

B R A C E Y S

Privacy Policy

Master privacy policy — patients, orthodontists, and guardians

VERSION

3.3 — Sri Lanka

ISSUED

24 August 2026

APPLICATION

Sri Lanka — see section 19

HOSTING

Mumbai, India

What this policy covers. It explains what Braceys collects, why, where it is stored, who it is shared with, and what you can ask us to do about it. The sections that matter most are **5** (facial data), **7** (children and guardians), **8** (who your data is shared with) and **13** (how long we keep it).

Read it together with the Braceys Terms and Conditions.

Privacy Policy

This Policy explains how **SimLanka (Private) Limited** ("Braceys", "we") handles personal data in the Braceys iOS app, its companion widget, and the Braceys website portal. It applies to patients, parents and guardians, and dental professionals. It applies one high standard of transparency to everyone, wherever they are, and adds a specific section for Sri Lanka.

1. Who we are and how to contact us

- Controller / Data Fiduciary: **SimLanka (Private) Limited** (registered number PV 10901), Ranmuthugala Estate, Kadawatha 11850, Sri Lanka
- **Privacy contact:** Pawan Tejwani, Managing Director — teambraceys@outlook.com
- **Data Protection Officer:** we have not appointed one. We are not required to appoint a Data Protection Officer at our current scale of processing. We keep this under review and will appoint one, and update this policy, if that changes.

2. Roles — Braceys, your orthodontist, and you

2.1 Braceys operates the platform. Your orthodontist independently provides your clinical care and holds their own records. Braceys gives no clinical advice of any kind; all advice and instruction reaching you through the app comes from your orthodontist.

2.2 **Where you use Braceys with a linked orthodontist (monitored use), your orthodontist or their practice is the controller — the data fiduciary — of the data processed for your clinical care, and Braceys acts solely as their processor**, on their documented instructions and under a data processing addendum. Braceys does not decide the purposes of that processing.

2.3 **Where you use Braceys without a linked orthodontist (independent use), there is no practice. You decide what goes into your record, you enter and manage your own treatment plan, and you decide what is kept and what is deleted. In that case you are the controller of your record and Braceys acts as your processor**, processing it on your instructions and for no purpose of our own.

2.4 In both cases, Braceys is an independent controller for a narrow and separate set of purposes: running, securing and lawfully administering the platform itself — account creation and authentication, security, abuse prevention, service integrity, billing and legal compliance. We are responsible for that processing ourselves.

2.5 If you move between monitored and independent use, the roles change accordingly from that point forward.

2.6 Your orthodontist's own privacy notice governs what they do with your data. We do not control that.

3. What we collect — complete inventory

The app's privacy manifest declares the following categories, none of which are used for tracking across apps or companies:

Declared type	What it is in Braceys	Sensitivity
User ID	Account identifier, username, display name, role, practice name	Standard
Health & fitness	Aligner wear sessions and derived compliance and habit statistics	Health data
Photos or videos	2D progress photos, 3D scan models, generated time-lapse	Health / biometric-adjacent
Other user content	Chat messages, treatment-plan notes	Health data (clinical content)
Device ID	APNs push token for delivering messages and reminders	Standard

4. Records we store, and where

Category	Fields and contents	Store
Profile	Email address (the guardian's, where the patient is under 18), username, display name, role, practice name, created date	Database
Sign-in and verification	Email address, password (stored hashed, never in readable form), and the short-lived one-time code used to confirm your email address at sign-up	Database
Care relationships	Patient-orthodontist links, status, who initiated or ended	Database
Invites and link requests	Invite codes, share tokens, request direction and status	Database
Messages	Message body, sender, timestamps, read receipts	Database
Wear sessions	Aligners in and out start and end times, source, notes	Database
Treatment plan and trays	Tray count, days per tray, current tray, wear goal, arch, dates	Database
Progress photos	JPEG image plus pose and alignment metadata, tray number, timestamp	Storage + DB
3D scans	USDZ and GLB model files plus capture metadata	Storage + DB
Time-lapse	Rendered before-and-after video plus completion record	Storage + DB
User settings	Enabled tools, reminder timing, accent, appearance	Database

Copies are cached on your device. Wear state is shared with the companion widget through an app group container on your device.

