POL-001 Policy Document

Cognispace, LLC

Privacy Policy

Active Release

POL-001 · Version 1.0

Policy Statement

POL-001 Version 1.0 is hereby designated as the active Privacy Policy for Cognispace, LLC, effective as of the date listed in Document Control.

All future revisions must be versioned and recorded in the revision history. Unless explicitly superseded by a later release, this version governs the collection, use, storage, and disclosure of information in connection with all Cognispace services, platforms, and products.

Document Control

Policy — Legal & Compliance

Document ID:	POL-001
Document Title:	Cognispace Privacy Policy
Document Type:	Policy — Legal & Compliance
Version:	1.0
Effective Date:	March 30, 2026
Last Updated:	March 30, 2026
Author:	Cognispace, LLC
Status:	Active — Initial Release
Replaces:	N/A
Supersedes:	N/A

Revision History

Version	Date	Modified By	Change Description
1.0	2026-03-30	Cognispace, LLC	Initial release. Foundational privacy policy covering scope, data collection, use, sharing, retention, security, user rights, and governance.

Distribution

This document is publicly available and applies to all users, customers, and enterprise clients of Cognispace, LLC services.

Document Classification

Class: POL (Policy) — Legal & Compliance

Privacy Policy

Effective Date: March 30, 2026 · **Last Updated:** March 30, 2026

Cognispace, LLC ("Cognispace," "we," "our," or "us") takes the privacy of the people who use our services seriously. This Privacy Policy describes how we collect, use, store, share, and protect information when you access or use our websites, software applications, APIs, research platforms, enterprise tools, and related offerings (collectively, the "Services").

Our Services are built to support structured analysis, interpretive workflows, and human-centered expression systems. This policy reflects our commitment to responsible data stewardship and transparent processing practices consistent with enterprise-grade trust and security expectations.

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy.

---

1. Scope and Applicability

This Privacy Policy applies to information collected, received, processed, stored, or otherwise handled by Cognispace in connection with the use of our Services.

1.1 What the Services Include

For purposes of this Policy, the "Services" include, without limitation:

- Cognispace websites and public-facing web properties
- Software platforms and applications
- Web-based and mobile interfaces
- APIs, SDKs, and third-party integrations
- Customer, team, and enterprise workspaces
- Uploaded media, documents, text, and other user-submitted content
- Research, analytical, and interpretive tools
- Customer support and communications channels
- Operational logging, performance diagnostics, and security telemetry
- Authentication, account, and subscription systems

1.2 Who This Policy Covers

This Policy applies to both individual users (including customers, researchers, and authorized users) and organizational users (including enterprise customers, institutional clients, and workspace members).

Where you access the Services through an employer, client organization, or enterprise customer, additional contractual terms may govern the relationship—such as a Data Processing Addendum, a Master Services Agreement, or customer-specific security terms. Where such an agreement conflicts with this Policy, the executed agreement controls.

This Policy does not apply to third-party websites, services, or integrations not owned or controlled by Cognispace. Users should review the privacy practices of any third-party services independently.

2. Information We Collect

Cognispace collects information reasonably necessary to operate, secure, improve, and support the Services. What we collect depends on how you interact with the Services—whether as an individual user, an enterprise workspace user, an administrator, or a customer representative. Information may come directly from you, automatically through your use of the Services, or from authorized third-party integrations and enterprise administrators.

2.1 Account and Identity Information

We collect information necessary to create, maintain, authenticate, and secure user accounts and workspace access. This may include:

- Full name, email address, username, or display name
- Company, institution, or organization name; job title or role
- Account credentials, authentication metadata, and security tokens
- Single sign-on (SSO) and identity provider metadata
- Multi-factor authentication settings and verification status
- Billing, invoicing, and subscription information
- Workspace role assignments and access permissions
- Account lifecycle information such as creation date, login history, and session records

For enterprise environments, we may also collect organization identifiers, workspace membership data, administrator-assigned permissions, and role-based access controls.

Where authentication is handled through third-party identity providers, we may receive identity and access metadata from those providers in accordance with their applicable terms.

