TALYX AI PRIVACY POLICY

Classification: Public Document
Effective Date: October 17, 2025
Last Reviewed: October 17, 2025
Document Version: 1.0

EXECUTIVE SUMMARY

Talyx AI, Inc. and its subsidiaries and affiliates (collectively "Talyx," "we," "us," or "our") is committed to protecting the privacy and security of personal data while maintaining the transparency essential to our guaranteed outcome methodology. This Privacy Policy describes how we collect, use, protect, and disclose personal data when you interact with our services, websites, applications, and business operations.

Talyx operates as a premium AI strategy implementation specialist delivering guaranteed operational alpha to growth-oriented businesses and elite wealth management teams. Our commitment to privacy reflects our broader commitment to transparency, outcome accountability, and capability development without dependency creation.

This policy applies when Talyx acts as a data controller, determining how and why personal data is processed. Where we process data on behalf of clients during service engagements, separate data processing agreements govern those activities.

SECTION 1: DATA CONTROLLER IDENTIFICATION

Talyx AI, Inc. serves as the primary data controller for personal data collected through our business operations. The specific Talyx entity serving as your data controller may vary based on your geographic location and the nature of your engagement with Talyx.

For inquiries regarding data controller identification or data protection matters:

Talyx AI, Inc.
Legal and Compliance Department
Email: info@talyx.ai

SECTION 2: PERSONAL DATA COLLECTION METHODS

Talyx collects personal data through multiple channels in the course of our business operations:

Direct Collection from Individuals

We collect personal data directly from you when you:

Engage with our websites, including www.talyx.ai and associated digital properties

Create user accounts or profiles within Talyx platforms

Request information about our services or guaranteed outcome methodology

Register for Talyx events, webinars, strategic briefings, or educational programs

Subscribe to Talyx Insights, newsletters, research publications, or thought leadership content

Participate in surveys, assessments, or capability maturity evaluations

Communicate with Talyx representatives via email, telephone, video conference, or in-person meetings

Submit inquiries through contact forms or chatbot interfaces

Engage with Talyx social media properties or content

Service Engagement Data Collection

During active client engagements, we collect personal data necessary to deliver our AI implementation services and validate guaranteed outcomes:

Operational data from client systems required for AI implementation and performance measurement

Contact information for client personnel involved in engagement activities

Performance metrics and operational alpha measurements validating guarantee fulfillment

Documentation of capability development activities and knowledge transfer sessions

Communication records related to project execution, milestone achievement, and outcome validation

Stakeholder feedback regarding engagement experience and certification processes

Third-Party Data Sources

Talyx may receive personal data from third-party sources, including:

Publicly available business information from corporate websites, professional networks, and industry databases

Data vendors providing business intelligence for market research and competitive analysis

Referral partners and strategic alliance members introducing prospective clients

Technology platforms and service providers supporting Talyx operations

In all cases where we receive data from third parties, we verify that the provider has lawfully collected the information and is authorized to share it with Talyx for our intended business purposes.

SECTION 3: CATEGORIES OF PERSONAL DATA AND PROCESSING PURPOSES

The following table details the categories of personal data we collect, our purposes for processing, legal bases for use, and data access parameters:

Identification and Contact Information

Purpose: Establish and maintain business relationships, communicate regarding services, deliver requested information, and fulfill contractual obligations.

Categories of Personal Data: Name, title, company affiliation, business address, email address, telephone number, professional credentials, LinkedIn profile information.

Legal Basis for Use: Legitimate interest in conducting business operations and building relationships; contractual necessity for service delivery; consent where specifically provided.

Data Access: Talyx subsidiaries and affiliates, authorized service providers as specified in Section 5.

Professional and Business Information

Purpose: Assess engagement fit, customize service delivery, understand organizational context, and optimize outcome delivery methodology.

Categories of Personal Data: Industry sector, company size, revenue range, organizational structure, technology infrastructure, business challenges, strategic objectives, competitive positioning.

Legal Basis for Use: Legitimate interest in delivering optimized services; contractual necessity for engagement execution.

