



DATA HANDLING & SECURITY OVERVIEW

How Nexor protects your data.

Prepared for **customer & vendor security review**



The short version.

Nexor AI Inc ("Nexor") provides an AI platform for customer-facing agents: conversational lead engagement, qualification, and scheduling across email, web, WhatsApp, SMS, and voice channels. This overview describes how Nexor receives, hosts, and protects the data it processes on behalf of its customers, and the state of its compliance program. It applies to any customer engagement; capabilities provisioned per engagement rather than already in production are labeled as such.

Hosting	AWS · US East (N. Virginia) · dedicated account
Encryption in transit	TLS 1.2+ on all connections
Encryption at rest	AES-256 across all data stores
Tenant isolation	row-level security · per-customer scope
Compliance platform	Vanta · trust management
Framework alignment	SOC 2 TSC · ISO 27001 Annex A
ISO/IEC 27001:2022	audit engagement opens Nov 12, 2026
Platform recovery objectives	RTO 4h · RPO 1h

Nexor's security posture can be reviewed at its Vanta Trust Center:
app.vanta.com/getnexor.ai/trust.

How data reaches Nexor and returns.

Inbound (customer → Nexor)

- REST API. Authenticated single and bulk lead creation and archival. Email-first by design: a lead can be created from an email address alone; every other field is optional.
- CRM integration. Native connector framework with bidirectional sync in production for HubSpot; Zoho, GoHighLevel, Kommo, and Pipedrive connectors live. Additional CRM syncs delivered per engagement on the same framework.
- Batch file import. CSV/spreadsheet cohort loads; the recommended pilot path (no CRM credentials, isolated tenant).
- Webhooks. Real-time lead create/update events from the customer's systems.

Knowledge material (PDFs, approved URLs) is ingested separately into a customer-scoped knowledge base; agents answer only from approved material. A managed SFTP endpoint (AWS

Transfer Family delivering into encrypted S3) is available per engagement.

Cadence

Real-time webhooks, scheduled sync jobs, and one-time batch imports all run in production; the pattern is chosen per customer.

Return flow (Nexor → customer CRM)

Engagement and status changes, full conversation transcripts as notes, call and meeting records, extracted data points, and outcomes, all mapped to the customer's field mapping. The customer's CRM remains the system of record.

STORAGE & ISOLATION

Storage, isolation & access.

- **Hosting.** All compute and storage on AWS (US East, N. Virginia): containerized services on ECS, object storage on S3, managed PostgreSQL primary database. US data residency today; other regions per engagement.
- **Tenant isolation.** Every record is scoped to a customer identifier and enforced with database row-level security, in the application and in the database layer. Pilots can run in a dedicated isolated environment.
- **No cross-customer training.** Customer data is never used to train or tune agents for other customers. LLM inference runs against OpenAI and Anthropic APIs under terms that exclude training on API data.
- **Encryption.** TLS 1.2+ enforced on all endpoints in transit; AES-256 at rest (S3 with versioning and full public-access block; managed database encryption). Secrets live in AWS Secrets Manager behind IAM and are never committed to code.
- **Access control.** Least-privilege IAM with per-service task roles; human production access limited to designated engineers with MFA, reviewed quarterly, revoked same-day on departure.
- **Monitoring.** Centralized logging in CloudWatch; all administrative and API-level activity in the cloud account recorded through AWS CloudTrail (multi-region, with log-file integrity validation); 90-day load-balancer access logs; and distributed tracing with automatic redaction of secrets and sensitive content on export.

PII

Personally identifiable information.

Nexor treats as PII any information that can distinguish or trace an individual's identity or is linkable to one, consistent with NIST SP 800-122. On the platform this is primarily information about a customer's leads and contacts, processed on behalf of and at the direction of the customer.

CATEGORY	EXAMPLES ON THE PLATFORM
Contact & identity data	Email address (the only required field); optionally name, phone, channel identifiers
Conversation content	Messages, voice-call content, and information a lead shares during outreach
Engagement data	Funnel/qualification status, scheduling details, fields synced with the customer's CRM

Safeguards

- Minimization by default. The platform operates fully on email-only records; every additional field is optional, and the customer decides which fields cross into Nexor.
- No sensitive documents. Nexor does not request government IDs, financial account data, or credentials, and agents never receive, store, or access sensitive documentation (e.g. KYC or verification files). Integrations pass only coarse status flags the customer chooses to send.
- Configuration-driven capture. The data points an agent extracts and persists from conversations are defined by customer configuration: qualification conditions and field mappings.
- PII in model prompts. Only the minimized field set enters LLM prompts, scoped to the single lead being processed, with no cross-lead or cross-tenant context. Inference providers are contractually barred from training on the data.
- PII in telemetry. Traces and logs exported for observability pass automatic redaction of secrets and sensitive content (authorization material, tokens, voice content) before leaving the platform.
- Highest classification. Under the Data Management Policy, customer PII is classified Confidential: mandatory encryption, need-to-know access, encrypted backups, and no use outside production.
- No secondary use. Lead PII is processed to deliver the contracted service; it is not sold, and shared only with the subprocessors required to operate the platform, each bound by data-protection obligations.
- Individual rights. Live mechanisms include unsubscribe links, a delivery suppression list, per-channel opt-out with reconciliation, and per-record export, archive, or hard delete on request. Each writes its status back to the customer CRM, and together they support customer obligations under GDPR and CCPA access, deletion, and objection requests.

