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

Privacy Policy

Version 1.1.0 | Effective date: 1 December 2026

1. Introduction and scope

This Privacy Policy explains how [บริษัท สยามวอยซ์ เอไอ จำกัด / Siam Voice AI Co., Ltd.] ("**Nexora AI Call**", "**we**", "**us**") collects, uses, discloses, stores and protects personal data when you use the Nexora AI Call website, applications, APIs, AI phone assistant, translation bridge calls, SMS, LINE Official Account messaging, enterprise knowledge base ("brain"), AI business-document drafting, prepaid wallet credit, subscriptions, reseller/agent programme and related support services (together, the "**Services**").

This Policy is written under the Personal Data Protection Act B.E. 2562 (2019) of Thailand ("**PDPA**") and applies to:

- **Users**: individuals who register an account (consumers, and staff or authorised users of business customers);
- **Business customers' contacts**: people whose phone numbers or details are uploaded or entered by a business customer and who may be called, texted or messaged through the Services;
- **Call recipients**: anyone who answers, receives or takes part in a call, SMS or message placed by or answered by our AI, whether or not they have an account;
- **Visitors** to our website and applications;
- **Resellers/agents** and their personnel.

Where a business customer uses the Services to process personal data of its own customers or contacts, the business customer is generally the data controller and Nexora AI Call acts as its data processor under a Data Processing Agreement. In that case the business customer's own privacy notice also applies, and you should direct requests to that business as well as, if you wish, to us.

2. Data controller and Data Protection Officer

Controller: [บริษัท สยามวอยซ์ เอไอ จำกัด / Siam Voice AI Co., Ltd.]
Address: [ที่อยู่สำนักงานใหญ่ / Head office address], กรุงเทพมหานคร
Tax ID: [เลขประจำตัวผู้เสียภาษี 13 หลัก]
Telephone: [เบอร์โทรศัพท์]
General support: [support@example.co.th]
Legal: [legal@example.co.th]

Data Protection Officer (DPO): [dpo@example.co.th]. The DPO monitors compliance, advises us, cooperates with the Personal Data Protection Committee Office (PDPC) and is the contact point for data

subjects.

Telecom services entity. Call minutes, SMS, number rental and carrier connectivity are supplied by a separate Thai telecom licensee, [Thai telecom licensee name / บริษัท [ชื่อ] จำกัด] (NBTC licence type [to be verified]), which acts as a controller for the carrier-related records it must keep (call detail records, number allocation records and the KYC records needed for carrier and regulatory compliance). The platform company and the telecom licensee share data only as needed for these purposes and under an inter-company agreement. [需核实: entity structure and licence type]

3. Personal data we collect

3.1 Account and identity data

Name, email address, Thai mobile number (E.164 format), password (stored only as an argon2id hash), preferred language, company name and role, login and OTP verification events, account settings.

3.2 KYC and verification documents

Depending on your KYC level (L0–L3): national ID card or passport copy, selfie/face-matching image (if the verification method requires it), company registration and VAT certificates, authorised-signatory documents, business address proof, proof of ownership of numbers you ask to use as caller ID, and verification results. Face images used for identity matching may be biometric data, which is **sensitive personal data** under the PDPA and is processed only with your explicit consent.

3.3 Voice recordings and transcripts

Audio of calls made or answered by our AI (only where recording notice or consent has been given before recording starts), automatic transcripts, translations, summaries, detected language, call outcomes, and, where relevant, spoken content that may reveal personal details. Voice recordings may identify an individual.

3.4 Contact numbers and data of third parties called

Telephone numbers, names, and any information supplied by a business customer or user about people to be contacted (for example contact lists, campaign lists, appointment details), as well as call detail records (time, duration, direction, result, carrier route, caller ID used).

3.5 Messages

SMS content and delivery status; LINE Official Account messages, LINE user IDs, display names and profile pictures that LINE provides to us when you add or message a connected Official Account or link your LINE account; support tickets and correspondence.

3.6 Payment and billing data

Top-up and subscription history, wallet balance and ledger, invoices and tax invoices, tax identification number and billing address, payment method type and masked reference returned by our payment gateway (e.g. last four digits, PromptPay reference). We do **not** store full card numbers; cards are processed by our PCI-compliant payment gateway.

