, times, locations, short location names, location coordinates where used, time-zone information, guest-list status, RSVP choices, plus-ones, co-host status, guest visibility settings, recurrence data and RSVP notes.
Communications and interaction data	Threads, comments, replies, announcements, reactions, polls, voting selections, poll outcomes, in-app notification records, support requests, problem reports, User reports, moderation workflow records and engagement qualification data.
Media and document data	Gallery photos, thread images, avatars, uploaded images, receipts, travel confirmations, booking documents, similar uploads, storage paths, URLs, metadata, validation results and OCR or extracted text from optional document-processing features.
Device, technical and usage data	Device tokens for push notifications, platform information, app boot records, crash and error telemetry, IP address, user-agent information, session identifiers, request metadata, access logs, debugging logs, rate-limiting signals and abuse-prevention signals.

Calendar subscription data	Subscription scope, token and URL, creation, revocation and regeneration timestamps, access count, last accessed time and requesting user-agent.
Subscription and billing entitlement data	Subscription product identifiers, store-managed entitlement status, renewal or expiry status, trial status and purchase or refund signals received from Apple App Store, Google Play Store or other authorized billing platforms where paid plans are offered.
Moderation, enforcement and legal data	Support report contents, User report contents, moderation state, suspension or restriction records, audit records, complaint correspondence, dispute correspondence and legal records.
Sensitive or special data in uploads	Data contained in documents, images or Event notes that may include health, accessibility, religious, financial, travel, government-document, children's or other sensitive information, depending on what Users choose to upload.

3.2 We do not describe invAlte as requiring biometric identifiers as a core feature of the current product. If we later introduce a feature that directly collects biometric data or another particularly sensitive category as a core feature, we expect to provide additional notice and, where required, obtain consent.

4.0 Sources of Personal Data

4.1 We may collect Data from the following sources:

Source	Description
Directly from you	When you create an Account, verify your phone number, edit your profile, create an Event, respond to an invitation, upload content, enable notifications, use location or document features, contact support, submit reports or exercise privacy choices.
From other Users	When a Host, inviter, co-host or other User uploads, selects or enters your contact details, adds you to a guest list, identifies you as an Invitee or attendee, submits a report involving you, or uploads content that includes your information.
From devices and integrated services	From Firebase, Google Cloud, Apple or Google notification infrastructure, Apple App Store or Google Play billing systems, operating-system permissions, media libraries, camera interfaces,

	document interfaces, calendar applications and mapping/location services.
From web and security mechanisms	From Web RSVP flows, access logs, throttling records, verification state, session controls, request metadata and other technical mechanisms used to secure access and maintain the Service.

5.0 Use of Personal Data

5.1 Data may be used or processed by us, or by our service providers, for the following purposes:

(a) to create, maintain, verify and secure Accounts;

(b) to authenticate Users through Firebase phone verification or other verification mechanisms;

(c) to secure Accounts, devices, sessions, invite flows, Web RSVP access and calendar tokens;

(d) to match selected Invitees to registered Users through privacy-preserving methods where appropriate;

(e) to route invitations and support Event access controls;

(f) to display and manage Event details, guest lists, RSVPs, polls, threads, co-host workflows, reminders, galleries and expense coordination records;

(g) to provide Web RSVP access tied to invite status, phone verification, session restrictions and Event rules;

(h) to send push notifications and other operational or service-related communications;

(i) to enable optional features that rely on permissions such as contacts, location, camera, photo library, media library or document access;

(j) to process, validate, normalize or extract data from uploaded images or documents where a feature requires it;

(k) to generate, serve, revoke and secure tokenized calendar subscription feeds;

(l) to administer Subscriptions, trials, entitlement checks, plan status, cancellations and store-managed refund or billing status;

(m) to respond to support requests, problem reports, safety issues, complaints and moderation reports;

(n) to investigate abuse, spam, fraud, unauthorized access, safety concerns, violations of Terms and Conditions or suspicious activity;

(o) to improve reliability, troubleshoot errors, debug issues, maintain service integrity, perform audit and risk management and protect the Service;

(p) to enforce our contracts, protect legal rights and defend claims;

(q) to comply with legal, regulatory, court, law-enforcement, App Store or governmental requirements; and

(r) for all other purposes incidental and associated with any of the above or otherwise permitted by Applicable Laws.