A Data Processing Agreement covering these commitments is available for execution.

Retention & deletion.

All customer data remains contractually the customer's. Retention windows are agreed per customer and per data class (e.g. two weeks, one month) and enforced through the platform's scheduled cleanup mechanism, configured per engagement.

- Archive (soft delete). Removes the lead from all processing and cancels every scheduled job and outreach; reversible.
- Permanent delete. Irreversible, gated behind a dedicated permission scope; every deletion writes a row to a dedicated audit table.
- Deletion on termination. Customer accounts and associated data are deleted within 30 days of contract termination.
- Backups. Encrypted, age out on a documented schedule, restored only for disaster recovery and never used to resurrect deleted records. Restoration has been validated in a live recovery and is exercised on the documented BC/DR testing cycle.
- Export. Full retrieval at any time via CSV report tools, bulk API read, or the continuous CRM sync-back.

Auditability & communications controls.

- Channel scoping. Channels are enabled per customer; email-only engagements are a supported configuration. (Email, WhatsApp, SMS, and voice are all production channels.)
- Complete interaction record. Every message with timestamp and recipient, the workflow rule that triggered it, the full transcript and outcome, escalations with reason, and agent-captured data, all synced to the customer's CRM as the authoritative record.
- Configuration audit trail. Agent instructions and workflows are versioned with rollback; any past conversation can be tied to the exact instructions, knowledge sources, and boundaries in force at that moment.
- Content boundaries. Per-deployment configuration, versioned: *may say* only content grounded in the approved knowledge base; *may not say* a deny-list defined with the customer's compliance team; *must hand off* to a human on regulated topics, complaints, or deletion/opt-out requests.

Compliance program.

Nexor manages its compliance program on Vanta, with the company's cloud infrastructure, source-code management, and identity systems connected for automated configuration checks against the control baseline. The policy framework is documented and mapped to the SOC 2 Trust Services Criteria (Security, Availability, Confidentiality) and ISO/IEC 27001:2022 Annex A, and remediation work is planned and tracked on the platform.

The company operates a documented Information Security Management System (ISMS): scope, roles and authorities, risk assessment and treatment, internal audit, management review, and corrective action. The policy library covers information security, access control, data management, cryptography, secure engineering, incident response, business continuity (RTO 4h / RPO 1h for the platform and customer database), third-party risk, and personnel security. Policies and evidence are available under NDA.

Nexor has committed to ISO/IEC 27001:2022 certification. The independent audit engagement is scheduled to open on November 12, 2026, as confirmed in writing by Vanta (Appendix A). Third-party penetration testing is planned alongside the audit cycle.

Incident response is documented, with severity levels, an Incident Manager role, and escalation paths; customers are notified of a confirmed breach affecting their data within 72 hours.

THIRD
PARTIES

Subprocessors & third-party risk.

Vendors are recorded in a register and tiered by criticality and data access. Critical vendors undergo due-diligence review of their SOC 2 / ISO 27001 attestations and privacy documentation, and are bound by data processing agreements where personal data is involved.

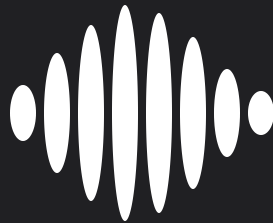
SUBPROCESSOR	FUNCTION
Amazon Web Services	Cloud infrastructure, storage, and hosting
PlanetScale	Managed PostgreSQL database
OpenAI · Anthropic	Large-language-model inference for agents
Twilio	SMS channel (only where SMS is in scope)
Retell AI	Voice-call infrastructure (only where voice is in scope)
Meta	WhatsApp Business messaging (only where WhatsApp is in scope)
SigNoz	Telemetry and tracing (PII-scrubbed)
CRM platforms (per customer)	CRM synchronization at the customer's direction

Supporting vendors include GitHub (source control) and Google Workspace (identity, productivity); neither holds customer data.

Questions & verification.

The practices described in this overview reflect Nexor's documented policies and current production configuration. Posture can be reviewed through the Vanta Trust Center (app.vanta.com/getnexor.ai/trust); questions, questionnaires, or requests for supporting documentation can be directed to Nexor through your account contact or via getnexor.ai.

Nexor AI Inc · Data Handling & Security Overview · NX-SEC-2026-09 Rev A · Restricted. Provided for vendor-assessment purposes. Appendix A follows the closing page.



Security that holds up
in every conversation.

GETNEXOR.AI

Vanta engagement letter.

The following page reproduces the engagement letter issued by Vanta, confirming Nexor's active subscription to continuous control monitoring and the ISO/IEC 27001:2022 audit engagement projected to open on November 12, 2026.

To Whom It May Concern,

This engagement letter confirms that getnexus.ai is an active client of Vanta's trust management platform, certifying the following;

- getnexus.ai has a Vanta subscription that includes continuous control monitoring.
- getnexus.ai has committed to produce an ISO 27001:2022 Report, with the audit engagement projected to start on November 12, 2026.
- getnexus.ai's real-time security posture is visible at <https://app.vanta.com/getnexus.ai/trust/insonjb0fh0zcl68fz0w3f> - this includes continuous control monitoring, security collateral, policies, and achieved compliance frameworks.

If you have further questions, please contact Vanta at support@vanta.com.

Sincerely,

Vanta

