> 需泰国律师审阅后正式启用 / Admin-only: requires review by a Thai lawyer before official activation

PDPA Privacy Notice (Short Form)

Version 1.1.0 | Effective date: 1 December 2026

This short-form notice is given under section 23 of the Personal Data Protection Act B.E. 2562 (2019) ("PDPA") at the time we collect personal data. It is displayed at signup, at KYC, in checkout, and (in spoken form) to people who receive calls from our AI. It summarises, and does not replace, our full Privacy Policy (docs key: privacy-policy). Thai version governs; the English and Chinese versions are translations (如有歧义以泰文版为准).

Part A. Notice to users (shown at signup, KYC and account settings)

A.1 Who we are

Data controller: [บริษัท สยามวอยซ์ เอไอ จำกัด / Siam Voice AI Co., Ltd.], [ที่อยู่สำนักงานใหญ่ / Head office address], กรุงเทพมหานคร. DPO: [dpo@example.co.th]. Telephone: [เบอร์โทรศัพท์].

A.2 What we collect and why

Collection point	Data	Purpose	Lawful basis
Signup	Name, email, Thai mobile number, password hash, language, OTP events, IP, user-agent	Create and secure your account, verify you, deliver the Service	Contract
Legal acceptances	Document key, version, hash, time, IP, user-agent	Prove what you accepted	Contract; legitimate interests
KYC (L0–L3)	ID/passport copy, selfie (face match), company documents, number-ownership proof	Verify identity, prevent fraud, unlock higher limits, verify caller ID	Legal obligation / legitimate interests; explicit consent for face (biometric) data (consent_kyc)
Checkout and wallet	Payment method type and masked reference, amount, tax details, billing address	Process payment, issue tax invoices, accounting	Contract; legal obligation
Calls and SMS	Numbers, call records, recordings (if recording consent given), transcripts, SMS content	Provide the Service, billing, support, security	Contract; consent for recording; legitimate interests
LINE linking	LINE user ID, display name, profile picture	Link your LINE account and deliver messages	Consent (consent_line_link)
Marketing (optional)	Email, phone, LINE ID	Send promotions	Consent (consent_marketing)

Collection point	Data	Purpose	Lawful basis
Login and device security	IP address and geolocation/ASN, browser/device fingerprint, login history	Login location and new-device alerts, prevent account takeover	Legitimate interests (security)
Fraud prevention	Fraud risk score and signals, trial-abuse signals (verified phone, device fingerprint, IP rate), flagged content, sampled transcripts	Block scams and toll fraud, prevent trial abuse, suspend abusive numbers or accounts	Legitimate interests; legal obligation where applicable
Call quality	Recordings (if recording consent given), transcripts, QA scores, supervisor monitoring logs	Score and improve call quality; business customers' supervisors may listen, whisper or take over a call	Contract; legitimate interests
LINE service	LINE user ID, messages	AI customer service and notifications on LINE	Consent (consent_line_link); contract for service messages once linked
Win-back, coupon and referral offers (optional)	Email, phone, LINE ID, inactivity or cancellation status	Send offers to inactive or cancelled users, coupons and referral invitations	Consent (consent_marketing and consent_winback)
Carrier and regulator compliance	End-customer KYC, sender-ID and number allocation records	Meet telecom operator audits and NBTC requirements	Legal obligation; legitimate interests; contract

A.3 Retention

Call recordings 90 days by default (configurable by business tenants); transcripts 1 year; billing, tax and accounting records 10 years (configurable default; 需持牌会计师/律师核实); audit logs 5 years; KYC documents for the relationship plus 5 years; support tickets 3 years; login-security, fraud-scoring and content-review records [12 months] (longer if tied to an incident or report); LINE data while the link is active; sender-ID, number-allocation and end-customer KYC records for the period required by the carrier agreement or NBTC (at least 5 years after the relationship ends). Other data is kept only as long as necessary for the stated purpose.

A.4 Who receives your data

Telecom operators and suppliers (including one affiliated supplier), payment gateway (Opn Payments / Omise), AI/LLM, speech (ASR/TTS), cloud hosting, LINE Corporation, email and monitoring providers, professional advisers and authorities where legally required. Some recipients are outside Thailand; transfers follow PDPA ss.28/29 and, where we rely on consent, consent_cross_border. We do not sell personal data. We do not train AI models on your content unless you opt in (consent_ai_training, default OFF).

A.5 Is providing data mandatory?

Data marked as required for the account, payment, legal compliance or KYC is necessary for us to provide the corresponding feature. If you do not provide it, we may be unable to create your account, process payments, raise your KYC level or place calls. Optional consents (recording, marketing, cross-border where optional, AI training, LINE linking) can be refused without affecting the core Service, though some features (for example call recording and transcripts, or LINE messaging) will not be available.