6.0 Contact Import, Non-User Invitees and Web RSVP Guests

6.1 Contact access is optional and is intended to help Users invite people more easily. If a User grants contact access, invAIte may read contacts locally on the device so the User can search, filter and choose who to invite.

6.2 We do not describe invAIte as automatically uploading a User's entire address book to our backend by default for invitation matching. For invitation routing and registration checks, the product is designed around the contacts or phone numbers the User actually selects, enters or submits for an invite flow.

6.3 We do not use imported contact data for unrelated marketing to those contacts.

6.4 invAIte may process limited Data about persons who do not yet have an Account, including a name supplied by a Host or inviter, phone number, phone hash, invitation status, guest-list placement, RSVP-related data, Event access records, verification records and support or moderation records related to an invitation or Event.

6.5 Non-user Invitee Data may come from Hosts, inviters, co-hosts, the Invitee's own Web RSVP interaction, Firebase phone verification or our security and logging systems. Such Data may be used to deliver or route invitations, match Invitees to existing Accounts where appropriate, protect Web RSVP flows, maintain guest lists, preserve Event records, investigate abuse and comply with law.

6.6 Non-users may contact us through support@invaite.app or https://invaite.app/privacy-choices.html to request access, correction, deletion or limitation of certain processing, or to ask us to stop further invitations where appropriate.

6.7 Where a person asks us not to send or route further invitations, we may retain limited suppression data, such as a phone number hash or similar identifier, for the purpose of honoring that request, preventing future unwanted invitations, preserving safety controls and maintaining abuse-prevention or compliance records.

6.8 We may not be able to delete or alter information that forms part of a Host's Event records, invite history, moderation records, legal records or records we must keep for security, fraud prevention, dispute resolution or compliance reasons. In those cases, we may instead limit future use, suppress certain routing or de-identify Data where feasible.

7.0 Disclosure of Personal Data

7.1 For the purposes above and for the purpose of providing, securing and operating the Service, Data may be disclosed to the following parties:

Recipient	Purpose / Examples
Service providers and Data Processors	Firebase / Google Cloud, Apple and Google notification infrastructure, storage, security, logging, technical support, email delivery providers such as Resend, mapping/location providers where used, and other infrastructure or operational providers.
App Stores and billing platforms	Apple App Store, Google Play Store or other authorized billing channels where needed to process purchases, renewals, cancellations, entitlement status, trial status, chargebacks or refunds for Paid Plans.
Other Users inside the Service	Hosts, co-hosts, Invitees or Event participants may see your name, avatar, RSVP status, guest-list presence, poll activity, thread participation, uploaded gallery content, co-host status or expense-related data depending on settings, roles and Event context.
Hosts, co-hosts and downstream handlers	Hosts and co-hosts may independently view, copy, screenshot, export, forward, store or otherwise handle guest or Event information outside invAIte. Such Users are responsible for their own legal, confidentiality and privacy obligations.
Legal, safety and enforcement recipients	Courts, regulators, law-enforcement agencies, governmental authorities, legal claimants, affected parties, investigators or other recipients where reasonably necessary to comply with law, respond to safety threats, investigate abuse, enforce rights or defend claims.
Professional advisers	Lawyers, auditors, accountants, tax advisers, consultants and other professional advisers appointed by us where necessary for legal, accounting, compliance, risk management or operational purposes.
Business transfer parties	A purchaser, assignee, transferee, successor, investor, adviser or other party involved in an actual or proposed restructuring, merger,

	sale, transfer, assignment or similar business or organizational change involving invAIte or its operations.

8.0 Cross-Border Processing and Storage

8.1 invAIte may use service providers or infrastructure that process, store or access Data outside Malaysia. As a result, Data may be transferred to, stored in, or accessed from jurisdictions that may not have privacy laws equivalent to those in Malaysia.

8.2 Where we transfer Data across borders, we intend to do so where we have an appropriate basis and with reasonable safeguards, contractual commitments or operational controls appropriate to the circumstances and Applicable Laws.

9.0 Security Measures and User Precautions

9.1 We use administrative, technical and organizational measures designed to help protect Data, including access controls, authentication flows, hashed identifiers in certain contexts, role-based restrictions, logging, rate-limiting, storage controls and security rules.