Data Access: Talyx engagement teams, authorized analytics providers, system integration partners under confidentiality obligations.

Engagement and Service Delivery Data

Purpose: Execute AI implementation services, measure guaranteed outcomes, validate operational alpha delivery, document capability development, and fulfill contractual commitments.

Categories of Personal Data: Project participation records, operational performance metrics, system integration data, process improvement measurements, capability assessment results, certification evaluation documentation, guarantee validation records.

Legal Basis for Use: Contractual necessity for service delivery and guarantee fulfillment; legitimate interest in maintaining quality standards and demonstrating outcome achievement.

Data Access: Talyx project teams, performance measurement systems, quality assurance personnel, third-party service providers supporting engagement delivery.

Financial and Transaction Information

Purpose: Process payments, manage accounts, fulfill contractual obligations, calculate performance bonuses, and maintain financial records.

Categories of Personal Data: Billing information, payment card details (processed through PCI-compliant third-party processors), invoicing records, performance-based fee calculations, guarantee fulfillment documentation.

Legal Basis for Use: Contractual necessity; legal compliance with financial reporting and tax requirements.

Data Access: Talyx finance department, authorized payment processors, accounting service providers, tax and legal advisors as required.

Website and Digital Property Usage Data

Purpose: Operate and improve our digital properties, personalize user experience, analyze usage patterns, enhance security, and optimize content delivery.

Categories of Personal Data: IP address, browser type and version, device identifiers, operating system, referring URLs, pages viewed, time spent on pages, clickstream data, search queries, cookie identifiers.

Legal Basis for Use: Legitimate interest in operating our digital properties and improving user experience; consent for non-essential cookies per our Cookie Policy.

Data Access: Talyx marketing and technology teams, website analytics providers, content delivery networks, security service providers.

Marketing and Communications Data

Purpose: Deliver thought leadership content, provide strategic insights, inform about new offerings, maintain relationships, and conduct market research.

Categories of Personal Data: Newsletter subscription preferences, content download history, event registration records, webinar attendance, research report access, communication preferences, engagement tracking data.

Legal Basis for Use: Consent for marketing communications; legitimate interest in maintaining business relationships and providing relevant content.

Data Access: Talyx marketing team, email service providers, event management platforms, analytics providers.

Research and Analytics Data

Purpose: Conduct market research, develop benchmarking insights, improve service methodologies, validate outcome frameworks, and contribute to thought leadership.

Categories of Personal Data: Aggregated performance metrics, industry benchmarking data, capability maturity assessments, operational improvement measurements, anonymized engagement outcomes.

Legal Basis for Use: Legitimate interest in research activities; consent where specifically obtained; contractual provisions allowing benchmarking participation.

Data Access: Talyx research teams, authorized analytics platforms, benchmarking consortium participants under confidentiality obligations.

Security and Fraud Prevention Data

Purpose: Protect Talyx systems and data, prevent unauthorized access, detect fraudulent activity, and maintain operational security.

Categories of Personal Data: Authentication credentials, access logs, security event records, threat detection data, system monitoring information.

Legal Basis for Use: Legitimate interest in protecting our business and stakeholder data; contractual necessity for secure service delivery.

Data Access: Talyx security personnel, cybersecurity service providers, threat intelligence platforms.

Legal Compliance and Governance Data

Purpose: Comply with legal obligations, respond to legal processes, enforce agreements, protect legal rights, and maintain corporate governance standards.

Categories of Personal Data: Documentation required for regulatory compliance, legal correspondence, dispute resolution records, audit trails, compliance verification information.

Legal Basis for Use: Legal obligation; legitimate interest in protecting legal rights and maintaining governance standards.

Data Access: Talyx legal department, external legal counsel, regulatory authorities as required, auditors and compliance assessors.