2.2 User-Provided Content

We collect information and content you voluntarily submit, upload, create, or transmit through the Services. This may include:

- Uploaded audio, text, image, video, and document files
- Transcripts, notes, annotations, and comments
- Workspace materials and project artifacts
- Reports, summaries, and interpretive outputs

- Configuration settings and user preferences
- Prompts, queries, and workflow inputs
- Support communications and feedback submissions

In enterprise environments, this may also include team-generated collaborative content created, edited, or shared by authorized workspace members—which may be visible to workspace owners, designated administrators, and users with role-based access.

Users are responsible for ensuring that content submitted to the Services is lawfully collected, appropriately authorized, and consistent with applicable laws and organizational policies.

2.3 Derived and Analytical Data

As part of delivering the Services, Cognispace may generate or derive additional data from user-submitted content, system interactions, and workflow activity. This derived data is produced through automated, analytical, or system-assisted processing designed to support service functionality.

Derived and analytical data may include:

- Timing metadata, structural sequencing, and temporal patterns
- Acoustic and linguistic features; signal-derived indicators
- Interaction summaries, workflow metrics, and usage trends
- System-generated interpretive artifacts and model-assisted outputs
- Confidence or uncertainty indicators
- Aggregated statistical summaries and de-identified performance data

Such data is generated solely for legitimate business and service-related purposes, including product functionality, workflow continuity, enterprise reporting, quality assurance, and security monitoring.

Derived outputs are descriptive, contextual, and analytical in nature. They are not intended to constitute—and should not be relied upon as—medical determinations, psychological assessments, employment decisions, legal conclusions, identity classifications, or risk scoring for real-world punitive decisions. This limitation reflects our human-centered, non-clinical framework boundaries.

2.4 Technical and Device Information

We automatically collect technical and operational information to support the performance, reliability, and security of the Services. This may include:

- IP address, browser type and version, operating system and device platform
- Network connection metadata, request and response logs, timestamps
- API usage metadata, session identifiers, authentication events
- Performance diagnostics, system health metrics, crash reports, and error logs
- Infrastructure telemetry and security event logs

This information is used to maintain service uptime, diagnose interruptions, investigate incidents, improve application performance, detect unauthorized access, and maintain security controls. It may be combined with account and usage information where reasonably necessary for operational support or security investigations.

2.5 Cookies and Similar Technologies

Cognispace may use cookies, local storage, session storage, pixels, tokens, and similar technologies to support the operation, security, and performance of the Services. These technologies may be placed by Cognispace or by authorized service providers acting on our behalf.

We may use these technologies to maintain authenticated sessions, remember user preferences, enable secure sign-in workflows, improve product performance, analyze service usage, support security monitoring, and detect fraud or unauthorized access.

Cookies may be categorized as essential (required for core functionality), performance and analytics, security, or preference cookies. Some expire at the end of a browser session; others persist for a defined period to support account continuity.

Users may manage or disable certain cookies through browser or device settings. Disabling essential cookies may limit the availability or security of certain features. Where required by applicable law, Cognispace may provide additional consent notices or preference controls.

3. How We Use Information

Cognispace uses collected information solely for legitimate business, operational, security, research, and service-related purposes. We may use information to:

- Provide, operate, and maintain the Services
- Authenticate users and validate access permissions
- Create, administer, and secure user accounts and workspaces
- Process submitted content and generate analytical or interpretive outputs
- Support collaboration and enterprise workflow continuity
- Improve service performance, reliability, and scalability
- Provide customer support, troubleshooting, and service communications
- Manage subscriptions, invoicing, and billing relationships
- Enforce contractual terms, acceptable use requirements, and workspace governance controls
- Comply with legal, regulatory, and contractual obligations
- Detect, prevent, and investigate abuse, fraud, unauthorized access, or misuse
- Conduct internal testing, quality assurance, and service validation
- Develop and improve current and future products and services
- Support internal research, workflow optimization, and responsible innovation

Where reasonably necessary, Cognispace may also use aggregated, anonymized, or de-identified information for internal research, product development, service benchmarking, and operational intelligence. Such processing is designed to remove or materially reduce the ability to identify individual users or organizations.

Cognispace does not use collected information for purposes inconsistent with this Privacy Policy, applicable contractual commitments, or governing law.

4. Interpretive Processing Disclosure

Certain Services may process user-submitted content, workspace materials, or workflow data to generate analytical, structural, or model-assisted outputs. This processing may involve automated, rules-based, statistical, or system-assisted methods designed to support understanding and contextual interpretation of information submitted through the Services.

