



1290 WORLD LLC | TWELVE NINETY CONNECTIONS

TNC Privacy Notice

Version 1.3

Document ID: TNC-PRIVACY-2026-08-23-002

Entity: 1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections ("TNC")

Audience: Public-site visitors, participants, account holders, candidates, clients, partners, service customers, and other persons whose information TNC processes

Effective Date: The date this version is accepted for a new account.

Prior versions: This version applies to new acceptances. Earlier accepted versions, signed copies, decisions, and receipts remain valid and retrievable.

1. SCOPE AND RESPONSIBLE ENTITY

This Privacy Notice explains how TNC may collect, use, disclose, retain, secure, and otherwise process personal information through the Integrated TNC Platform in connection with public websites and pages, T.E.A., accounts, Network Portals, recruiting, services, World Connections, communications, Events, relationship programs, documents, payment references,

When a person first accesses a TNC-controlled website or public page, the Integrated TNC Platform may automatically receive technical, security, routing, and interaction information reasonably necessary to deliver the page, maintain the session, protect the service, diagnose errors, enforce limits, preserve source and referral context, and record the request. Necessary processing may occur without a logged-in Account. Nonessential analytics, advertising, cross-site, targeted-advertising, or similarly regulated technologies require the additional notice, choice, or consent applicable to the technology and jurisdiction.

support, and authorized technology-assisted workflows.

TNC may act as the controller or business responsible for information used for its own relationships and operations. For certain organization-directed activities, TNC may act as a processor, service provider, contractor, recruiting partner, or other role defined by the applicable agreement and law. The controlling agreement determines the parties' responsibilities for that activity.

Network-specific terms, action-specific instruments, notices at collection, recording notices, publicity authorizations, sensitive-data consents, and jurisdiction-specific supplements may provide additional information. The more specific instrument controls its stated subject.

2. DEFINITIONS

"Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a person or household, as defined by applicable law.

"Sensitive Information" means a category requiring additional protection or consent under applicable law, which may include government identifiers, account credentials, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, citizenship or immigration status, health information, genetic or biometric information, sexual orientation, information from a known child, and other legally designated categories.

"Relationship Chapter" means the separately governed record of a person's or organization's role, purpose, permissions, confidentiality, consent, agreements, receipts, and activity within a particular TNC Network or relationship context.

"T.E.A." means the public-facing identity and interaction layer of TNC's integrated end-to-end platform. A visitor or Participant may encounter T.E.A. through TNC-controlled websites, public pages, forms, assistants, portals, and other frontend surfaces. T.E.A. is not a separate company, controller, provider, or independent platform.

"1290 CRM" means TNC's private governed relationship and operational backend. It is the administrative, record, workflow, permission, audit, and command surface corresponding to TNC's public-facing frontend. It may preserve validated identity, organization, relationship, authority, activity, communication, agreement, receipt, event, service, opportunity, payment-reference, and outcome records according to applicable purposes, permissions, confidentiality, and retention rules.



Public interaction with T.E.A. or another frontend surface does not grant access to the backend.

“Integrated TNC Platform” means the single end-to-end system comprising TNC-controlled public websites and pages, T.E.A., authenticated portals and participant-facing functions, and the private governed CRM backend. The public-facing frontend and the private backend are two operational faces of one TNC-controlled system, not separate platforms, providers, or participant relationships. From the time a visitor accesses a TNC-controlled website or page, the request and resulting interaction may be received, secured, routed, processed, contextualized, and recorded as described in the TNC Privacy Notice and other applicable instruments. TNC retains exclusive administrative control of the private backend. Integration does not merge Relationship Chapters, broaden an audience, create access, widen permissions, or authorize a new purpose or consequential action.

3. PERSONAL INFORMATION TNC MAY COLLECT

Depending on the person, relationship, source, and function, TNC may collect the following categories:

