

Privacy Notice

How VoxTelAI handles personal data as a controller: what it collects and why, how long it keeps it, who it discloses to, where data goes, and the rights individuals can exercise.

EDITION	EFFECTIVE	SUPPLIER	FORMATS
VTA-PN-2026.08	2026-08-01	VoxTelAI, LLC, a Delaware limited liability company	HTML · PDF · plain text

P1. Who we are, and how to reach us

P1.1 VoxTelAI, LLC is a Delaware limited liability company. We sell business communications services — telephone numbers, SIP trunking, voice termination, outbound calling tools, a hosted Cloud PBX, AI voice agents, recording and transcription, and business SMS — through the Platform: `rolycall.ai`, `portal.rolycall.com` and other `*.rolycall.com` hosts, `trunkmint.com` and `*.trunkmint.com` hosts, and `voice-tele.com` and `*.voice-tele.com` hosts. Whichever domain you use, VoxTelAI, LLC supplies the service and handles your data; this notice covers them all.

P1.2 Contact. Privacy questions and rights requests: **legal@rolycall.com**, by post to the address above marked "Privacy", or by telephone. Security incidents and abuse, around the clock: **abuse@rolycall.com**. A named individual accountable for our data protection compliance is reachable at `legal@rolycall.com`; we are not required to appoint a data protection officer, and will publish any appointment here.

P1.3 Representatives. **We have not appointed a representative in the European Economic Area or the United Kingdom under Article 27 of the GDPR or the UK GDPR**, nor in any other country. If we appoint one we will publish its details here; until then, address anything you would send to a representative to `legal@rolycall.com`. Annex 1 (DPA15) and Module EU/UK (EU4) point here for our representative status.

P2. What this notice covers, and what it does not

P2.1 We handle personal data in two roles. This notice covers one of them.

Data	Who decides how it is used	Governed by
Call content and everything generated from it — recordings, transcripts and other AI Output, prompts and knowledge sources, PBX and voicemail records, contact lists, consent records, message bodies	Our business customer , as controller; we act on its instructions as processor	Annex 1, the Data Processing Addendum at <code>rolycall.ai/dpa</code> — not this notice
Everything in the table at P3: call detail records and message delivery metadata, account, billing and fraud-prevention data, Number registration data, the website, sales, support and recruitment data we collect — and, only where the law of a Destination requires us to keep one for traceback or abuse handling, a copy of a message body for our record-keeping period, then deleted	We do , as independent controller	This notice

P2.2 The roles table in Annex 1 (DPA2) is the authoritative allocation; we do not restate it.

P2.3 *Processor-side retention is the customer's to set.* Recordings, transcripts and other AI Output, voicemail and message bodies are kept for the periods our customer configures in the Portal; the defaults are shown there; only our customer can change them. Recordings and the outputs derived from them are separate categories: deleting one does not delete the other. Deletion takes effect on active systems immediately and works through backups within the period in Annex 1 (DPA12). We may preserve an item longer where a legal hold, lawful process or a legal claim notified or reasonably anticipated requires it, segregated and used only for that purpose. **The periods in the table at P3 are the ones we set as controller, for our own obligations, and no customer configuration changes them.**

P2.4 *If your call was recorded, transcribed or answered by an AI agent,* our business customer controls whether the default recording and transcription remain enabled, and controls any AI agent use and content — ask them. If you write to us we will point you to them where we lawfully can and forward your request.

P3. What we collect as controller, why, and for how long

Category and fields	Source	Purpose	Basis (GDPR Article 6)	Retention
Website visitors — IP address, browser, device, operating system, referring URL, pages viewed and request times, from server access logs	Your browser	Serve and secure the sites, investigate abuse	6(1)(f): sites that work and are not attacked	12 months. Cookies: P5
Lead-form and sales enquiries on any Platform site — name, business email, company, telephone, country, product asked about, your message	You	Answer you, qualify the enquiry, send what you asked for	6(1)(b) where you are or would be our customer, otherwise 6(1)(f) answering a business enquiry; 6(1)(a) consent for marketing email where the ePrivacy Rules require it	24 months from last contact, unless you become a customer or ask us to erase sooner
Portal account holders — name, business email, telephone, job title, username, hashed password, MFA factor, roles, login IP and user-agent, Portal activity, acceptance records, jurisdiction answers, recording and announcement settings	You, or the customer that created your account	Authenticate you, apply permissions, keep an audit trail, prove what was agreed	6(1)(f) administering our contract with your employer, security and audit; 6(1)(b) where you are our customer; 6(1)(c) where law requires the record	Term plus 24 months; acceptance records 6 years after the account closes