3.7 Enterprise knowledge and documents

Files, text and data that business customers upload to their knowledge base, and documents drafted by our AI tools (quotations, contract packs), which may contain personal data of third parties.

3.8 Technical, usage and security data

IP address, device and browser type, user-agent, time zone, API key identifiers (not secrets), webhook delivery logs, audit logs (hash-chained), fraud-scoring signals and outcomes, blacklist/DNC entries, session data, cookie identifiers (see Section 14), error and performance data.

3.9 Legal acceptance and consent records

For each legal document and consent you accept or withdraw: document key, version, content hash, timestamp, IP address, user-agent and the account concerned.

3.10 Data from other sources

Data supplied by business customers about their contacts; data from LINE when you link accounts; data from payment gateways, telecom operators and suppliers (e.g. delivery reports, number validity); data from fraud-prevention and sanction/blacklist sources where lawful.

3.11 Security, device and fraud-prevention data

IP address and its geolocation and network (ASN), browser/device fingerprint derived from the user-agent, login and new-device history (used to send login location and new-device alerts), trial-eligibility signals (verified phone number, device fingerprint, IP rate, disposable-email check), fraud risk scores and the signals behind them (account age, KYC level, bursts, number of distinct destinations, short-call ratio, complaints, flagged content), and number, tenant and suspension records.

3.12 Content review, call quality and monitoring data

Samples of outbound call and SMS transcripts and items flagged by keyword or language-model scam detection, together with reviewer decisions; call-quality (QA) scores produced by a language-model rubric and rules from recordings and transcripts (for example whether the AI disclosure was given, whether the goal was achieved, politeness, hallucination flags); and logs of live supervisor monitoring (who listened, whispered to the AI or took over a call, and when).

3.13 LINE Official Account data

LINE user ID, display name, profile picture, the content and time of messages you exchange with our LINE Official Account (including conversations answered by our AI customer service and any hand-off to a support ticket), and the delivery of notifications (for example call summaries) sent to you by LINE.

3.14 Carrier and regulatory compliance records

Sender-ID registrations, records of which telephone number was allocated to which end customer and when, and the related end-customer KYC reference, which we keep to meet the requirements of telecom operators and the NBTC.

We do not knowingly collect other sensitive personal data (e.g. health, religion, criminal records). Please do not upload or speak such data unless necessary, and business customers must not use the Services to collect it without a valid legal basis and, where required, explicit consent.

4. Purposes and lawful bases

#	Purpose	Data	Lawful basis (PDPA)
1	Create and manage accounts, authenticate users, send OTPs	Account, technical	Contract
2	Provide AI calling, answering, translation bridge, SMS, LINE, knowledge base, document drafting	Account, voice, transcripts, contact data, messages	Contract; for call recipients, legitimate interests or the business customer's basis
3	Record calls and produce transcripts	Voice recordings, transcripts	Consent (consent_recording) obtained before recording; for service quality, evidence and dispute handling also legitimate interests where lawful
4	Billing, wallet, refunds, tax invoices, accounting	Payment, billing	Contract; legal obligation (accounting and tax laws, Revenue Code)
5	KYC, anti-fraud, anti-abuse, caller-ID verification, DNC, sampling of outbound content, suspension	KYC, call, technical	Legal obligation where applicable; legitimate interests (preventing fraud and unlawful use); explicit consent for sensitive biometric data
6	Security, audit logs, incident response, breach notification	Technical, audit	Legitimate interests; legal obligation
7	Customer support, tickets, complaints	Account, tickets, call data	Contract; legitimate interests
8	Marketing communications about Nexora AI Call (email, SMS, LINE)	Contact, account	Consent (consent_marketing)
9	Transfer of data to recipients abroad	As needed	PDPA ss.28/29 mechanisms; consent (consent_cross_border) where we rely on it
10	Improve models using your content (AI training)	Voice, transcripts, documents	Consent only (consent_ai_training), default OFF
11	Product analytics (aggregated, de-identified where possible)	Technical	Legitimate interests; optional cookies by consent