SECTION 4: DATA PROCESSING LIMITATIONS AND COMMITMENTS

Talyx makes the following commitments regarding data processing practices:

Deidentification and Anonymization Standards

When we aggregate, deidentify, or anonymize personal data such that it no longer identifies specific individuals under applicable law, we maintain such data in deidentified form and commit to:

Maintaining technical and administrative safeguards preventing reidentification

Prohibiting attempts to reidentify individuals within deidentified datasets

Restricting deidentified data use to legitimate research, analytics, benchmarking, and service improvement purposes

Requiring contractual commitments from any recipients of deidentified data to maintain its deidentified status

No Sale of Personal Data

Talyx does not sell personal data as defined under California Civil Code Section 1798.140 or other applicable privacy laws. We do not exchange personal data for monetary or other valuable consideration. Any data sharing occurs solely for the business purposes described in this policy under appropriate contractual safeguards.

Processing Limitations

We limit personal data processing to purposes that are:

Specified, explicit, and legitimate at the time of collection

Necessary for the stated purposes

Compatible with original collection purposes or supported by additional legal basis

Transparent and disclosed to data subjects

Subject to appropriate retention limitations

Automated Decision-Making

Talyx does not employ automated decision-making or profiling that produces legal effects or similarly significantly affects individuals without human oversight and intervention opportunity. Where we use automated analysis tools for service optimization or capability assessment, human review and judgment remain integral to all significant decisions.

SECTION 5: DATA RECIPIENTS AND INTERNATIONAL TRANSFERS

Data Recipients

Personal data collected by Talyx may be shared with the following categories of recipients for the business purposes described in Section 3:

Talyx Subsidiaries and Affiliates: Personal data may be shared among Talyx entities worldwide to support coordinated service delivery, research collaboration, and operational efficiency.

Service Providers and Processors: We engage third-party service providers to perform functions on our behalf, including:

Technology infrastructure providers (cloud hosting, data storage, system integration)

Communication platforms (email services, video conferencing, collaboration tools)

Analytics and research platforms (performance measurement, benchmarking, market intelligence)

Payment processors (PCI-compliant transaction processing)

Professional service providers (legal counsel, accounting, auditing, insurance)

Marketing and event management platforms

Security and fraud prevention services

All service providers operate under contractual obligations limiting data use to specified purposes and requiring appropriate security measures.

Professional Advisors: Legal counsel, accountants, auditors, insurers, and other professional advisors as necessary for business operations and legal compliance.

Regulatory and Legal Authorities: Government agencies, regulatory bodies, courts, and law enforcement when required by applicable law or legal process.

Business Transaction Parties: In the event of merger, acquisition, financing, asset sale, or similar corporate transaction, personal data may be transferred to relevant parties under appropriate confidentiality obligations.

Client-Authorized Recipients: During service engagements, we may share personal data with parties you specifically authorize for project execution and outcome delivery.

International Data Transfers

Talyx operates globally and may transfer personal data to countries outside your jurisdiction, including countries that may not provide equivalent data protection standards. When we transfer personal data internationally, we implement appropriate safeguards including:

Standard Contractual Clauses: We use European Commission-approved Standard Contractual Clauses for transfers from the European Economic Area to countries without adequacy decisions.

Binding Corporate Rules: Transfers among Talyx entities are governed by internal policies ensuring consistent data protection standards globally.

Adequacy Decisions: Where available, we rely on adequacy decisions by relevant authorities finding recipient countries provide adequate protection.

Additional Safeguards: Technical and organizational measures supplementing legal mechanisms to ensure data protection throughout international transfers.

For specific information regarding international data transfers relevant to your engagement, contact info@talyx.ai.

SECTION 6: DATA SECURITY

Talyx implements comprehensive technical, administrative, and physical security measures to protect personal data against unauthorized access, disclosure, alteration, and destruction. Our security program includes:

Technical Security Controls

Encryption of data in transit using industry-standard protocols (TLS 1.2 or higher)

Encryption of data at rest for sensitive information categories

Multi-factor authentication for system access

Regular security testing including vulnerability assessments and penetration testing