Category and fields	Source	Purpose	Basis (GDPR Article 6)	Retention
Billing and payment contacts — name, billing email and address, telephone, invoices, payment-method token and last four digits, refund bank details, tax identifiers	You, or the customer	Take payment, invoice, collect debt, keep tax records	6(1)(f) administering and collecting on our contract with your employer; 6(1)(b) where you are our customer; 6(1)(c) tax and accounting law	As long as tax, accounting and limitation law requires — at least 24 months, not beyond 7 years unless a live investigation, claim or legal hold requires it
Verification, fraud prevention and sanctions screening — identity or incorporation documents, addresses, beneficial owners, intended use, screening matches; authentication and IP logs, traffic-anomaly records, blocked Destinations, fraud case notes, traceback evidence	You; identity, fraud and sanctions-screening providers; the Platform; carriers	Verify who we contract with, meet sanctions and financial-crime duties, stop fraud, protect the network	6(1)(c) legal obligation; 6(1)(f) fraud prevention and network security	24 months, extended to the period sanctions, financial-crime or tax law requires, not beyond 7 years unless a live investigation, claim or legal hold requires it
Support and abuse correspondence — tickets, emails, notes of calls with our staff, diagnostics, complaints, traceback and enforcement correspondence, sender and campaign registration records	You; carriers, registries, regulators, traceback bodies, complainants	Answer support requests, investigate abuse, meet traceback obligations	6(1)(f) answering and evidencing support requests, investigating abuse, meeting traceback obligations; 6(1)(c) where a response is required by law	24 months from closure; traceback, abuse and registration records at least 24 months, then deleted unless a claim or legal hold is live

Category and fields	Source	Purpose	Basis (GDPR Article 6)	Retention
Number registration data — the name, or registered name and company number, of the person a Number is registered for under a customer's registration profile; service address; proof of identity and address; tax identifier	Our customer , under its registration profiles	Submit, re-verify and produce the record to the numbering authority, underlying carrier or regulator — a duty on us as holder of the Number	6(1)(c) legal obligation	As long as the numbering authority requires, and at least 24 months after the Number is released; then deleted unless a live investigation, claim or legal hold requires otherwise
Call detail records and signalling — calling and called numbers, CLI, date, time, duration, disposition, route, SIP response codes, message delivery metadata, rating	Our network	Convey the call or message, bill, prevent fraud, protect the network, answer traceback, comply with lawful process	6(1)(b) and (f) conveyance and billing; 6(1)(f) fraud, security, record-keeping; 6(1)(c) lawful process	At least 24 months under the record-keeping obligation in General Terms section 10, then deleted — unless numbering, tax or sanctions law, a live investigation or a legal hold requires longer, and never beyond 7 years without one of those reasons
Job applicants — CV, contact details, work history, right-to-work information, interview notes, references	You; recruiters; public profiles	Assess your application	6(1)(b) steps before a contract at your request; 6(1)(f) a record of the decision; 6(1)(c) right-to-work checks where law requires them	12 months after the decision, unless you agree we may keep it

P3.1 *Where data is required, and what happens if you do not give it.* Identity, address, beneficial-ownership and sanctions-screening data is required by law and by our contract; we cannot open or keep an account without it. Number registration data is required by the numbering authority of the Number's country; without it the Number cannot be assigned and will be withdrawn. Billing contact data is required to perform the contract; right-to-work information by law where we recruit. The lead form is voluntary, though we cannot answer without a reply address.

P3.2 *How we find customers.* We market to businesses, not consumers. Where we obtain a business contact's details from a source other than that person, we tell them the source at first contact (P3.3) and honour every objection; if you believe we hold your details and cannot see why, write to legal@rolycall.com and we will tell you the source and delete them if you ask. What our customers do with their own calling lists is governed by the law of each Destination and by Schedule D, not by this notice.

P3.3 *Where your data did not come from you.* This page is our notice under Article 14. For a business customer's Number registration record we rely on that customer to give this notice when it collects the documents — its obligation under Annex 1 — and we keep this page available and answer requests directly. For call detail records of callers and called parties we rely on Article 14(5)(b): we hold no contact details for those individuals and contacting them would be impossible or disproportionate. For applicants, prospects and screening data we give or confirm this notice within one month of obtaining the data or, where we contact you, at first contact.

P3.4 We build no advertising profiles, and never use data we process for a customer for our own marketing.

P4. Special-category data, and automated decisions

P4.1 *Special-category data.* As controller we do not seek Article 9 special-category data, and no Service requires it. Sanctions and financial-crime screening matches names against sanctions, politically-exposed-person and adverse-media lists, which can involve suspected offences within Article 10; law requires it, and a match does not of itself affect an account (P4.2).

