Othello Trust and Compliance

Frequently Asked Questions

Last updated: July 2026

Visit our Trust Center: trust.othello.ai

Welcome to the Othello Trust Center FAQ. This document answers the questions we hear most often from customers, prospective customers, and their IT, security, legal, and procurement teams. It's organized into sections so you can jump straight to what you need. For anything not covered here, reach out to us at trust@othello.ai.

Table of Contents

1. About Othello

Q: What is Othello?

A: Othello is a real-time sales coaching platform that provides in-call guidance directly to sellers during their conversations, along with pre-call preparation, in-call context, and post-call follow-up powered by CRM and calendar integrations.

Q: Who is the legal entity behind Othello?

A: Othello is a product of Cicero, Inc. (“Cicero,” “Othello,” “we,” “us,” or “our”).

Q: Where can I find your latest compliance documentation, certifications, and subprocessor list?

A: The most current versions of our compliance documentation, certifications, and supporting materials are maintained at our Trust Center. A current, complete subprocessor list is maintained there and updated within 30 days of any change. Customers receive advance notice of material subprocessor changes per our Data Processing Agreement (DPA).

Q: Who do we contact with security or compliance questions?

A: You can reach our team directly at trust@othello.ai for security documentation, compliance evidence, or any additional questions.

2. Security & Compliance Program

Q: Does Othello have a formal information security program?

A: Yes. Othello maintains an Information Security Management System (ISMS) governed by an internal Oversight Committee, which is responsible for aligning our security program with ISO/IEC 27001:2022, setting security policy and objectives, allocating resources, monitoring performance, and driving continual improvement. The Oversight Committee meets at least quarterly.

Q: Is there board-level oversight of security and risk?

A: Yes. A Risk and Governance Executive Committee (RGEC), which includes board representation, oversees our overall risk governance structure — including our risk management framework, cybersecurity risk, and business continuity and disaster recovery planning. The RGEC meets at least twice a year and has the authority to investigate any matter and retain independent consultants as needed.

Q: Does Othello conduct regular risk assessments?

A: Yes. Management and our CISO perform a formal, company-wide risk assessment at least annually, or whenever significant changes occur. This includes identifying assets, threats, and vulnerabilities, and assessing the likelihood and impact of each. Identified risks and mitigation strategies are logged in a risk register and tracked through to resolution, with residual risk approved by leadership.

Q: What compliance frameworks and certifications does Othello pursue?

A: Our security and compliance program is built around ISO/IEC 27001:2022, and our risk treatment activities are explicitly mapped to ISO 27001 Annex A controls. We also maintain a completed CSA CAIQ (Consensus Assessments Initiative Questionnaire v4), available upon request, to support vendor security reviews.

Q: Has Othello undergone third-party security testing?

A: Yes. We undergo regular third-party penetration testing and maintain an ongoing cadence of security audits and vulnerability assessments as part of our security program.

Q: Can I get a copy of your completed CAIQ or other compliance evidence?

A: Yes — contact your account team or trust@othello.ai and we'll provide the relevant compliance package for your review.

3. Data Privacy & Data Protection

Q: What types of customer data does Othello collect?

A: We collect user account information (name, email, organization), meeting data (transcripts, notes, action items), CRM data (contacts, accounts, opportunities), and usage analytics. The specific data collected depends on which features and integrations a customer enables.

Q: Does Othello record and store meeting audio, video, or transcripts?

A: Yes. By default, Othello records calls and generates transcripts, notes, and related meeting data in order to power its real-time coaching, pre-call preparation, and post-call follow-up features, and this data is stored in accordance with our standard retention policy described below. Customers with more specific data-minimization requirements can work with their account team to configure a shorter, custom time-to-live (TTL) for stored meeting data — TTL configuration is optional and available on request.

Q: What is the legal basis for processing customer data?

A: We process customer data based on the contractual relationship with the customer (performance of a contract), and rely on explicit consent where required. We act as a data processor on behalf of our customers, who act as the data controller for their own data.

Q: Does Othello offer a Data Processing Agreement (DPA)?

A: Yes. We offer a DPA to all customers outlining data-processing obligations, sub-processor disclosures, data-breach notification commitments, and data-subject rights procedures. It's available upon request and can be executed as part of your customer agreement.

Q: Is Othello GDPR compliant?

A: Yes. Our platform is designed around GDPR requirements, including data-minimization principles, mechanisms to support data-subject rights, records of processing activities, and a documented lawful basis for all processing.

Q: Is Othello CCPA compliant?