Intrusion detection and prevention systems

Security information and event management (SIEM) platforms

Data loss prevention technologies

Secure software development lifecycle practices

Administrative Security Controls

Comprehensive information security policies and procedures

Employee security training and awareness programs

Background checks for personnel with data access

Role-based access controls limiting data access to business need

Vendor management program ensuring third-party security standards

Incident response and breach notification procedures

Regular security audits and compliance assessments

Physical Security Controls

Restricted access to facilities housing data systems

Environmental controls protecting technology infrastructure

Visitor management and facility access logging

Secure disposal procedures for physical media

Security Program Maintenance

Our security program undergoes continuous improvement through:

Regular risk assessments identifying evolving threats

Incorporation of industry best practices and emerging standards

Monitoring of regulatory developments and compliance requirements

Third-party security certifications and audits

Incident analysis and corrective action implementation

While no security measures provide absolute protection, Talyx maintains industry-leading security practices commensurate with the sensitivity of data we process.

SECTION 7: DATA RETENTION

Talyx retains personal data for periods necessary to fulfill the purposes described in this policy, comply with legal obligations, resolve disputes, and enforce agreements. Specific retention periods vary based on data categories and processing purposes:

General Retention Principles

Business Relationship Data: Maintained while business relationship remains active plus periods required for legal compliance and legitimate business purposes.

Service Engagement Data: Retained for engagement duration plus minimum seven years to support guarantee validation, capability certification verification, and legal compliance requirements.

Performance and Outcome Data: Retained for extended periods to support benchmarking research, methodology validation, and long-term outcome analysis; deidentified where feasible after primary purposes conclude.

Marketing Communications Data: Retained until consent withdrawal or relationship termination plus periods required for legal compliance.

Financial Records: Retained per applicable tax, accounting, and financial reporting requirements, typically minimum seven years.

Legal and Compliance Data: Retained per regulatory requirements and litigation hold obligations.

Website Usage Data: Retained for limited periods per Cookie Policy unless longer retention necessary for security or legal purposes.

Specific Retention Categories

Guarantee Validation Documentation: Minimum seven years from engagement completion to support contractual obligations and dispute resolution.

Capability Certification Records: Minimum ten years to maintain certification program integrity and verification capabilities.

Audit and Compliance Records: Per regulatory requirements, typically seven to ten years.

Security Logs and Incident Documentation: Minimum two years or per regulatory requirements, whichever is longer.

Upon expiration of retention periods, we securely delete or anonymize personal data unless extended retention is required by legal obligation or legitimate business purpose requiring specific data retention.

SECTION 8: DATA COLLECTION FROM MINORS

Talyx services target business professionals and organizational clients. We do not knowingly collect personal data from individuals under 18 years of age. If we become aware that we have inadvertently collected data from a minor, we will take prompt steps to delete such information. Parents or guardians believing we may have collected data from minors should contact info@talyx.ai.

SECTION 9: DATA SUBJECT RIGHTS

Subject to applicable law, individuals have rights regarding their personal data. Talyx respects and facilitates exercise of these rights within legal frameworks governing data protection.

Right to Access

You may request confirmation of whether we process your personal data and obtain access to such data along with information about processing purposes, data categories, recipients, retention periods, and your rights.

Right to Rectification

You may request correction of inaccurate personal data and completion of incomplete data relevant to processing purposes.

Right to Erasure

Subject to legal and contractual limitations, you may request deletion of personal data when:

Data no longer necessary for original processing purposes

Consent is withdrawn and no alternative legal basis exists

Processing is unlawful

Legal obligation requires erasure

You object to processing and no overriding legitimate grounds exist

Right to Restriction of Processing

You may request restriction of processing when:

Data accuracy is contested during verification

Processing is unlawful but you prefer restriction over erasure

We no longer need the data but you require it for legal claims

You have objected to processing pending verification of legitimate grounds

Right to Data Portability

Where processing is based on consent or contractual necessity and carried out by automated means, you may receive personal data in structured, commonly used, machine-readable format and request transmission to another controller where technically feasible.

Right to Object

You may object to processing based on legitimate interests or for direct marketing purposes. Upon objection, we will cease processing unless we demonstrate compelling legitimate grounds overriding your interests or processing is necessary for legal claims.