P4.2 *Automated decisions.* Our fraud and network-protection controls block or rate-limit traffic, Destinations, Numbers, trunks and endpoints automatically and apply spend limits without prior notice. Those decisions are about traffic, not about you as an individual; we tell the affected account holder as General Terms section 9 provides and restore once the cause is remedied. Verification and sanctions screening can affect whether we open or keep an account. Where law gives you a right not to be subject to a decision based solely on automated processing, we respect it: you may ask for human review of the result and the reasoning, and contest the outcome at legal@rolycall.com.

P5. Cookies and similar technologies

P5.1 *One position for every host.* This section states the cookie position for every Platform host listed in P1.1; none has a separate cookie regime or controller. A host that shows no cookie banner sets **strictly necessary cookies only**: a session cookie that keeps you signed in to the Portal or another application host and, where the host is fronted by the access network in P9.1, an access or security cookie that screens requests. EEA, UK and Swiss law does not require consent for those.

P5.2 *Anything else asks first.* Where a Platform host uses an analytics, preference or advertising cookie or a comparable technology, that host asks for your consent before setting it and shows a settings panel, reopenable at any time, listing each cookie, its provider, purpose and lifetime; a change of that kind is a change to this notice under P14. We disclose no website data from any Platform host for cross-context behavioural advertising, and honour the global privacy control signal where law gives it effect.

P6. Call detail records and network records

P6.1 Our network records who called or messaged whom, when, for how long, over which route, how the call ended, whether the message was delivered and what it cost. We generate, rate, retain and disclose those records for our own obligations, not on a customer's instructions; no customer instruction can stop us generating them or make us delete them. Message bodies themselves are our customer's data (P2.1).

P6.2 *How we use them.* We do not use who you called, when or for how long to market to you, and disclose that information only as this notice describes, as the customer authorises, or as lawful process requires. Where a country's telecommunications rules place further duties on network information we hold, we comply to the extent they bind us; the United States rules are addressed in Module US.

P6.3 *No emergency-services data.* None of the Services carries calls to any Emergency Number. We hold no registered address or other emergency location data for any Service, and send no personal data to any emergency authority.

P7. AI features: speech, text, and what we do not do with them

P7.1 *What happens.* Where our customer uses them, the AI features turn call audio into text, generate synthesised speech, and send text and call context to large language models that produce answers, summaries, translations, extractions and scores. Recording and transcription are **enabled by default** and shown with the call detail records; our customer can disable or scope them — per tenant, extension, queue, Number, campaign or AI Agent flow — and decides retention and access. A recording announcement, and a disclosure prompt that says an AI system is speaking, are features our customer enables; it owes any notice, disclosure and consent the law of a connected jurisdiction requires, and we may require either for a campaign, Destination or tenant where a regulator, carrier, the law or a complaint pattern calls for it.

P7.2 *Where the processing happens.* Speech recognition for stored recordings is performed on our own hardware in Germany. Live AI-agent conversations, speech synthesis, and language-model inference are performed by third-party providers in the European Union and the United States, per feature, as the Sub-processor list records (P8.3). For those live/inference features, call audio and/or text leave our own servers for that processing; each provider is bound by contract to use the data only to perform the service for us, keep it no longer than that requires, and not train on it (P7.4). Stored audio, transcripts and AI Output sit on our own Platform in Germany (P9.1).

P7.3 *Output is generated, and can be wrong.* These are probabilistic models: transcripts mis-hear, summaries drop or invent detail, scores are estimates. AI Output is not a verbatim record or professional advice. Every AI voice agent in production must offer a working route to a human being.

P7.4 *We do not train on this data.* We do not use call content, recordings, transcripts or other AI Output, prompts, contact data or message content to train, fine-tune or develop any machine-learning model, ours or anyone else's, including internal-only models. Every AI model provider we use is under the same prohibition by contract, and we enable their no-training and zero-retention settings where offered. We do not try to re-identify anyone from this material except to perform the Services or investigate abuse.

P8. Who we disclose personal data to

P8.1 *Providers who act for us.* Speech recognition and synthesis; language-model inference, for the AI features and the in-Portal assistant; the content-delivery and access network that fronts our sites; and our support, monitoring and business tooling. **The Platform itself runs on hardware we operate** (P9.1); the data centre that houses it has no access to your data. Each provider is engaged under a written contract, may use the data only to perform its service for us, and is bound by the no-training commitment in P7.4; we name any of them on request.