9.2 No system is completely secure. We cannot guarantee absolute security, uninterrupted availability or that unauthorized access will never occur. You also play an important role in security and should keep your phone, OTPs, PINs, invite links, calendar subscription URLs, devices and other credentials secure.

9.3 If you receive Data or information through the Service which is not intended for you, you should notify us promptly at support@invaite.app and should not misuse, disclose, copy or retain the information except as necessary to report the issue.

10.0 Retention

10.1 We retain Data for as long as reasonably necessary for the purposes described in this Privacy Notice, including service delivery, Event integrity, recordkeeping, legal compliance, security, enforcement, dispute resolution, audit, fraud prevention, backup and archival purposes. The periods below are operational targets and may be extended where law, disputes, safety incidents, fraud prevention or technical constraints require longer retention.

Data / Record Type	Indicative Retention Approach
Account and profile data	Generally retained while the Account remains active. After a verified deletion request or closure, we generally aim to remove or disable core account access within thirty (30) days, while certain residual records may remain longer for backup, legal, fraud-prevention, audit or support purposes.
Authentication and security records	OTP workflow records, phone-verification records, PIN security metadata, trusted-device records, failed-attempt counters and security logs are generally retained for short-to-medium security periods, typically from ninety (90) days up to three hundred sixty-five (365) days, and longer where linked to abuse, fraud, account recovery, incident response or disputes.
Event and communication records	Invitation records, guest lists, RSVPs, Event details, thread messages, poll records and related Event history may be retained while the relevant Event or Account remains active and afterward for as long as reasonably necessary for Event integrity, user history, support continuity, dispute evidence or legal rights.
Gallery and post-event media	Post-event gallery content is currently intended to be retained for up to thirty (30) days after the Event ends, after which it may be deleted or cleaned up through operational processes, subject to exceptions for legal, safety, incident-response or backup purposes.
Web RSVP, calendar-feed and technical access logs	Generally retained on shorter rolling periods, typically around thirty (30) to one hundred eighty (180) days, unless needed longer for security analysis, abuse prevention, troubleshooting or legal holds.
Support, moderation and dispute files	Generally retained for the life of the matter and commonly for up to twenty-four (24) months after closure, and longer where repeat-

	abuse analysis, legal claims, regulatory compliance or safety concerns require it.
Backups and residual copies	Residual copies may remain in backups, logs or technical archives for a limited period, typically up to ninety (90) days, and may not be removed immediately from every system at the same time.
Suppression data	Limited suppression data may be retained for as long as reasonably necessary to honor opt-out, stop-invite, abuse-prevention or safety requests.

11.0 Account Deletion and Data Deletion

11.1 If you created an invAIte Account, you may generally initiate Account deletion from within the app through the account settings, profile flow or another deletion mechanism made available by invAIte. We also provide a public outside-app request channel at https://invaite.app/delete-account.html.

11.2 For broader privacy choices, including rights requests and non-user Invitee requests, we also provide https://invaite.app/privacy-choices.html.

11.3 We may require identity verification before completing deletion, including phone verification, in-app confirmation, a current PIN, supporting information or similar checks appropriate to the circumstances.

11.4 A completed and verified deletion request generally results in disabling or deleting account access and associated authentication access, deleting or detaching certain profile data, deleting certain User-linked records where operationally appropriate, and anonymizing or de-linking certain historical records where full removal would break Event history or record integrity.

11.5 Account deletion does not necessarily mean every historical or downstream record will be erased. We may retain, archive, anonymize, de-identify or preserve certain information where reasonably necessary to maintain Event integrity, preserve invite history, keep safety or moderation records, comply with law, resolve disputes, enforce rights, honor suppression requests, maintain backups or preserve system integrity.

11.6 Deleting an invAIte Account does not by itself cancel an Apple App Store or Google Play Subscription. If you have an active store-managed Subscription, you must also cancel it through the relevant store interface to stop future renewals.

12.0 Rights, Requests and Choices

12.1 Subject to Applicable Laws and lawful limitations, you may have rights in relation to your Data, including the right to request access, request correction of inaccurate or outdated Data, withdraw consent where processing is based on consent, request limitation or cessation of certain processing, object to direct marketing, request information about how Data is used or disclosed, and make a complaint regarding our processing practices.