A: Yes. We comply with the California Consumer Privacy Act. Customers can exercise their rights to know, delete, and opt out of the sale of personal information. Othello does not sell personal information.

Q: Where is customer data stored geographically?

A: Customer data is stored in data centers located in the United States, within a single, specific Google Cloud Platform (GCP) region. Customers requiring data residency in a different jurisdiction should contact us to discuss available options.

Q: Does customer data ever leave that storage region?

A: No. Data is processed and stored within the designated cloud region. It may transit through our cloud provider's global network during encrypted transmission, but it is not stored outside the designated region.

Q: Does Othello support customer-managed encryption keys (CMEK)?

A: Encryption keys are managed by our cloud provider's key management service by default. Customer-managed encryption keys are available upon request for enterprise customers.

Q: What is Othello's data retention policy?

A: Customer data is retained for the duration of the active subscription, plus a defined wind-down period. After account termination, data is deleted within the timeframe specified in your customer agreement — typically 30–90 days. Customers can request earlier deletion at any time.

Q: How do you handle Data Subject Access Requests (DSARs)?

A: We provide mechanisms for our customers (as data controllers) to fulfill DSARs from their own data subjects, including the ability to export, correct, and delete personal data tied to specific individuals.

Q: Does Othello support data portability?

A: Yes. Customers can export their data — including meeting data and contact records — in standard, machine-readable formats.

Q: How does Othello handle special categories of sensitive personal data (e.g., health, biometric, or genetic data)?

A: We maintain a data classification framework covering special categories of personal data under GDPR Article 9 (racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and sexual orientation data). Any processing of this data requires a documented legal basis reviewed by our Data Protection Officer before processing begins, and high-risk processing activities require a formal Data Protection Impact Assessment (DPIA).

Q: How does Othello handle objections to data processing (GDPR Article 21)?

A: Objections to direct marketing are honored immediately and without exception — no justification is required from the data subject. Objections based on legitimate interests are formally assessed, with the assessment and any override justification documented.

Q: How is data securely disposed of when it's no longer needed?

A: Electronic data is deleted using secure deletion methods designed to prevent recovery. Any physical records are shredded or destroyed. Disposal requires authorization, and records of disposal (including method and approval) are retained for audit purposes.

Q: Does Othello use customer data to train AI models?

A: No. Customer data — including call transcripts, CRM records, and metadata — is never used to train, fine-tune, or otherwise improve shared or general-purpose AI models. See Section 8 for more detail on our AI data handling practices.

4. Data Security & Encryption

Q: How is data encrypted at rest?

A: All customer data is encrypted at rest using AES-256 encryption, with keys managed through our cloud provider's key management service, which handles key generation, rotation, and storage in hardware security modules (HSMs).

Q: How is data encrypted in transit?

A: All data in transit is encrypted using TLS 1.2 or higher. We enforce HTTPS for all external connections and do not accept unencrypted HTTP traffic. Internal service-to-service communication also runs over encrypted channels.

Q: How does Othello manage secrets and API keys?

A: Secrets, API keys, and credentials are stored in a dedicated cloud secrets-management service. They are never stored in source code, configuration files, or environment variables at rest — secrets are injected into the runtime environment at deployment time.

Q: Does Othello have a Web Application Firewall (WAF) or DDoS protection?

A: Yes. Our edge layer includes a cloud-native WAF and DDoS mitigation service providing rate limiting, adaptive protection, IP-based access controls, and protection against common web exploits (OWASP Top 10).

Q: Does Othello have network intrusion detection and monitoring?

A: Yes. We use firewalls and intrusion detection systems to separate our network from the public internet and third-party networks, and we continuously monitor traffic for anomalies and potential threats. All administrator access to network and security tooling is logged and reviewed.

5. Cloud Architecture & Infrastructure

Q: Which cloud provider hosts Othello?

A: Othello is hosted on Google Cloud Platform (GCP), using managed compute, networking, database, and storage services.

Q: Is Othello deployed in a single region or multiple regions?

A: Othello currently uses a single-region deployment (a US-based GCP region), with all compute, storage, and database resources co-located to simplify data-residency controls.

Q: What compute platform does Othello run on?

A: Othello runs on a fully managed, serverless compute service that automatically handles scaling, patching, and infrastructure management — there's no manual server maintenance involved.

Q: How does Othello handle traffic spikes and scaling?

A: Our compute layer auto-scales horizontally (adding more instances, not larger ones) based on incoming request volume, with configurable minimum and maximum instance counts.

Q: How is the network architecture designed?

A: Othello runs inside a Virtual Private Cloud (VPC) with private subnets. Public-facing services are reachable only through load balancers at the network edge; internal services, databases, and caches are isolated within the private network and are not directly reachable from the internet.