P8.2 *Providers who act for themselves.* Our payment processors and our identity, fraud and sanctions-screening providers generally act as **independent controllers** under their own terms, for their own payment, compliance and fraud-prevention purposes; where one acts for us instead, P8.1 applies. We do

not control what they do for their own purposes and do not represent that they are bound by P7.4; we disclose only what verification, payment and fraud prevention require, and their own privacy notices govern what they do next.

P8.3 Sub-processor list. For data we process on a customer's instructions, Annex 1 (DPA6) governs the Sub-processors, what each receives, its region, transfer mechanism and no-training position. The categories are public (P8.1); **the named list is confidential, provided to our customers on request** at legal@rolycall.com within 5 Business Days.

P8.4 Carriers, numbering authorities and registries. We pass calling and called numbers, CLI, signalling and the media of the call or message to the carriers that convey it — they are not our processors and carry it under their own legal obligations (Annex 1, DPA11); registration and porting data to numbering authorities and the underlying, losing or gaining carrier to provision or port a Number; and, for messaging, sender, campaign and contact-person details to the registries, aggregators and carriers of the Destination, which handle them on their own terms.

P8.5 Regulators, courts and law enforcement, on lawful process, and industry traceback. We notify the affected customer first where lawfully permitted, disclose only the minimum, and challenge an unlawful request.

P8.6 No sale. We do not sell personal data or disclose it for targeted advertising, and no money or other value passes for it in either direction. P12 states the position for residents of certain United States states.

P8.7 Professional advisers — auditors and lawyers — under a duty of confidence; and, *in a corporate transaction*, the other party under confidentiality, with the data transferring with the business and this notice applying until a successor is notified to you.

P9. International transfers

P9.1 Where we are and where the data sits. VoxTelAI, LLC is established in the United States. The Platform, and the recordings, transcripts, account data and records it holds, are hosted on hardware we operate in **Germany** (Falkenstein, Saxony). The Portal and `rolycall.ai` are fronted by a global content-delivery and access network with points of presence worldwide. AI processing happens in the European Union and the United States (P7.2). Calls and messages are carried by the carriers serving the origin and Destination of each one, wherever those are. If you are in the EEA, the UK or Switzerland, some of your data leaves your country.

P9.2 When you give us data yourself. Where you give us data directly from the EEA, the UK or Switzerland there is no transfer mechanism to apply between you and us: you are not a data exporter and cannot sign transfer clauses. Where the GDPR or UK GDPR applies to us as controller, this notice is your notice, and **we have no Article 27 representative (P1.3)** — write to legal@rolycall.com. The clauses below govern data we receive from a business customer and data we pass to our providers.

P9.3 Data we receive from a business customer. For the data we hold as independent controller — Number registration data and account, billing, verification and screening data — the customer sending it to us is the exporter; Annex 1 (DPA11) incorporates the controller-to-controller module of the EU SCCs for those transfers, with the UK Addendum for UK data and the Swiss adaptations for Swiss data. Transfers of data we process **on a customer's instructions** are governed by the same Annex.

P9.4 Data we pass to our providers. Where a provider receives data subject to EEA, UK or Swiss law we rely on an adequacy decision where one covers it, and otherwise on the EU SCCs with the UK Addendum for UK data and the Swiss adaptations for Swiss data, with the supplementary measures identified in our

transfer assessments — including our commitment to challenge unlawful government access requests, disclose only the minimum a request permits, and notify the customer or individual where not prohibited.

P9.5 Carriage of your call. We hand a call's or message's signalling and media to the carriers serving its origin and Destination (P8.4). That hand-off is made under the transfer mechanism the carrier has put in place or, where none is available, on the basis Data Protection Law provides for the carriage of that communication (Annex 1, DPA11); it does not rest on a contract with the called or messaged party.

P9.6 Transatlantic framework. **We are not certified under the EU–US Data Privacy Framework**, and none of our transfers relies on it; the mechanisms above are our operative ones. If we certify, we will say so on this page.

P9.7 Copies. The clauses we use, with commercial terms redacted, and a summary of our transfer assessment are available from legal@rolycall.com.

P10. Security, and what we do when something goes wrong

P10.1 We encrypt data in transit and at rest, restrict access on a least-privilege, logged and MFA-protected basis, bind our people to a duty of confidence and train them, and test our security, each as Annex 1 (DPA5) describes, which is the authoritative statement of our measures. **We claim no certification we do not hold:** unless a report or certification is identified in the Portal (Annex 1, DPA10), we hold none.