- Identity and contact information: legal name, preferred name, approved display name, email address, telephone number, mailing address, time zone, language, and contact preferences.
- Account, authentication, and security information: account identifiers, login and verification events, passkey or authentication status, device and session information, recovery information, IP address, security alerts, access logs, fraud signals, and incident records. TNC should not receive raw passwords, secret keys, or full payment-card credentials through ordinary participant fields.
- Organization and authority information: entity name, affiliation, title, role, department, ownership or management information where relevant, signatory authority, administrator authority, billing authority, approved users, delegation, and revocation information.
- Professional, education, and career information: résumé, work history, education, licenses, credentials, skills, compensation, availability, work authorization, location, career interests, preferences, and professional goals.
- Recruiting and Talent information: jobs, searches, Candidate source, opportunity interests, disclosure permissions, submissions, interviews, assessments, references, offers, placements, Start Dates, onboarding, guarantees, communications, and follow-up.
- Client and business information: hiring needs, role descriptions, compensation structures, business units, locations, decision processes, confidential-search information, contacts, relationship history, and organization access requests.
- Partner and Services information: collaboration roles, referrals, source evidence, Shared Searches, split schedules, service scopes, deliverables, dependencies, acceptance, support, and closeout information.
- World Connections information: verified identity classifications, membership or relationship status, profile information, Signals, Circles, Rooms, Tables, introductions, Events, interests, offers, asks, audiences, moderation, participation, and meaningful relationship outcomes.
- Communications and content: emails, texts, calls, in-platform messages, support requests, meeting details, notes, attachments, documents, images, audio, video, Community Content, and authorized recordings or transcripts.
- Transaction and agreement information: agreement versions, authorizations, elections, signatures, invoices, payment-status references, transaction identifiers, refunds or credits, receipt records, and audit evidence. The approved financial system remains the source of truth for financial facts.
- Website, device, and interaction information: initial page or resource requests, browser and device characteristics, network and protocol information, IP address, pages and features used, referring source, timestamps, session and routing information, performance, errors, cookies, analytics events, preference signals, security telemetry, and other information generated when a person interacts with the Integrated TNC Platform.
- Event and location information: registrations, attendance, travel or venue information voluntarily supplied for an Event, accessibility needs, and location information reasonably necessary for a requested function. TNC does not require precise geolocation unless the function specifically requires it and the appropriate notice and control exist.
- Preferences and support information: accessibility requests, communication settings, privacy choices, relationship preferences, support history, and dispute or appeal information.



- Public and third-party professional information: information from public professional sources, organization websites, lawful research, referrals, authorized providers, and other sources permitted by the person, organization, agreement, or law.
- Inferences and recommendations: relationship context, classifications, summaries, match assessments, risk or fraud signals, likely interests, recommended next actions, and other outputs derived from authorized information.
- Sensitive Information: only when necessary for an authorized purpose, specifically requested through an approved process, and subject to the required legal, security, access, retention, and consent controls.

Participants should not submit Social Security numbers, government identifiers, health information, financial-account credentials, protected-trait information, biometric information, or other Sensitive Information unless TNC specifically requests it through an approved secure channel for a lawful purpose.

4. SOURCES OF PERSONAL INFORMATION

TNC may receive personal information:

- directly from the person or an authorized representative;
- from an organization, Client, employer, Candidate, Talent participant, Partner, reference, service customer, Event participant, or World Connections participant involved in an authorized relationship;
- from public professional sources and lawful research;
- from the Integrated TNC Platform, including TNC websites and public pages, T.E.A., portals, communications, forms, files, Events, the private CRM backend, and related technology systems;
- from connected providers or integrations authorized by the person or organization;
- from hosting, authentication, communications, payment, scheduling, document, analytics, security, and support providers; and
- from source records preserved for provenance, correction, reconciliation, fraud prevention, security, dispute resolution, or audit.

TNC should preserve source, date, status, and confidence where material. Imported, public, third-party, or inferred information is not verified merely because it was received or generated.

5. PURPOSES OF PROCESSING

TNC may process Personal Information to:

- create, authenticate, secure, recover, and administer accounts and separate Relationship Chapters;
- verify identity, organization, affiliation, role, authority, eligibility, jurisdiction, consent, and source;
- operate the Integrated TNC Platform, including public websites and pages, T.E.A., Network Portals, the private CRM backend, secure communications, files, forms, Events, support, and related functions;
- provide recruiting, Protected Search, Talent, Partner, Services, World Connections, and other authorized relationships;
- match and route authorized opportunities, Candidates, services, people, organizations, conversations, Events, and relationship requests;
- manage searches, submissions, interviews, references, offers, placements, onboarding, guarantees, services, collaboration, and follow-up;
- prepare, present, execute, preserve, and administer agreements, notices, authorizations, consents, elections, approvals, receipts, and records;
- communicate about accounts, security, relationships, services, recruiting, opportunities, Events, billing, legal matters, support, and promotional information as permitted;
- maintain context continuity, personalize authorized experiences, and reduce unnecessary repetition;
- analyze, summarize, compare, classify, retrieve, reconcile, and improve authorized information and workflows;



- detect and prevent fraud, misuse, duplicate identity, unauthorized access, harassment, unlawful discrimination, spam, security incidents, and operational failure;
- conduct quality assurance, accessibility work, security testing, risk assessment, research, and product or service improvement consistent with disclosed purposes and applicable law;
- comply with law, enforce agreements, preserve evidence, respond to lawful requests, and protect TNC and affected persons;
- support a merger, financing, reorganization, sale, or transfer subject to appropriate confidentiality and legal controls; and
- create aggregated, statistical, or de-identified information and maintain it in de-identified form where required.