Right to Withdraw Consent

Where processing is based on consent, you may withdraw consent at any time without affecting lawfulness of processing prior to withdrawal.

Right to Lodge Complaints

You have the right to lodge complaints with supervisory authorities regarding our data processing practices. Relevant supervisory authority depends on your jurisdiction:

European Economic Area residents: Data protection authority in your country of residence

California residents: California Attorney General

Other jurisdictions: Applicable privacy regulatory authority

Right to Non-Discrimination

Talyx does not discriminate against individuals exercising privacy rights under applicable law, including CCPA provisions prohibiting denial of services, charging different prices, providing different service quality, or suggesting you will receive different service levels.

SECTION 10: EXERCISING DATA PROTECTION RIGHTS

To exercise any rights described in Section 9, submit requests through:

Email: info@talyx.ai

Written Request: Talyx AI, Inc., Legal and Compliance Department, [Address]

Online Portal: [Privacy request portal URL when available]

Request Requirements

To process your request efficiently and securely, provide:

Sufficient information to identify you and verify your identity

Specific description of the right you wish to exercise

Reasonable details enabling us to locate relevant personal data

Proof of identity and, where applicable, proof of authority to act on behalf of another individual

Response Timeline

We will respond to verified requests within legally required timeframes:

GDPR Requests: Within one month, extendable by two months for complex requests

CCPA Requests: Within 45 days, extendable by 45 days for complex requests

Other Jurisdictions: Per applicable legal requirements

We will notify you if additional time is required and explain reasons for extension.

Request Verification

To protect against fraudulent requests, we verify requester identity using risk-based approach considering data sensitivity and processing risks. Verification may require:

Matching provided information against existing records

Requesting additional identification documentation

Using third-party identity verification services

For high-sensitivity requests, we may require additional verification measures.

Authorized Agent Requests

California residents may designate authorized agents to submit privacy requests. Authorized agents must:

Provide proof of written authorization from data subject

Verify their own identity

Provide data subject's verification information as required

We may require data subject confirmation directly from the individual to validate authorized agent status.

Fee Structure

We do not charge fees for processing privacy rights requests unless:

Requests are manifestly unfounded or excessive

Requests require disproportionate effort beyond legal obligations

Individuals request additional copies beyond the first free copy

Where fees apply, we will notify you and provide cost estimates before completing requests.

SECTION 11: NEWSLETTER AND MARKETING COMMUNICATIONS

Subscription Management

If you subscribe to Talyx newsletters, insights, or other marketing communications, you may manage preferences or unsubscribe through:

Unsubscribe links in email communications

Account preference settings on Talyx platforms

Email request to marketing@talyx.ai

Contact to info@talyx.ai

We honor opt-out requests promptly, typically within 10 business days. Note that you may continue receiving transactional or relationship communications necessary for business operations even after marketing opt-out.

Communication Types

Marketing Communications: Thought leadership content, research reports, service offerings, event invitations, strategic insights. Sent based on consent or legitimate interest in maintaining business relationships.

Transactional Communications: Engagement-related updates, performance reports, guarantee validation documentation, contractual communications. Sent based on contractual necessity and cannot be opted out while relationship exists.

Relationship Communications: Account management, client success activities, capability certification updates. Sent based on legitimate business interest in supporting client success.

SECTION 12: COOKIES AND TRACKING TECHNOLOGIES

Talyx uses cookies and similar tracking technologies on our websites and digital properties. Comprehensive information regarding our cookie practices, types of cookies deployed, purposes, and management options is available in our separate Cookie Policy.

Key points regarding cookies:

We use strictly necessary, functional, analytics, and marketing cookies

You control cookie preferences through browser settings and our cookie management tools

Refusing non-essential cookies may limit certain website features

Third-party cookies are subject to respective providers' privacy policies

For detailed information, review our Cookie Policy at [Cookie Policy URL].

SECTION 13: CALIFORNIA PRIVACY RIGHTS

California residents have specific rights under California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

Right to Know

California residents may request disclosure of:

Categories of personal information collected

Categories of sources from which information is collected

Business or commercial purposes for collection

Categories of third parties with whom information is shared

Specific pieces of personal information collected

Right to Delete

California residents may request deletion of personal information, subject to exceptions for legal compliance, service completion, security purposes, and other specified uses.

