Telagento Trust Packet

Version 1.9 | 2026-08-05

Owner: Ecco Studio Labs LLC

Telagento starts with a secure standard platform and configurable enterprise rails. Whether your priorities are hosting, data location, access, privacy, retention, service providers, integration controls, or evidence, we align the deployment to the needs of your engagement.

Security and data protection

Encryption in transit

Telagento uses HTTPS/TLS for customer-facing traffic and managed-provider API connections. This protects the confidentiality and integrity of data while it moves between a user's browser, Telagento, and selected service providers.

Identity and access management

Dashboard and administrative routes require authentication and apply role-based authorization. Access is limited to the functions assigned to each user. Runtime secrets are stored outside source code.

Organization data isolation

Every Telagento user and data request is evaluated within an organization context. Organization-scoped authorization and database queries apply that context to workspace and record access. Row-level controls add defense in depth on covered tables. Authorized Telagento administrators may access an organization when required to assist the customer.

Application and integration security

Covered Twilio voice and ElevenLabs conversational and post-call callbacks use signature verification so Telagento can check who sent them. Telagento-managed webhook clients covered by this control require HTTPS, reject private network destinations and redirects, pin approved DNS results, and limit response size and duration.

Data lifecycle management and privacy rights

Administrative erasure covers covered conversation, call, transcript, and widget records in active Telagento-operated systems. Configurable retention applies to covered call and transcript data. Covered call records can be exported administratively, and covered conversation transcripts can be exported per conversation. The privacy section below explains what these actions cover and where provider, backup, or connected-system boundaries apply.

Secure software development and vulnerability response

Telagento uses branch-based code review, automated tests, controlled promotion from development through release environments, operational logging, and private vulnerability reporting. These practices reduce release risk and provide a defined path to investigate security concerns.

GDPR and CCPA data rights

For verified GDPR or CCPA requests, Telagento works with the customer that controls the data to export or delete covered records held in Telagento-operated systems.

GDPR access and deletion

For a verified GDPR request, Telagento can export covered call records and individual conversation transcripts, and can delete covered conversation, call, transcript, and widget records from active Telagento-operated systems. Telagento coordinates fulfillment with the customer responsible for the data.

CCPA access and deletion

For a verified California consumer request, Telagento can export covered call records and individual conversation transcripts, and can delete covered conversation, call, transcript, and widget records from active Telagento-operated systems. Telagento coordinates fulfillment with the customer responsible for the data.

Scope of access and deletion

Requests about customer-directed conversation data are coordinated with the customer responsible for that data. Telagento can export covered call records and individual conversation transcripts, and can delete covered conversation, call, transcript, and widget records from active Telagento-operated systems. Deleting Telagento-operated records does not independently delete copies retained by enabled service providers. Derived analytics and aggregate records remain subject to applicable retention and customer terms. Legal retention requirements and normal backup-expiration schedules may delay final removal from every copy. Data written to a customer's connected systems remains under that customer's control, and provider-held copies follow the applicable provider procedure and contract.

Primary application and database location

Primary application and database hosting

Telagento application services and the primary database run on dedicated Linode/Akamai infrastructure in the United States.

Service providers and data locations

A subprocessor is an outside company that may process customer data while helping Telagento deliver a selected service. We publish the providers that may be used and why. Except for the Akamai/Linode row describing Telagento's current primary hosting, geography below describes provider-published defaults or available regional options rather than Telagento's selected configuration. The Akamai/Linode statement is Telagento's description of its current deployment; the linked provider documentation identifies available infrastructure locations but does not independently verify Telagento's selection. The exact provider set and configuration depend on each customer deployment, and customers can review applicable provider and data-processing terms during enterprise onboarding.

Twilio - Telecommunications

Provider documentation: United States region by default. Eligible products can use Ireland or Australia; telecommunications networks may process data elsewhere.

Official source 1: https://www.twilio.com/docs/global-infrastructure
Official source 2: https://www.twilio.com/docs/global-infrastructure/understanding-twilio-regions

ElevenLabs - Conversational voice AI

Provider documentation: Enterprise regional deployments are available in Europe, India, and Singapore. The active region depends on the customer configuration.