12.2 To exercise a request, contact us at support@invaite.app or use https://invaite.app/privacy-choices.html. We may need to verify your identity, request additional information or decline a request where Applicable Laws permit us to do so. Where allowed by law, we may charge a reasonable fee for an access request.

12.3 We aim to respond within the timeframes required by Applicable Laws. If we need more time where the law permits, we will tell you. If you act for a minor or another person and the law permits it, we may request proof of your authority.

13.0 Direct Marketing and Service Communications

13.1 invAIte may send operational or service-related communications such as verification messages, security notices, Event invitations, Event reminders, support replies, account-related notices, Subscription status notices and legal notices.

13.2 If we use Data for direct marketing in a way that requires notice, consent or choice under Applicable Laws, we will provide the relevant opt-out or control mechanism. You may also contact us to object to direct marketing through support@invaite.app or https://invaite.app/privacy-choices.html.

13.3 Operational, security, billing and service-critical messages may still be sent where reasonably necessary even if you opt out of marketing communications.

14.0 Children and Minors

14.1 invAIte is not intended for children under thirteen (13) years old.

14.2 If you are under the age of majority where you live but at least thirteen (13), you may use invAIte only with parent or guardian involvement and acceptance of the applicable terms.

14.3 Because invAIte involves real-world coordination, Event attendance, guest interactions, media sharing, location-related features and possible document uploads, parents and guardians should supervise use by minors appropriately.

14.4 Users should not upload minors' personal data, images, documents or sensitive information unless they have lawful authority and any required consent. If you believe a child under thirteen (13) has provided Data through invAIte without authorization, contact us at support@invaite.app.

15.0 Cookies, Web Technologies and Limited Telemetry

15.1 Our web surfaces may use essential technical mechanisms such as session identifiers, local storage, server-side session controls, request logs, throttling tools and similar technologies to maintain Web RSVP flows, support security, preserve session state, diagnose errors and operate the Service.

15.2 We may collect limited telemetry and technical diagnostics, including crash and error information, to help maintain and improve reliability. We do not describe the current invAIte product as relying on third-party advertising cookies, cross-site ad tracking or similar advertising profiling tools as a core part of the present implementation.

15.3 If we later introduce non-essential tracking technologies, we may provide additional notice or choices as required by Applicable Laws.

16.0 Personal Data Breach Handling

16.1 If we become aware of a personal data breach that triggers notification obligations under Applicable Laws, we will assess the incident and take steps we consider reasonably necessary in the circumstances, which may include containment, investigation, remediation and notification.

16.2 Where required by Applicable Laws, we will notify the relevant Commissioner or authority without unnecessary delay and within the required timeframe after becoming aware of the breach, and notify affected Data Subjects where such notification is legally required.

16.3 The timing, content and recipients of any notification will depend on Applicable Laws, the nature of the incident, the risk involved and the information reasonably available at the time.

17.0 Amendments to Privacy Notice

17.1 We may amend, supplement or replace this Privacy Notice from time to time. If we make material changes, we may provide notice through the app, website, support channels or other reasonable means.

17.2 The revised Privacy Notice will apply from the updated effective date unless otherwise stated.

18.0 Contact Us, Complaints and Language

18.1 If you have questions, concerns, requests or complaints about this Privacy Notice or our handling of Data, contact:

- Email: support@invaite.app
- Privacy Contact: Privacy Contact (support@invaite.app)
- Legal Notices / Privacy Requests: support@invaite.app. A physical service address is not published in this public version and may be provided where legally required or through a designated representative if appointed.
- Data Controller: MORROWLINE GLOBAL (Registration No. 202603116289 (NS0322389-P)), as operator of the application known as invAIte
- Account Deletion Request Page: https://invaite.app/delete-account.html
- Privacy Choices Page: https://invaite.app/privacy-choices.html

18.2 If you are dissatisfied with our response, you may also have the right to complain to the relevant Malaysian personal data protection authority or other competent regulator.

18.3 This Privacy Notice may be made available in English and Bahasa Malaysia. If there is any inconsistency between versions, the English version shall prevail except where Applicable Laws require otherwise.