P10.2 Breach. If personal data we hold as controller is breached we investigate and contain it without undue delay. Where the GDPR or UK GDPR applies and the breach is likely to be a risk to people, we notify the supervisory authority within 72 hours of becoming aware of it, where feasible, and affected individuals where the risk is high; we also make any notification the law of your state or country requires. A breach affecting data we process for a customer is notified to that customer without undue delay under Annex 1 (DPA9), and it notifies the individuals. Report incidents to abuse@rolycall.com.

P11. Your rights under the GDPR and UK GDPR

P11.1 Where the GDPR, UK GDPR or Swiss law applies to us as controller you may **access** your data and get a copy, **rectify** or **erase** it, **restrict** processing, take it elsewhere (**portability**) where we process it automatically on consent or contract, **object** to processing based on legitimate interests and at any time to direct marketing, and **withdraw consent** without affecting what we did before. If your identity or address documents were registered against a Number under a customer's registration profile, **we hold that record as controller and you may exercise these rights with us directly**. Where we rely on legitimate interests we have carried out a balancing assessment; ask us for a summary.

P11.2 What we may keep. We decline to erase only where a legal obligation requires retention (numbering registration, sanctions, financial-crime and tax records, telecommunications record-keeping duties), where an overriding legitimate interest we have identified requires it (call detail and traceback records needed to bill, prevent fraud, secure the network and answer tracebacks), or where the data is needed for a legal claim or is under legal hold; we assess each request on its facts, tell you the reason and erase the rest.

P11.3 How to ask, and how we verify. Email legal@rolycall.com with "Privacy request" in the subject, write to the address in P1, or telephone us. We verify against records we already hold — for a Portal account, write from the registered address or authenticate in the Portal — ask only for what we need to match you, and delete anything collected solely for verification once the request is closed.

P11.4 Timing. We respond within one month, extendable by two further months for complex or numerous requests, and tell you inside the first month if we extend. Requests are free unless manifestly unfounded or excessive.

P11.5 Complaints. You may complain to the supervisory authority where you live or work, or where the issue arose: in the UK the ICO (ico.org.uk), in Switzerland the federal data protection commissioner, in the EEA the authority listed for your country at edpb.europa.eu .

P12. Residents of certain United States states

P12.1 Where the consumer-privacy law of a United States state applies to you, you may ask us to confirm whether we process your personal data and to **access** it; to **correct** or **delete** it; to receive a **portable copy**; to **opt out** of its sale, of its disclosure for targeted advertising and of profiling with legal or similarly significant effects; to **limit** the use of sensitive personal data; and to **appeal** a refusal — reply marking it "Appeal" and we answer within the period that law sets, with reasons and how to complain to the authority of your state.

P12.2 The table at P3 is our notice at collection — the categories we collect, their sources, purposes, recipients (P8) and retention. We do not sell personal data or disclose it for targeted advertising and have done neither in the preceding 12 months (P8.6); we record an opt-out request anyway. The sensitive data we hold — government identifiers and identity documents submitted for Number registration, verification and sanctions screening, tax identifiers and log-in credentials — is used only to verify identity, register Numbers, meet financial-crime obligations and secure accounts, never to infer characteristics about you. We do not knowingly sell or share the personal data of anyone under 16 (P13).

P12.3 Ask as P11.3 describes; an authorised agent must show your signed permission. We acknowledge and answer within the periods that law sets, telling you if we need more time and why, and do not charge, refuse service, change price or quality or otherwise penalise you for exercising these rights; we run no financial-incentive programme.

P13. Children, and business use

We sell to businesses, not consumers; you must be 18 to open an account. We do not knowingly process the data of anyone under 16, except as an incidental caller or called party on traffic we carry. If you think we hold a child's data, write to legal@rolycall.com and we will delete it unless law requires otherwise; where a child calls one of our customers, that customer controls the call content.

P14. Changes to this notice

Each version carries an identifier, an effective date and the hash of its canonical text in the footer; superseded versions stay at rolycall.ai/legal/archive/ for 24 months. We give at least **30 days'** **notice** before a material change — one that reduces your rights, adds an unexpected purpose or a category of recipient — by email to registered account contacts, in the Portal, and by publishing the new version with a summary of what changed. Corrections and contact or URL updates take effect on publication.

Version **VTA-PN-2026.08** · effective **2026-08-01** · published at rolycall.ai/privacy · SHA-256 of the canonical text: 9b43fffc7cbf18e60881a4ea4864a97de11f96202e277f8cf394be961615a66 · Superseded versions remain available at rolycall.ai/legal/archive/ for 24 months.

VoxTelAI, LLC, a Delaware limited liability company · EIN 36-5176377 · 1111b South Governors Avenue, Suite 55006, Dover, DE 19904, United States · +1 (302) 342-6155 · legal@rolycall.com