Official source 1: https://elevenlabs.io/blog/introducing-european-data-residency
Official source 2: https://elevenlabs.io/blog/introducing-india-data-residency
Official source 3: https://elevenlabs.io/blog/introducing-singapore-data-residency

OpenAI - Speech and model services

Provider documentation: Eligible API projects can select regional storage. Regional processing is documented for eligible configurations in the United States and Europe.

Official source 1: https://developers.openai.com/api/docs/guides/your-data#data-residency-controls

Anthropic - Language-model services

Provider documentation: Global inference is the default. Eligible current models can restrict inference to United States infrastructure; workspace storage is currently United States-based.

Official source 1: https://platform.claude.com/docs/en/manage-claude/data-residency
Official source 2: https://platform.claude.com/docs/en/manage-claude/api-and-data-retention

Google Gemini - Language-model services

Provider documentation: Processing-location commitments depend on the Gemini service selected and the applicable Google terms. Customer-specific location must be confirmed for the active configuration.

Official source 1: https://ai.google.dev/gemini-api/terms
Official source 2: https://cloud.google.com/terms/data-residency

xAI - Language-model services

Provider documentation: The cited API and enterprise pages do not state a default API processing or storage region. Enterprise deployment terms may vary.

Official source 1: https://docs.x.ai/developers/faq/security
Official source 2: https://docs.x.ai/build/enterprise

Linode / Akamai - Cloud infrastructure

Telagento statement: Application services and the primary database are hosted in a Telagento-selected Akamai Cloud data center in the United States.

Official source 1: https://techdocs.akamai.com/cloud-computing/docs/how-to-choose-a-data-center

Google Identity - Identity services

Provider documentation: Google's privacy policy describes servers located around the world and processing outside a user's country.

Official source 1: https://policies.google.com/privacy

Google Workspace - Productivity services

Provider documentation: Eligible Workspace editions can select the United States or Europe for covered data at rest and covered processing; the policy does not cover every Workspace data type.

Official source 1: https://knowledge.workspace.google.com/admin/compliance/data-covered-by-data-regions?hl=en

Resend - Transactional email

Provider documentation: The cited provider list identifies United States-based infrastructure and service providers. Email delivery may involve recipient systems in other locations; the cited page does not state a customer-selectable region.

Official source 1: https://resend.com/legal/subprocessors

Cloudflare Turnstile - Anti-abuse protection

Provider documentation: Cloudflare primarily stores information in the United States and European Economic Area and may transfer or access it globally.

Official source 1: https://www.cloudflare.com/turnstile-privacy-policy/
Official source 2: https://www.cloudflare.com/privacypolicy/

Stripe - Billing and payments

Provider documentation: Global processing. Personal data may be transferred outside its country of origin, including to the United States and India.

Official source 1: https://stripe.com/privacy#6-international-data-transfers

Salesforce - CRM integration

Provider documentation: Multiple deployment regions. Customer data is generally stored in the country assigned to the Salesforce organization when the selected services are available there.

Official source 1: https://www.salesforce.com/platform/public-cloud-infrastructure/

HubSpot - CRM integration

Provider documentation: Accounts are assigned to a hosting location in the United States, European Union, Canada, or Australia. Documented exclusions may involve other regions.

Official source 1: https://knowledge.hubspot.com/account-security/hubspot-cloud-infrastructure-and-data-hosting-frequently-asked-questions

Square - Commerce integration

Provider documentation: Global processing. Service providers may process or store information in the United States, Japan, United Kingdom, European Union, and other countries.

Official source 1: https://squareup.com/us/en/legal/general/privacy

Built around your enterprise requirements

Bring us your requirements. Telagento is built to adapt: we translate customer-specific security, privacy, hosting, integration, and assurance needs into agreed controls, architecture, configuration, evidence, and a delivery plan.

When requirements extend beyond the standard environment, Telagento can design and support a dedicated customer deployment or an approved customer-specific partner-hosted deployment. NearLinx infrastructure is available as a partner-hosted option. The selected services, data location, applicable assurance evidence, and responsibilities are documented for the agreed customer deployment boundary.

Security, privacy, and deployment capabilities are reviewed and improved as customer requirements and the platform evolve.

Telagento works directly with customer security, legal, procurement, and infrastructure teams to turn questionnaires, control requirements, architecture and data-flow needs, hosting and location requirements, provider selection, evidence requests, and contractual controls into an agreed deployment plan.

Contact

Privacy: privacy@telagento.com
Private security reports: legal@telagento.com