5. Facial data — classified as biometric data

5.1 Braceys classifies your 3D scan models and the facial measurements stored with your progress photos as biometric data. We apply that classification in every market in which the app operates, and we do not wait for a particular law to compel it. This data is also treated as special-category or sensitive personal data, and as health data, wherever those categories apply. In practice this means it is treated as special-category data under the Sri Lanka PDPA, and to the standard that regime requires.

5.2 3D scans. Scans use your iPhone's front TrueDepth camera. Reconstruction happens entirely on your device — depth fusion, meshing, and texture baking — and raw depth and capture data never leave your device. Only the finished model files you save (USDZ and GLB) and capture metadata are uploaded.

5.3 Photo alignment metadata. With each 2D progress photo we store head pose (roll, yaw, pitch), face-box, inter-ocular distance, alignment score, and pixel dimensions, solely to stabilise frames for comparison and time-lapse. Because these are measurements of facial geometry, they fall within the classification in section 5.1.

5.4 Consent. Biometric data is collected only with your separate, express, written, opt-in consent, given on its own screen and recorded — not bundled into acceptance of the Terms or the Privacy Policy. You may decline and continue to use every other part of Braceys, and you may withdraw consent and delete all saved models at any time.

5.5 Use. Biometric data is used only to show you your own record, to generate the comparison and time-lapse views you ask for, and — in monitored use — to make *your 3D scans and photographs* available to your linked orthodontist. **Your time-lapse is not shared with them unless you release it** (see section 8). We do not use it for identification, recognition, matching, authentication, profiling, advertising, or model training. We do not sell, lease, trade or otherwise profit from it.

5.6 Retention and destruction. Biometric data is held under the published retention-and-destruction schedule in section 13, and is destroyed when the purpose is satisfied or within 3 years of your last interaction, whichever comes first.

6. Why we process it, and our legal bases

Purpose	Data	Basis for processing
Create and run your account	Profile, credentials	Contract
Verify your email address at sign-up	Email address, one-time code	Contract, and our legitimate interest in keeping accounts secure
Wear tracking, plan, reminders, insights	Wear sessions, plan, settings	Contract + explicit consent (Art. 9(2)(a)) for health data

Purpose	Data	Basis for processing
Store photos, 3D scans, time-lapse	Images, models, metadata	Explicit consent
Share with your linked orthodontist	All clinical content	Explicit consent + contract
Messaging and read receipts	Messages, timestamps	Contract + explicit consent
Delivering reminders and notifications	Plan and settings, APNs token	Contract
Security, abuse prevention, service integrity	Account, device, log data	Legitimate interests
Legal compliance, breach notification	As required	Legal obligation
Marketing use of your time-lapse or images	Images, video	Separate opt-in consent only

The basis shown is described in ordinary language. The precise statutory basis differs by country: under the Sri Lanka PDPA we rely on the lawful bases set out in that Act;

We never use children's data for tracking, behavioural monitoring, profiling, or targeted advertising.

7. Children and guardians

7.1 Many orthodontic patients are minors, particularly in braces treatment. We apply high-privacy defaults and collect the minimum necessary.

7.1A **A person under 18 cannot use Braceys without a clinic.** Independent use — using the app with no linked orthodontist — is available only to patients aged 18 or over. Every minor on Braceys therefore reaches us through a clinic.

7.1B **How parental consent is obtained.** The orthodontist is contractually required to obtain valid, verifiable parental or guardian consent — to the minor's use of the app, to the processing of their personal data including biometric data, and to messaging — *before* inviting them, and to record it in a form they can produce on request. Braceys relies on that confirmation. Because minors cannot use the app independently, there is no route by which a child's data reaches us without a clinic having first obtained consent.

7.1C **If a minor's link to their clinic ends.** The minor cannot continue independently. Their account moves to a limited state in which their existing record is preserved and remains available to them and their guardian, but nothing new is collected and messaging is unavailable, until a new clinic link is established or they turn 18. Nothing is deleted.

7.2 **Everywhere we operate.** We treat every person under 18 as a child. We obtain verifiable parental consent before processing a child's data, and we do not track, behaviourally monitor, profile, or target advertising at children.