#	Purpose	Data	Lawful basis (PDPA)
12	Compliance with law, court or authority orders; establish, exercise or defend legal claims	As needed	Legal obligation; legitimate interests
13	LINE account linking	LINE ID, profile	Consent (consent_line_link)
14	Reseller/agent administration and commission	Agent, payment	Contract
15	Login location and new-device alerts; device fingerprinting for account security	IP geolocation/ASN, user-agent, login history	Legitimate interests (account security, preventing takeover and fraud)
16	Fraud scoring, toll-fraud prevention, trial-abuse prevention, number/tenant suspension	Account, call, technical, fraud signals	Legitimate interests; legal obligation where applicable
17	Sampling and review of outbound call/SMS content for scams	Transcripts, SMS content, flags	Legitimate interests (preventing fraud and unlawful use); legal obligation; call recipients are informed under Section 5
18	Quality (QA) scoring of calls	Recordings (only where recording consent was given), transcripts	Contract (service quality); legitimate interests
19	Live supervisor monitoring (listen, whisper, take over) by a business customer's authorised supervisors	Live audio/transcript stream, monitoring logs	Contract with the business customer; legitimate interests; participants are informed under Section 5
20	Disclosure of end-customer KYC, sender-ID and number allocation records to telecom operators and the NBTC; fraud/complaint reports to them	KYC, number and sender-ID records, reports	Legal obligation; legitimate interests; contract
21	AI customer service and notifications through LINE	LINE user ID, messages	Consent (consent_line_link) for linking; contract for service messages once linked
22	Churn win-back, coupon and referral offers by SMS, LINE and email	Contact, account activity (inactivity, cancellation)	Consent (consent_marketing and consent_winback); never to anyone who has opted out
23	Referral programme administration (referrer commission on referee's paid top-ups)	Referral code, referee's top-up amounts, payout details	Contract; legitimate interests

Where we rely on consent you may withdraw it at any time (Section 11) without affecting prior lawful processing. Refusing optional consents does not affect your use of the core Services. Consent to the core Service (consent_service) is the required collection and use of data necessary to provide the Service; it is never bundled with optional consents.

5. Calls to and from third parties

When our AI places or answers a call on behalf of a user or business customer:

1. The AI always states at the start of the call that it is an AI assistant and, for business calls, that it is calling on behalf of [business name]. This cannot be disabled.
2. Recording happens only after a notice or consent is given before recording begins. If the recipient declines, the call proceeds without recording where the Service allows, or ends politely.
3. The recipient may at any time ask not to be called again; we add the number to the platform DNC/blacklist and the customer's DNC list.
4. Business customers must have a lawful basis (recorded in the call request), call within permitted hours (default 08:00–20:00 Asia/Bangkok; marketing 09:00–18:00 on weekdays), use only caller IDs they own and have verified, and must not spoof numbers.
5. Recipients can exercise PDPA rights with us or with the business that called them (Section 11).
6. A business customer's authorised supervisors may listen to a live call, whisper instructions to the AI, or take the call over. The AI opening or the call notice says that the call may be monitored by a supervisor where this feature is active. Monitoring is logged.
7. Calls and SMS may be sampled and reviewed by authorised Nexora AI Call staff, and scored for quality, as described in Sections 3.12 and 4.

We receive recipients' numbers and call content only as needed to perform and secure the call. We do not sell recipients' data.

6. Who receives personal data

- **Business customers** (for their own tenant data, recordings, transcripts and reports).
- **Sub-processors and service providers** (Section 7).
- **Telecom operators and affiliated or independent suppliers** who carry calls and SMS (they necessarily receive numbers and, for voice, the audio). One supplier is an affiliated supplier within the owner's group; it is bound by contract and receives only the data needed for carriage.
- **Telecom operators, the NBTC and other authorities** where carrier agreements or law require: end-customer KYC, sender-ID and number allocation records, and fraud and complaint reports may be disclosed for carrier audits and regulatory compliance, under confidentiality obligations.
- **Payment gateway** (Opn Payments / Omise, Thailand), banks and PromptPay.
- **LINE Corporation** for LINE messaging.
- **Professional advisers, auditors, insurers**, under confidentiality.
- **Authorities and courts** where legally required.
- **Successors** in a merger or sale of business, subject to this Policy.

We do not sell personal data.