Where carrier agreements or law require, end-customer KYC, sender-ID and number allocation records and fraud or complaint reports may be disclosed to telecom operators and the NBTC. To serve each language we route calls and text to AI sub-processors by category: Thai speech recognition and text-to-speech, large language models, and Chinese speech recognition and synthesis. Data may therefore be transferred to or processed in Singapore, China, the United States or the European Union under PDPA ss.28/29 safeguards. Your stored data is kept in the region set for your tenant: Thailand (Bangkok) or Singapore. The vendors in use are listed in our sub-processor register, available on request, and no vendor may train models on your data.

A.6 Your rights

Access, copy, portability, object, erasure, restriction, rectification, withdraw consent (PDPA ss.30–36). Response within 30 days. Use the in-app data export/delete tools or [dpo@example.co.th]. You may complain to the Personal Data Protection Committee Office (PDPC).

A.7 Monitoring, fraud prevention and quality

We analyse login location and device fingerprints to send new-device and unusual-location alerts and to block account takeover. We calculate fraud risk scores, apply caps and a night-time anomaly cut-off, and sample and review outbound call and SMS content for scams; flagged cases may lead to suspension. Calls may be scored for quality (QA), and a business customer's supervisors may listen to, whisper to the AI during, or take over a live call; this is logged. You may ask for human review of a block or suspension.

Part B. Notice to people who receive or answer calls from our AI

Written notice (shown on our website and, where applicable, in messages), and spoken short form at the start of calls.

B.1 Spoken opening (summary)

"This is an AI assistant calling on behalf of [business name]. [If recording] This call may be recorded to provide the service and as evidence; do you agree? You can say no and the call will continue without recording or end. You can ask not to be called again at any time. Details: [URL / phone]."

B.2 Who is responsible

The business that asked the AI to call you (named at the start of the call) decides why your number is used and is generally the data controller. [บริษัท สยามวอยซ์ เอไอ จำกัด / Siam Voice AI Co., Ltd.] operates the platform

as processor and, for platform safety, billing, fraud prevention and legal compliance, as controller of the call records it keeps.

B.3 What we process about you

Your telephone number; the date, time, duration and result of the call; what is said during the call (audio only if recording is notified and not refused; transcripts and summaries); and, if you reply by SMS or LINE, the content of your reply.

B.4 Why

To carry out the call or message requested by the business customer; to provide interpretation or translation on a call; to keep evidence and quality records; to prevent fraud and abuse; to honour your do-not-call request; and to comply with law.

B.5 Recording

We record only after telling you and obtaining your consent. Refusing recording has no negative consequence for you. Default retention: recordings 90 days (the business may set a different period), transcripts 1 year.

B.6 Recipients

The business customer; our sub-processors (AI language model, speech recognition and synthesis, cloud hosting, telephony carriers); authorities where required by law. We do not sell your data, and our vendors may not train models on it.

B.7 Your rights and how to stop calls

Say "do not call me again", reply STOP / ยกเลิก / 退订 / หยุด / UNSUBSCRIBE to an SMS (processed immediately and at the latest within 24 hours across all systems; one confirmation SMS is sent), or contact [dpo@example.co.th]. You may also exercise PDPA rights (access, erasure, objection, etc.) against us or against the business customer. We respond within 30 days. You may complain to the PDPC.

B.8 Monitoring, review and quality scoring

Where a business customer's supervisor monitors a call, the opening or call notice says so. Calls and SMS made through our platform may be sampled and reviewed by authorised staff to detect scams and abuse, and scored for quality. Reviewers are bound by confidentiality and access is logged. Where law or a carrier agreement requires, records about calls that appear fraudulent may be reported to telecom operators and the NBTC.

Part C. Notice to contacts uploaded by business customers

This notice is for people whose details (name, phone number, other information) a business customer has uploaded or typed into Nexora AI Call so that they may be called, texted or messaged.

C.1 How we got your data

From the business customer that has a relationship with you or has another lawful basis to contact you. We did not collect it from you directly. The customer is responsible for having a lawful basis, which it must record before any call is placed, and for any consent needed for marketing. The business customer must give you its own privacy notice at or before first contact.

C.2 What we hold and why

Your name, number and any fields the customer supplied (for example appointment details) are used only to place or answer calls and messages the customer requests, apply do-not-call rules, calling-hour and frequency limits, bill the customer, prevent abuse and keep legally required records.

C.3 Retention

Contact lists are held for the period the customer keeps them in the platform and are deleted when the customer deletes them or closes the account (subject to the legal retention periods in the Privacy Policy). Call records follow the retention periods above.

Your number may also appear in call or SMS samples reviewed by authorised staff to detect scams, and in quality scores and supervisor-monitoring logs. If a number is reported in connection with fraud, related records may be shared with telecom operators and the NBTC.

C.4 Your choices

You may ask us or the customer to stop contacting you, to tell you what we hold, to correct or delete it. If you object, we add your number to the do-not-call list so that no tenant on the platform can contact you for marketing. Contact [dpo@example.co.th]. We respond within 30 days. You may also complain to the PDPC.

Part D. Notice of changes

We will update this notice when our processing changes materially, with a new version number recorded in our system.