TNC will not use Personal Information for a materially incompatible purpose without the notice, consent, agreement, or other lawful basis required for that purpose.

6. RELATIONSHIP CHAPTERS AND CONTEXTUAL USE

TNC may maintain one verified global identity while preserving separate Client, Talent, Partner, Services, World Connections, Event, communication, payment, and other Relationship Chapters.

Because the public frontend and private backend are one integrated system, information and authorized context may move through the Integrated TNC Platform for the stated purpose. The fact that information is stored in that system or technically available to TNC does not authorize its use, disclosure, transfer, recommendation, or action in another context. Each use must remain supported by the information's source, purpose, Network, relationship, role, organization, authority, audience, confidentiality, consent or other lawful basis, sensitivity, effective date, and action-specific permission.

Information privately supplied in one context must not be silently used against the person or disclosed in another context merely because TNC has access to it. More intelligence does not create more entitlement.

7. T.E.A., INFERENCES, PROFILING, AND HUMAN REVIEW

T.E.A. is the public-facing interface of the Integrated TNC Platform. T.E.A. and other technology-assisted functions operating through that platform may support research, drafting, summarization, comparison, classification, retrieval, matching, fraud detection, moderation support, workflow routing, and preparation of recommendations or governed actions.

Technology-assisted output may be incomplete, outdated, inferred, or incorrect. TNC may distinguish verified facts, Participant statements, evidence, inferences, recommendations, drafts, approvals, conflicts, and unknowns. An inference is not a verified fact merely because it is generated or stored.

TNC does not authorize T.E.A. to make an employer's final employment decision, independently grant Client or organization access, accept an agreement, create payment authority, make an investment decision, or override a required human or organizational approval.

Where applicable law grants rights concerning automated decisionmaking, profiling, or significant decisions, TNC will provide the required notice, explanation, access, correction, opt-out, appeal, or human-review process before the regulated use occurs. TNC should conduct and document required risk assessments before activating covered high-risk processing.

8. HOW TNC MAY DISCLOSE PERSONAL INFORMATION

Subject to purpose, confidentiality, consent, authority, and access controls, TNC may disclose Personal Information to:

- Clients, employers, Candidates, Talent participants, Partners, service customers, World Connections participants, Event participants, and other persons involved in an authorized relationship or action;
- organization administrators and Authorized Users within the exact recorded scope;
- hosting, authentication, communications, payment, scheduling, document, analytics, accessibility, security, support, and other service providers acting for TNC;
- professional advisers, auditors, insurers, accountants, and legal representatives;
- regulators, courts, law enforcement, government agencies, and other persons when required or permitted by law;
- persons reasonably necessary to protect safety, rights, security, contracts, or the integrity of the ecosystem;



- a potential or actual successor, purchaser, lender, investor, or transaction participant in a merger, financing, reorganization, sale, or transfer, subject to appropriate protection; and
- the public only as permitted by the TNC Public & Commercial Participation Terms and any additional authorization required for identifiable, endorsement-style, confidential, or restricted material.

TNC does not disclose Candidate Data, private Client accounts, confidential searches, private compensation, credentials, Sensitive Information, or restricted communications merely because a general relationship, membership, title, payment, or organization affiliation exists.

9. SERVICE PROVIDERS AND CONTRACTUAL CONTROLS

TNC may use service providers for functions such as hosting, authentication, communications, payment processing, scheduling, document delivery, analytics, security, accessibility, and support. Providers should receive only the information reasonably necessary for their function and should be subject to appropriate contractual, confidentiality, security, deletion, return, audit, and use restrictions.

A connected provider does not authorize unrelated use, sale, sharing, training, advertising, or disclosure. TNC must separately approve provider access, scope, environment, permissions, and any production write or deletion authority.

Where an organization requires a data-processing agreement, security addendum, subprocessor list, international-transfer mechanism, or similar contract, that instrument must be completed before the covered processing begins.

10. SALE, SHARING, TARGETED ADVERTISING, AND COMMERCIAL USE

TNC does not intend to sell Personal Information for money. TNC does not sell Candidate Data, confidential relationship data, or private communications as a product.

Some privacy laws define “sale,” “sharing,” “targeted advertising,” or “profiling” more broadly than an exchange for money. If a TNC activity is legally treated as one of those regulated uses, TNC will provide the required clear notice and opt-out or consent mechanism before or at the time required by law.