7. Sub-processors and cross-border transfers

Our sub-processor categories are: large language model providers (for example Anthropic, OpenAI, Google); speech recognition (ASR) and text-to-speech (TTS) providers; cloud hosting (Thailand or Singapore

region according to the tenant's storage_region setting); payment gateway; telephony/SMS suppliers (Thailand); LINE Corporation; email delivery; error monitoring. The current list is available on request at [dpo@example.co.th] and on our website.

Some providers are located or process data outside Thailand (for example Singapore, China, the United States, the European Union and Japan). We transfer personal data abroad only in accordance with PDPA ss.28 and 29, namely where (a) the destination has adequate data protection standards, (b) appropriate safeguards are in place (contractual clauses, binding corporate rules or equivalent that make data subject rights enforceable), (c) you have given consent after being informed of the inadequacy, or (d) a legal exception applies, such as necessity for performance of a contract with you or at your request. Where we rely on consent, it is collected separately (consent_cross_border).

AI vendors and language routing. To serve each language well we route calls and text to different AI providers, each a sub-processor: Thai speech recognition (for example iApp OpenThai, Typhoon), Thai text-to-speech (for example Botnoi), large language models (for example Claude, OpenAI, Gemini, Typhoon, and for Chinese Qwen, DeepSeek, Doubao, Kimi), and Chinese speech recognition and synthesis (for example Volcengine, Alibaba, iFlytek, MiniMax). Depending on the language and route, data may be transferred to or processed in Singapore, China, the United States or the European Union. The list of vendors in use is kept in our sub-processor register (Section below) and is available on request. No vendor may train models on customer data.

Data residency. Each tenant's stored data (recordings, transcripts, documents, files) is held in the region set by its storage_region setting: Thailand (Bangkok, th-bkk) or Singapore (sg), according to plan and availability. Some processing (for example by language-model, speech or messaging providers) may occur in other countries as described above. Platform back-ups are encrypted and kept offsite.

Sub-processor register. We keep a register of vendors that process personal data (telephony, SMS, language model, speech recognition/synthesis, payment, storage and LINE), recording for each its data-processing agreement status, the data categories, the region and the transfer mechanism, and the date and reference of the agreement. We give notice of material new sub-processors [30] days in advance on our website or by email, and customers may object as stated in the Data Processing Agreement.

Cross-border transfer mechanisms are those listed in PDPA ss.28/29 above: adequacy, contractual or other appropriate safeguards, consent (consent_cross_border) or a statutory exception. We rely on the specific mechanism recorded in the register for each vendor. [需泰国律师审阅: mechanism for each vendor]

AI training: We do not use customer content (voice, transcripts, messages, documents, knowledge base) to train or fine-tune AI models, and our model, ASR and TTS vendors are contractually prohibited from training on customer data. This changes only if you opt in through the separate checkbox consent_ai_training, which is OFF by default and may be withdrawn at any time.

8. Retention

Data	Retention
Call recordings	90 days by default (business tenants may configure a different period); then purged
Transcripts	1 year
Billing, tax and accounting records (invoices, tax invoices, credit notes, WHT certificates, referral commissions and payouts)	10 years. This is a configurable default; the legal minimum under Thai tax and accounting law is stated in SPEC as at least 5 years and we apply 10 years for safety. [需泰国律师审阅 / 需持牌会计师/律师核实]
Audit logs	5 years
KYC documents	Duration of the relationship plus 5 years after termination (AML and fraud-prevention)
Support tickets	3 years
Marketing consent and opt-out records	For as long as needed to prove consent or opt-out, and at least for the relationship plus 5 years
Legal acceptance records	Duration of the relationship plus 5 years
Account data	Duration of the account; deleted or anonymised within a reasonable period after closure unless another row applies
Login security data (IP geolocation, device fingerprint, login/new-device alerts)	[12 months] (configurable default)
Fraud scores, fraud flags and content-review records	[12 months]; records linked to a suspension, incident or report are kept with the audit logs (5 years)
Call-quality (QA) scores	Same as the transcript of the call (1 year)
Supervisor monitoring logs	5 years (with audit logs); live audio is not stored unless the call is being recorded
LINE data (user ID, messages)	While the LINE link is active; after unlinking, deleted or dissociated within [30 days], except messages kept in support tickets (3 years) or as the law requires
Sender-ID, number allocation and end-customer KYC records for carriers/NBTC	Duration of the relationship plus the longer of 5 years and the period required by the carrier agreement or the NBTC

When a period ends we delete or irreversibly anonymise the data, subject to legal holds (for example a pending dispute or authority request). Deleted data moves first to a soft-delete state and is then hard-purged by scheduled jobs; backups are overwritten in their normal cycle.