Q: How is the database secured?

A: Othello's database uses private connectivity only — it is never assigned a public IP address, and all database traffic flows over private network endpoints, never touching the public internet. Our managed database provider holds SOC 2 Type II, ISO 27001, and HIPAA compliance certifications.

Q: Does Othello use Infrastructure-as-Code?

A: Yes. Our infrastructure is defined and managed as code, ensuring consistent, repeatable, auditable deployments, with all changes reviewed and version-controlled.

Q: How are deployments managed?

A: We use immutable, containerized deployments — containers are built once, tested, and promoted through environments without in-place changes to running containers.

Q: Does Othello maintain separate environments for development, staging, and production?

A: Yes, we maintain fully separate staging and production environments.

6. Authentication, SSO & Access Control

Q: How does authentication work in Othello?

A: Othello uses token-based authentication with JSON Web Tokens (JWTs). Every API request must include a valid, signed JWT in the Authorization header; requests without one are rejected before reaching any application logic.

Q: Who issues these tokens, and does Othello store passwords?

A: Tokens are issued by a dedicated, third-party identity provider (Auth0). Othello never stores, processes, or has access to user passwords — all credential management is handled by the external identity provider.

Q: How are tokens validated and secured?

A: Tokens are signed using the RS256 asymmetric algorithm and validated against the identity provider's public key set. A middleware layer checks the signature, expiration, issuer, and audience on every request, before any business logic executes, and there is no mechanism to bypass this for authenticated endpoints.

Q: Does Othello support Single Sign-On (SSO)?

A: Yes. Othello supports enterprise SSO via SAML 2.0 and OpenID Connect (OIDC), letting your employees authenticate through your corporate identity provider (e.g., Okta, Azure AD, Google Workspace, OneLogin, Ping Identity) rather than managing separate credentials. A detailed SSO setup guide is available on request from your account team.

Q: Does Othello support multi-factor authentication (MFA)?

A: MFA is enforced at the identity-provider level. Since authentication is fully delegated to your IdP when SSO is configured, whatever MFA policy you set there (TOTP, hardware keys, push notifications) is respected automatically — your identity administrator controls this centrally.

Q: How are user sessions managed?

A: Sessions are stateless and based on JWT validity — there's no server-side session store, which eliminates risks associated with server-side session hijacking. When a token expires, the client obtains a new one from the identity provider.

Q: How is token revocation handled?

A: Token revocation happens at the identity-provider level. When an administrator disables a user or revokes sessions in the IdP, no new tokens can be issued, and existing tokens expire naturally based on their short-lived expiration claim.

Q: Does Othello support role-based access control (RBAC)?

A: Yes. Roles (e.g., admin, member) are assigned per user by organization administrators and evaluated server-side on every request to determine access. Custom role definitions are on our product roadmap.

7. Multi-Tenancy & Data Isolation

Q: Is Othello multi-tenant?

A: Yes. Othello is a multi-tenant SaaS application — multiple customer organizations share the same infrastructure while maintaining strict logical isolation of data between tenants.

Q: How is tenant isolation enforced?

A: Every data record carries a mandatory tenant identifier, and all database reads and writes are scoped to the authenticated user's tenant. This is enforced systematically through shared infrastructure code (a repository pattern) that injects the tenant filter on every query — not left to individual developer discipline.

Q: Can one customer ever access another customer's data?

A: No. The tenant identifier is derived server-side from the authenticated user's JWT — it is never accepted from request bodies, headers, or query parameters — which prevents tenant-spoofing. Queries without a tenant scope are treated as security defects and caught during code review.

Q: Does Othello use a shared database or a database-per-tenant model?

A: Othello uses a shared database with logical tenant isolation, which provides cost efficiency and consistent schema management while still enforcing the same security guarantees as physical separation.

Q: Can one customer's usage impact performance for others (“noisy neighbor” effects)?

A: Our managed, auto-scaling infrastructure distributes workload across compute instances, so individual tenant workloads do not meaningfully impact other tenants' performance.

Q: What happens to a tenant's data when they leave?

A: When a tenant is deprovisioned, all associated data — database records, stored files, and integration tokens — is identified by the tenant identifier and deleted within the timeframe specified in the customer agreement.

8. AI Model Usage & Data Handling

Q: Does Othello train AI models on customer data?

A: No. Customer data — including call transcripts, CRM records, and metadata — is never used to train, fine-tune, or otherwise improve shared or base AI models. This applies both to any models Othello operates itself and to third-party model providers we use.