These outputs are intended solely to support legitimate operational, research, and enterprise workflow purposes—including communication analysis, workflow interpretation, human-centered reflective systems, enterprise intelligence, structured reporting, and operational decision support.

Interpretive outputs may include descriptive summaries, signal-derived observations, structural patterns, contextual insights, uncertainty indicators, and model-assisted recommendations.

Cognispace does not represent or market these outputs as:

- Clinical conclusions or medical assessments
- Psychological diagnoses or behavioral determinations
- Employment, legal, or disciplinary conclusions
- Predictive certainty or identity-defining classifications

Interpretive outputs are contextual, descriptive, probabilistic, and subject to uncertainty. They are designed to support informed human review and should not replace professional judgment, qualified expert review, or authorized organizational decision-making processes.

Users and enterprise customers are responsible for ensuring that qualified human decision-makers evaluate and contextualize interpretive outputs before relying on them for consequential actions. Cognispace expressly discourages the use of interpretive outputs as the sole basis for high-impact decisions involving individuals.

This disclosure is intentionally aligned with Cognispace’s human-centered, interpretive, and non-clinical framework boundaries.

5. How We Share Information

Cognispace does not sell personal information. We do not sell, rent, or trade personal information to third parties for monetary consideration or for unrelated commercial marketing purposes.

Information is shared only as reasonably necessary to operate, secure, support, and improve the Services; comply with legal obligations; or fulfill authorized customer and enterprise workflows.

5.1 Service Providers and Infrastructure Partners

We may share information with trusted third-party service providers and infrastructure partners that support our operations. These may include providers of cloud infrastructure and hosting, storage and content delivery, authentication and identity management, billing and payment processing, customer support systems, security monitoring, communications and notification services, and backup and disaster recovery.

These providers are authorized to access information only to the extent necessary to perform services on our behalf. They are contractually required to process information in accordance with our instructions, maintain appropriate confidentiality protections, implement commercially reasonable security controls, and refrain from using information for their own unrelated purposes.

5.2 Enterprise and Workspace Administrators

If you access the Services through an organization or enterprise-managed workspace, authorized administrators designated by that organization may be able to access, manage, or export information associated with that workspace. This may include account identifiers, user profile and role information, workspace activity, uploaded content, generated outputs, and audit records.

The extent of administrator access depends on the permissions and governance settings established by the relevant organization. If your use of the Services is managed by an enterprise customer, your information may be subject to that organization’s internal privacy, security, monitoring, retention, and acceptable use policies. Cognispace is not responsible for the privacy practices of customer organizations beyond the Services we provide.

5.3 Legal and Regulatory Compliance

We may disclose information when we believe, in good faith, that such disclosure is reasonably necessary to comply with applicable legal, regulatory, or public safety obligations. This includes responding to subpoenas, court orders, or other legal process; cooperating with law enforcement or regulatory authorities; protecting the rights, safety, or property of Cognispace, our users, or the public; investigating fraud or security incidents; and establishing, exercising, or defending legal claims.

Where legally permitted and reasonably appropriate, Cognispace may notify affected users or enterprise customers prior to disclosure. Nothing in this section requires disclosure beyond what applicable law demands.

5.4 Business Transactions

In connection with a merger, acquisition, financing, corporate reorganization, sale of assets, or similar business transaction, information may be transferred or disclosed as part of the due

diligence process or as part of the completed transaction. Any such transfer remains subject to applicable confidentiality, security, and data protection obligations. Where required by law or where reasonably appropriate, Cognispace will provide notice to affected users or enterprise customers.

6. Data Retention

Cognispace retains information only for as long as reasonably necessary to fulfill legitimate business, legal, operational, security, and contractual purposes—including providing and maintaining the Services, complying with legal and regulatory obligations, resolving disputes, supporting security investigations, and maintaining audit trails.

Retention periods may vary depending on account status, subscription plan, workspace settings, administrator controls, enterprise contractual requirements, legal holds, and backup or archival system schedules.

Where enterprise customers control retention settings, Cognispace may retain information in accordance with administrator-configured policies and applicable contractual terms.