9. Security

We apply measures appropriate to risk, including encryption in transit and at rest, argon2id password hashing, hashed API keys and signed (HMAC-SHA256) webhooks, role-based access and tenant isolation, session cookies with httpOnly/secure flags, CSRF protection, tamper-evident (hash-chained) audit logs, fraud scoring, access logging, staff confidentiality obligations and vendor due diligence. If a personal data breach is likely to pose a risk to your rights and freedoms we notify the PDPC within 72 hours of becoming

aware, and notify affected individuals without delay where the risk is high. No system is perfectly secure; please protect your credentials and notify us of suspected compromise.

Specific technical and organisational measures include AES-256-GCM field-level encryption (with key versioning) of ID numbers, tax documents, provider credentials and KYC phone numbers; mandatory TOTP two-factor authentication for our staff and for enterprise owners and finance users; four-eyes approval for refunds above THB 1,000, manual credit adjustments, provider configuration changes, lifting of number suspensions and cross-tenant exports; redaction of phone and ID numbers in logs; tenant isolation by row-level security; recordings encrypted at rest in S3-compatible storage with lifecycle rules; and daily full PostgreSQL backups with offsite WAL archiving and regular restore drills. Login location and new-device alerts help you detect unauthorised access.

10. Automated processing

Fraud scoring (allow / review / block) is partly automated; blocked or suspended accounts can request human review by contacting support. Our AI voice assistant generates speech and responses automatically; it always identifies itself as an AI.

Quality scoring of calls (by language-model rubric and rules) is used to improve and monitor the service and is reviewed by people; it is not used to make decisions with legal effect on the call recipient. Caller speech is treated as untrusted data by the AI. Fraud scores and content flags may lead to review, throttling or suspension of an account; you may ask for human review of such a decision.

11. Your rights

Under PDPA ss.30–36 you have the right to: (1) access and obtain a copy of your personal data and information on its sources and disclosures; (2) data portability in a readable format where applicable; (3) object to collection, use or disclosure; (4) request erasure or anonymisation; (5) request restriction of use; (6) rectify inaccurate or incomplete data; (7) withdraw consent at any time as easily as it was given; and (8) complain to the PDPC.

To exercise a right use the in-app data export/delete function, or email [dpo@example.co.th]. We may need to verify your identity. We respond within 30 days of receipt of a valid request. We may refuse or limit a request as the law permits (for example where retention is required by law or to defend legal claims) and will explain why. Exercising rights is free unless requests are manifestly unfounded or excessive.

12. Children

The Services are intended for persons aged 20 or over (or minors who have the consent of their parent or legal guardian where the law requires it). We do not knowingly collect personal data from minors without the required consent of the person exercising parental authority. If you believe a minor has provided data, contact [dpo@example.co.th] and we will delete it unless law requires otherwise. Business customers must not use the Services to call or profile children for marketing.

13. Links and third parties

The Services may link to third-party sites (including LINE). Their privacy practices are governed by their own policies.

14. Cookies

We use strictly necessary cookies (sv_session, csrf, locale) and, only with your consent, optional analytics cookies. See our Cookie Notice for details and to change your choices.

15. Complaints

If you believe we violated the PDPA, please contact the DPO first at [dpo@example.co.th]. You may also lodge a complaint with the Personal Data Protection Committee Office (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, PDPC) or seek remedies through the competent courts.

16. Changes to this Policy

We may update this Policy. For material changes we will notify you by email, in-app notice or LINE at least 30 days before they take effect where practicable, and obtain fresh consent where the law requires. The version number, effective date and content hash of each accepted version are recorded. Previous versions are available on request.

17. Language and governing law

This Policy is governed by the laws of Thailand. This English version is a translation; **the Thai version governs in case of any discrepancy.** (如有歧义以泰文版为准.)

18. Contact

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