7.4 **Everywhere.** Whatever the local age threshold, we apply high-privacy settings by default to any account held for or by a person under 18, and we do not profile them or serve them advertising.

7.5 **Sri Lanka.** Children's special-category data is processed only with guardian consent and appropriate safeguards.

7.5A **A minor's account is registered to the guardian's email address.** Where the patient is under 18, the email address on the account must be the parent's or guardian's, not the minor's. The one-time verification code is sent to that address, so **the guardian activates the account**, and password resets and recovery emails go to them. This is also how we know that a guardian exists and is involved. When the patient turns 18 they may change the address to their own, which requires a fresh code sent to the new address.

7.6 **Guardian access — what a parent or guardian can see, and how.** Because the account is registered to them, the guardian simply signs in to it, on any device, using that email address and the password. **There is no separate guardian login and no guardian portal.** Whoever is signed in can see everything in the account: progress photographs, 3D scans, wear and habit data, the treatment plan, appointments, and messages with the orthodontist.

7.7 **What that means in practice.** A guardian does not need the minor's phone — they can sign in on their own device at any time. We cannot provide a separate guardian view. The app tells the young person clearly, at the outset and in language they can understand, that the account holder can see what is in it. Nothing about their record is hidden from them.

7.8 **Raising a concern.** Messaging is only ever possible with the one verified orthodontist the patient is linked to — no other user of Braceys can message them. If a young person or their guardian is worried about any message or anything else in the account, they should contact us at teambraceys@outlook.com. We may suspend the link with the clinic while we look into it. This does not replace contacting the police or another appropriate authority where that is warranted.

8. Who your data is shared with

- **Your linked orthodontist** — images, 3D models, wear data, insights, plan and messages, once a care link is active. Ending the link stops future sharing. **Your end-of-treatment time-lapse is not included:** your orthodontist cannot view, download or share it unless you separately release it to them in the app, and publishing it for marketing requires a further, separate consent. Both can be withdrawn.
- **Your linked patients** (if you are an orthodontist) — the plan, notes and messages you send.
- **Service providers:** Supabase, Inc. (authentication, PostgreSQL database with per-user row-level security, file storage, realtime messaging and edge functions); Amazon Web Services, Inc. (the cloud infrastructure Supabase runs on); Apple Inc. (push delivery and App Store distribution); Google LLC (Firebase Cloud Messaging on Android, and hosted libraries used to render 3D scans in the web portal); Cloudflare, Inc. (hosting, DNS and

content delivery for the Braceys website and web portal); and **Resend, Inc.** (delivery of account emails, including the one-time code that verifies your email address at sign-up — Resend receives your email address and the content of that email, and nothing else).

- **Legal:** where required by law, regulation, or to protect vital interests or safety.

We do not share with advertisers, data brokers, or analytics companies. We do not sell personal data.

9. What we do not do

- No cross-app or cross-company tracking — the app's privacy manifest declares tracking as false.
- No advertising SDKs and no third-party analytics SDKs in the build.
- No Apple Health (HealthKit), Apple Music, Apple Maps, or Calendar integration. Wear-time is our own data and is not read from or written to HealthKit.
- No third-party or social sign-in.
- No sale, no behavioural profiling, no model training on your content.

9A. Features that are not available yet

This policy describes the data we collect today. Some tools referred to in our Terms and Conditions are not built yet, and we collect nothing for them.

- **Appointment scheduling.** We do not currently collect or store appointment times, locations or appointment notes. If we introduce this feature, we will collect the scheduled time and any location or notes your clinic enters, share them with you and your linked clinic, and **update this policy and our app store privacy disclosures before the feature goes live.**

We will not begin collecting a new category of data without first updating this policy and, where the law requires it, asking for your consent.

10. Device permissions

Permission	Why
Camera	2D progress photos and 3D smile scans (front camera)
Photo library (add)	Saving progress photos and time-lapse to your library
Notifications	Reminders and new-message pushes
App group (entitlement)	Sharing wear state with the companion widget
Push / APNs (entitlement)	Message and reminder delivery

You can change or withdraw permissions in iOS settings at any time; some features will stop working.