Right to Opt-Out of Sale

Talyx does not sell personal information as defined under CCPA. Should our practices change, we will provide notice and implement opt-out mechanisms.

Right to Correct

California residents may request correction of inaccurate personal information.

Right to Limit Use of Sensitive Personal Information

California residents may limit use and disclosure of sensitive personal information. Talyx does not use sensitive personal information in ways requiring limitation rights.

Authorized Agent Requests

California residents may designate authorized agents to submit privacy requests on their behalf per procedures described in Section 10.

Non-Discrimination

Talyx does not discriminate against California residents exercising CCPA rights.

Shine the Light

Under California Civil Code Section 1798.83, California residents may request information about personal information shared with third parties for direct marketing purposes. Talyx does not share personal information with third parties for their direct marketing purposes.

SECTION 14: EUROPEAN ECONOMIC AREA AND UK RIGHTS

EEA and UK residents have specific rights under General Data Protection Regulation (GDPR) and UK GDPR.

Legal Bases for Processing

We process personal data under the following legal bases:

Contractual Necessity: Processing necessary to fulfill contractual obligations for service delivery

Legitimate Interests: Processing necessary for legitimate business interests not overridden by individual rights

Legal Obligation: Processing required to comply with legal requirements

Consent: Processing based on specific, informed, freely given consent

International Data Transfers

Transfers from EEA/UK to countries without adequacy decisions are protected by Standard Contractual Clauses and supplementary measures ensuring adequate protection.

Supervisory Authority

EEA residents may lodge complaints with data protection authorities in their country of residence. UK residents may contact the Information Commissioner's Office.

Representative

For EEA data protection matters, contact our EU representative at [EU representative contact information].

For UK data protection matters, contact our UK representative at [UK representative contact information].

SECTION 15: POLICY UPDATES AND CHANGES

Talyx reserves the right to update this Privacy Policy to reflect changes in our practices, services, legal requirements, or other operational considerations.

Change Notification

Material changes will be communicated through:

Prominent notice on our website

Email notification to registered users

In-platform notifications for account holders

Notice during active service engagements

Effective Date of Changes

Updated policies become effective on the date specified in the revised policy. Continued use of Talyx services after effective date constitutes acceptance of updated terms.

Historical Versions

Previous policy versions are available upon request to info@talyx.ai for users seeking to review prior terms applicable during specific timeframes.

SECTION 16: CONTACT INFORMATION

For questions, concerns, or requests regarding this Privacy Policy or Talyx data processing practices:

Primary Contact:
Talyx AI, Inc.
Legal and Compliance Department
Email: info@talyx.ai

Data Protection Officer:
Email: info@talyx.ai

SECTION 17: SUPPLEMENTAL JURISDICTION-SPECIFIC PROVISIONS

This section contains additional provisions applicable to residents of specific jurisdictions beyond those addressed in dedicated sections above.

Canada

Canadian residents have rights under Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial legislation. Contact our Canadian Privacy Officer at info@talyx.ai for jurisdiction-specific inquiries.

Australia

Australian residents have rights under Privacy Act 1988. We comply with Australian Privacy Principles governing collection, use, and disclosure of personal information.

Other Jurisdictions

Residents of jurisdictions with specific privacy laws not otherwise addressed in this policy should contact info@talyx.ai for information regarding applicable rights and our compliance with local requirements.

DOCUMENT CERTIFICATION

This Privacy Policy has been reviewed and approved by Talyx legal and compliance personnel to ensure alignment with applicable privacy laws, industry standards, and Talyx's commitment to transparency and data protection.

The policy reflects Talyx's core values of transparency, outcome accountability, and stakeholder trust while implementing comprehensive data protection measures consistent with our position as a premium AI strategy implementation specialist serving sophisticated business clients.

Talyx AI, Inc.
Privacy Policy Version 1.0
Effective Date: October 17, 2025

END OF DOCUMENT