Q: How is customer data processed by AI models?

A: AI models process customer data only during real-time inference, triggered by a user action. Data is passed to the model for a single inference call and is not stored by the model provider beyond that call's completion.

Q: How long are AI inputs and outputs retained?

A: Othello retains inference inputs and outputs only as needed to power product features you use — for example, conversation history or call summaries — within our standard data-retention window (see Section 3). Raw prompts and completions are not persisted beyond that window.

Q: Is one customer's data ever mixed into another customer's AI session?

A: No. Each tenant's data is processed with isolated context. There is no prompt chaining, retrieval, or context injection that would cause one tenant's data to appear in another tenant's AI session.

Q: Does Othello take steps to guard against prompt injection or misuse of AI features?

A: Yes. We apply input sanitization and context-handling controls as part of our AI processing pipeline. Full technical detail on these controls is available to customers' security teams on request.

Q: What contractual protections govern our AI infrastructure providers?

A: Where available, we put contractual data-protection and reduced/zero data-retention terms in place with our AI infrastructure providers, consistent with our “no training on customer data” commitment above. For example, Othello maintains a Zero Data Retention (ZDR) agreement with OpenAI, one of our AI infrastructure providers — under this agreement, prompts and completions processed through that integration are not retained by OpenAI beyond what's needed to service the individual request.

9. CRM, Calendar & Third-Party Integrations

Q: Which CRM systems does Othello integrate with?

A: Othello integrates with Salesforce, HubSpot, and Microsoft Dynamics 365. Our integration architecture is provider-agnostic, so additional CRM systems can be added without changes to the core platform.

Q: How does Othello authenticate with CRM systems?

A: All CRM integrations use OAuth 2.0. Each user authorizes access through the CRM vendor's own standard consent screen — Othello never receives or stores CRM passwords. For Salesforce, this is done through an admin-approved External Client App (ECA); for Dynamics, through per-user OAuth authorization following the standard Dynamics integration model.

Q: Where are CRM tokens stored, and how are they refreshed?

A: OAuth tokens are stored in a dedicated, encrypted integration-management layer that handles token lifecycle and automatic refresh. Application logic doesn't have direct access to raw token values.

Q: What CRM data does Othello access, and can we control it?

A: We access the data needed for meeting-intelligence and contact-enrichment features — typically contact records, account information, opportunity data, and related metadata — scoped to the minimum required for functionality. The OAuth consent flow shows exactly which scopes are being granted, and field-level mapping configuration lets you control which specific CRM fields are read from and written to.

Q: Does Othello write data back to our CRM?

A: Yes, but only in a controlled way. Othello can write meeting notes, insights, and enriched contact data back to the CRM; write operations are scoped to specific object types and fields, and you control what gets synchronized.

Q: Is our CRM data isolated from other customers?

A: Yes — the same tenant-scoping guarantees described in Section 7 apply to all synchronized CRM data.

Q: Does Othello support Salesforce sandbox environments?

A: Yes, both production and sandbox Salesforce environments are supported, so you can test integrations before deploying to production.

Q: What happens to CRM data if we disconnect an integration?

A: OAuth tokens are revoked and deleted from our integration-management layer immediately. Previously synchronized CRM data can be deleted on request.

Q: Does the calendar integration give Othello access to our email or files?

A: No. Calendar permissions are scoped strictly to calendar-related access (meeting metadata) — the integration is not designed to grant access to unrelated workspace data such as files, Drive content, chat messages, or general mailbox content. We support Google Calendar and Microsoft Outlook.

Q: Why does Othello request "maintain access" or offline-access permissions during OAuth?

A: This corresponds to the standard OAuth 2.0 offline_access scope, which is requested by virtually every enterprise SaaS application that integrates with services like Microsoft 365 — including Microsoft's own first-party apps. It simply allows Othello to refresh a short-lived access token (typically valid 60–90 minutes) so your session doesn't expire mid-workflow. It does not mean Othello continuously scans, harvests, or processes your data in the background; tokens are only used in response to a user-initiated or explicitly scheduled action.

Q: What's the difference between "delegated" and "app-only" CRM permissions, and which does Othello use?

A: Othello uses delegated permissions, not app-only (application-level) permissions. Delegated access means Othello acts on behalf of a specific signed-in user and can only see what that user could already see in your CRM — it cannot access data the user themselves cannot access. App-only permissions, by contrast, would grant access independent of any user, potentially across your entire tenant. Choosing delegated access is a deliberate least-privilege design decision; your existing CRM role-based access controls remain the controlling boundary for what Othello can see.