11. Lock Screen and widget visibility

If you enable the Live Activity, an "aligners out" timer may appear on your Lock Screen and Dynamic Island, and the widget may show wear state on your Home Screen. This means treatment-related information can be visible to anyone who can see your phone without unlocking it. You can disable both.

12. Security

12.1 Measures include encryption in transit and at rest, authenticated access, and per-user row-level security enforced server-side in the database, so a user can only reach their own records and those shared through an active care link.

12.1A **How your account is protected.** We verify your email address with a one-time code when you create your account, and again if you change the address. **After that, signing in needs only your email address and your password — we do not send a code each time you sign in.** Your password is stored hashed and we never see it in readable form. Because your password is what protects your account, use one you do not use anywhere else, and tell us at teambraceys@outlook.com if you think someone else knows it.

12.2 The key shipped in the app is a public "publishable" key; it grants no data access by itself — access is enforced server-side.

12.3 Invite codes and share tokens control who can link to an account. Keep them confidential and tell us at teambraceys@outlook.com if one is exposed.

12.4 No system is perfectly secure. We maintain an incident-response plan and the notification commitments in section 16.

13. Retention

We keep your data for as long as your account is open, and then delete it. The periods below apply.

Data	How long we keep it
Account and profile	For the life of your account, then deleted within 30 days of the account being closed
Progress photos, 3D models and time-lapse	Until you delete them, or within 30 days of the account being closed. If you finish treatment and do not subscribe, we keep the reduced Smile Record described in section 13.1 for as long as your account remains open.
Wear sessions and insights	For the life of your account, then deleted within 30 days of closure

Data	How long we keep it
Messages and any appointment notes	For the life of your account, then deleted within 30 days of closure. Your orthodontist keeps their own copy under their professional obligations, and we cannot delete that.
Invite codes and expired tokens	30 days
Backups	Purged on a rolling 7-day cycle
Biometric data (3D models and facial measurements)	Destroyed when the purpose is satisfied, or within 3 years of your last interaction with the App, whichever comes first

Where we are required by law to keep something for longer, we keep only what the law requires and only for as long as it requires.

14. International transfers — hosting location

14.1 Data is hosted in **Mumbai, India**. Personal data of users in Sri Lanka is therefore transferred to and stored in India. Separately, a small amount of data — your email address and the content of account emails — is processed outside India by the providers named in section 8, in particular for sending your verification code.

14.3 **Sri Lanka users.** Sri Lankan law does not restrict the transfer of your data out of Sri Lanka. While your data is in India it is subject to Indian data protection law, and we comply with that law in respect of it.

14.5 Request a copy of the safeguards at teambraceys@outlook.com.

15. Your rights

To exercise any right, contact teambraceys@outlook.com. We will not discriminate against you for exercising rights. Withdrawing consent is as easy as giving it, and does not affect processing before withdrawal.

- **Sri Lanka (PDPA):** access, rectification, erasure, withdraw consent, object. Complain to the Data Protection Authority of Sri Lanka.

Deleting data from Braceys does not delete your orthodontist's clinical records, which they retain under their own professional and legal duties.

16. Breach notification

We will notify regulators and affected individuals within the timeframes each law requires — including under the Sri Lanka PDPA.

17. Changes to this policy

We will post updates here and give additional notice of material changes. Current version date: 24 August 2026.

18. Complaints

Contact teambraceys@outlook.com first. You may also complain to the Data Protection Authority of Sri Lanka.

19. Where this policy applies

19.1 This is a master policy. It applies to everyone who uses Braceys, in every country in which Braceys is made available.

19.2 Sections 7, 14, 15 and 18 record the position for Sri Lanka. As Braceys becomes available in a new country, we will add that country to those sections rather than issue a separate policy, and we will tell you if the position applying to you changes.

19.3 Nothing in this policy removes any right you have under the law of the country you live in.

19.4 Currently available in: **Sri Lanka**.

Braceys — Privacy Policy. Version 3.3, issued 24 August 2026 for Sri Lanka. SimLanka (Private) Limited, registered number PV 10901, Ranmuthugala Estate, Kadawatha 11850, Sri Lanka. Read together with the Braceys Terms and Conditions for Patients and the Braceys Terms and Conditions for Orthodontists.