Where feasible and commercially reasonable, information that has reached the end of its applicable retention period may be deleted, anonymized, aggregated, de-identified, or archived in restricted-access systems. Certain information may persist for limited periods in backups, audit logs, or legally required archives even after deletion from active systems.

7. Security Safeguards

Cognispace maintains administrative, technical, physical, and organizational safeguards designed to protect information against unauthorized access, disclosure, alteration, misuse, loss, and destruction. These safeguards are implemented in a manner consistent with commercially reasonable enterprise SaaS security practices.

Security measures may include:

- Encryption in transit and at rest
- Access controls, least-privilege permissions, and role-based access controls
- Tenant and workspace isolation
- Identity and authentication controls, session management, and token validation
- Audit logging and access traceability
- Infrastructure monitoring, vulnerability management, and patching procedures
- Security event detection, alerting, and incident response procedures
- Secure backup, recovery, and disaster recovery controls
- Secure software development and deployment controls

Access to systems and data is restricted to authorized personnel, subprocessors, and enterprise administrators with a legitimate operational need. Cognispace maintains processes to support security investigations, threat detection, credential compromise response, service restoration, and incident documentation.

No method of transmission, storage, or electronic processing can be guaranteed to be completely secure. Accordingly, Cognispace cannot warrant or guarantee absolute security.

Users are responsible for maintaining the confidentiality of their credentials, API keys, access tokens, and authentication devices. Please notify Cognispace promptly of any suspected unauthorized account access, credential compromise, workspace misuse, or suspicious activity.

8. Your Privacy Rights and Choices

Depending on your jurisdiction and applicable law, you may have certain rights regarding your personal information. Subject to verification, legal limitations, and operational constraints, these rights may include the right to:

- Access your information or request a copy
- Correct inaccurate or incomplete information
- Request deletion of personal information
- Request export, transfer, or data portability
- Restrict or limit certain processing activities
- Object to certain processing activities
- Withdraw consent where processing is based on consent
- Request information regarding categories of data collected and how it is used

Cognispace will evaluate and respond to verified requests in accordance with applicable law, contractual obligations, security requirements, and operational feasibility. Requests may be submitted through designated support, privacy, or legal contact channels. Where identity verification is reasonably necessary, Cognispace may request additional information before processing a request.

For enterprise-managed accounts, certain rights requests may need to be directed through your organization’s workspace administrator or designated data controller. In such cases, Cognispace may act as a service provider or processor on behalf of the enterprise customer.

9. International Data Transfers

Cognispace may process, store, access, or back up information in jurisdictions outside your state, province, or country of residence. This may include transfers to cloud infrastructure providers, authorized subprocessors, support personnel, and enterprise systems operating in multiple jurisdictions.

Where required by applicable law, Cognispace implements appropriate contractual, organizational, and technical safeguards to support lawful cross-border data transfers. Such safeguards may include contractual transfer clauses, data processing agreements, confidentiality obligations, access restrictions, encryption controls, and regional infrastructure controls where available.

By using the Services, you acknowledge that information may be transferred to and processed in jurisdictions that may have different data protection laws than your jurisdiction of residence.

10. Children's Privacy

The Services are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13 without legally valid authorization. Where applicable law requires a higher age threshold, Cognispace will comply with the relevant jurisdictional requirement.

If we become aware that personal information from a child has been collected in violation of applicable law, we will take reasonable steps to suspend access where appropriate, remove the information from active systems, and delete it consistent with operational and legal requirements.

Parents, guardians, schools, or authorized institutions who believe information has been submitted in error may contact Cognispace through the designated privacy channels.

11. Policy Updates

Cognispace may update this Privacy Policy from time to time to reflect changes in our services and product functionality, legal or regulatory requirements, security and infrastructure controls, operational practices, or business structure.

When material changes are made, we will update the "Last Updated" date and, where appropriate, provide additional notice through the Services, email communications, administrative notices, or website postings.

Continued use of the Services after the effective date of an updated Privacy Policy constitutes acceptance of the revised Policy to the extent permitted by applicable law.

12. Contact Information

For privacy-related questions, requests, legal notices, or concerns, please contact:

Cognispace, LLC

Privacy Office
privacy@cognispacehq.com

This Privacy Policy was prepared by Cognispace, LLC. It is intended to clearly describe our data practices and does not constitute legal advice.