Q: Why does Othello use a per-user connection model for integrations instead of one shared account?

A: Per-user OAuth connections give you cleaner, user-level visibility, provisioning, and revocation. You can map every action back to a specific authorized user, onboard and offboard individuals without disrupting the rest of your deployment, and avoid relying on broad, unmanaged, tenant-wide access through a single shared account.

10. Vendor & Subprocessor Management

Q: Does Othello have a formal vendor management program?

A: Yes. We maintain an inventory of critical third-party vendors, apply baseline security requirements, and periodically evaluate vendor performance and risk.

Q: What due diligence do you perform before onboarding a vendor?

A: We conduct a risk assessment before engaging any vendor and repeat it annually, evaluating information security, business continuity, data exposure, and regulatory compliance considerations. Vendor contracts require confidentiality obligations, defined security responsibilities, and immediate breach-notification requirements.

Q: How do you monitor vendors on an ongoing basis?

A: At onboarding and annually thereafter, we review SOC 2 reports (or equivalent) from our service providers and vendors to assess the scope and impact of any identified exceptions.

Q: Where can I find your current subprocessor list?

A: A current, complete subprocessor list is published in our Trust Center and updated within 30 days of any change, with advance notice of material changes provided per our DPA.

11. Personnel Security & Internal Governance

Q: Does Othello conduct background checks on employees?

A: Yes. We conduct background and/or reference checks on all new employees and contractors prior to their start date, in accordance with applicable laws and proportional to the role.

Q: Do employees sign confidentiality agreements?

A: Yes. All personnel sign a confidentiality agreement covering intellectual property, code of business conduct, ethical standards, and information security responsibilities at the time of hire, and formally reaffirm this understanding annually.

Q: Do employees receive security training?

A: Yes. Employees complete information security and awareness training upon hire and at least annually thereafter.

Q: How are security roles and responsibilities defined internally?

A: We maintain a documented organizational chart defining reporting lines and authority for development, quality assurance, and security operations, reviewed and updated as needed. Senior management and security-related roles have specific oversight duties documented in their job descriptions.

12. Incident Response, Risk Management & Business Continuity

Q: Does Othello have a documented incident response process?

A: Yes. We maintain documented and tested procedures for rapid detection, escalation, and remediation of security incidents, backed by continuous monitoring for anomalies and potential threats.

Q: How does Othello identify and treat security risks?

A: Risks are assessed based on likelihood and impact and assigned a treatment strategy — Mitigate, Transfer, Accept, or Avoid — each explicitly mapped to relevant ISO/IEC 27001:2022 Annex A controls. Every risk has a named owner and approver, and residual risk must be approved by leadership before it's accepted.

Q: Who oversees business continuity and disaster recovery planning?

A: Our Risk and Governance Executive Committee evaluates significant risk exposures — including business continuity and disaster recovery planning and testing — and reports findings and mitigation plans to the Board.

13. Contracts, Data Ownership & AI Output Disclaimers

Q: Who owns our data when we use Othello?

A: You do. Your data (referred to in our agreement as “Client Data”) remains yours — meeting recordings, CRM data, transcripts, prompts, and other content you submit. You grant Othello a limited license solely to provide the services to you.

Q: What can't we do with the Othello platform under our license?

A: Standard SaaS restrictions apply: no reverse engineering or attempting to extract source code, model weights, or system prompts; no unauthorized penetration testing, load testing, or scraping without our prior written consent; and no using the service to train a competing product.

Q: Should we treat AI-generated outputs (summaries, coaching prompts, recommendations) as final answers?

A: No — please treat them as assistive, not authoritative. AI-generated outputs may be inaccurate or incomplete and are not a substitute for human judgment, legal advice, financial advice, medical advice, or compliance review. You're responsible for reviewing and approving outputs before relying on or acting on them.

Q: What level of uptime/availability does Othello commit to?

A: We use commercially reasonable efforts to keep the service available, excluding scheduled maintenance, emergency maintenance, beta features, third-party outages, and other disruptions outside our reasonable control. Specific SLA terms, where applicable, are defined in your Order Form.

14. Getting More Information

Q: I have a question that isn't answered here — who do I contact?

A: Reach out to trust@othello.ai. Our team can provide additional documentation, evidence packages, or direct support through your security or procurement review process.

Q: What additional documents can you provide upon request?

A: Depending on your review needs, we can share: our completed CAIQ questionnaire, our Data Processing Agreement (DPA), a detailed SSO/SAML setup guide for your IT team, technical integration documentation for CRM and calendar connections, and our current subprocessor list.

This FAQ is maintained by Othello's Trust & Compliance team.