TNC will process legally recognized universal opt-out preference signals where required and supported by the released implementation. A person should not be required to verify identity merely to exercise an opt-out that applicable law permits without verification.

TNC does not currently offer a financial incentive or price difference in exchange for the sale or sharing of Personal Information. Any future program involving a legally regulated financial incentive must be separately documented and disclosed before enrollment.

11. COOKIES, ANALYTICS, AND SIMILAR TECHNOLOGIES

TNC may use necessary technologies for authentication, security, fraud prevention, routing, preferences, accessibility, session continuity, and service operation.

TNC may use functional or analytics technologies to understand use, diagnose errors, measure performance, improve quality, and maintain the platform. Before deploying nonessential advertising, cross-site, targeted-advertising, or similarly regulated tracking, TNC must classify the technology, update the applicable Cookie Notice, implement a preference center, obtain consent where required, and honor legally required opt-outs and preference signals.

A browser “Do Not Track” setting may not have a uniform legal meaning. TNC will honor recognized opt-out preference signals where applicable law requires.

12. COMMUNICATIONS, RECORDINGS, AND PUBLICITY

TNC may process communications and related metadata for account, security, relationship, recruiting, service, support, quality, legal, audit, Event, and continuity purposes. Promotional communications remain subject to the TNC Communications Notice and applicable consent, unsubscribe, STOP, suppression, sender-identification, and channel-specific rules.

Recording or transcription is governed by the TNC Recording & Transcription Notice and the consent or notice requirements applicable to the participants, purpose, channel, and jurisdiction.



Recording consent is not publicity consent. Identifiable public or commercial use of a person's name, image, likeness, voice, quote, testimonial, story, organization, logo, Event attendance, or private communication requires the applicable authorization and confidentiality controls.

13. SENSITIVE INFORMATION

TNC limits Sensitive Information to what is reasonably necessary for an authorized, lawful purpose. TNC may require separate consent, enhanced authentication, restricted access, short retention, encryption or secure transfer, documented risk assessment, and human review before processing Sensitive Information.

TNC will not infer consent to process Sensitive Information from a general account, Network, membership, payment, Event registration, or acceptance of this Notice.

Where applicable law grants a right to limit the use or disclosure of Sensitive Information, TNC will provide the required method and will not retaliate for exercising the right.

14. CANDIDATE, TALENT, AND EMPLOYMENT-RELATED INFORMATION

Candidate and Talent information is relationship-scoped and purpose-limited. TNC may collect and use it to evaluate, represent, match, communicate about, and administer authorized opportunities and recruiting relationships.

Candidate identity, résumé, contact, compensation, references, or other information may be disclosed only through an authorized recruiting process, supported by the required consent or other lawful authority, approved recipient, permitted disclosure state, and applicable receipt.

TNC is not the employer and does not control an employer's final selection, classification, accommodation, background-check, work-authorization, payroll, supervision, or employment decision. Background screening or consumer-report activity requires separate lawful authorization and procedures.

Some state consumer privacy laws exclude or treat employment-context data differently. TNC will apply the rights and notices required by the law governing the person and processing and may voluntarily provide additional access or correction options where feasible.

15. ORGANIZATION AND BUSINESS-CONTACT INFORMATION

Business-contact and organization information may be used to administer relationships, validate authority, communicate about services and opportunities, maintain records, prevent fraud, support business development, and operate the applicable Network.

The existence of a business relationship does not eliminate applicable privacy, communications, confidentiality, or access rights. Organization administrators may receive only information within their recorded authority and matter scope.

16. RETENTION AND DELETION

TNC retains Personal Information only as reasonably necessary for the disclosed purpose, relationship continuity, contracts, searches, services, consent records, Candidate or source protection, legal requirements, limitation periods, security, fraud prevention, audit, accounting references, disputes, legal holds, and records management.

Retention varies by information category, source, Network, relationship status, contract, consent, security need, legal requirement, and whether the information remains necessary. TNC may delete, de-identify, restrict, archive, or preserve information under the applicable retention schedule and legal hold.

TNC may preserve a minimal record of a prior acceptance, transaction, source, correction, opt-out, privacy request, dispute, moderation action, or security event after other information is deleted when necessary to honor the person's choice, prevent re-collection, comply with law, or preserve evidence.

A current retention schedule, deletion workflow, legal-hold process, and provider-deletion process must control production implementation. TNC will not promise immediate deletion where a lawful exception or surviving obligation applies.



17. SECURITY

TNC uses administrative, technical, physical, and organizational safeguards appropriate to the nature and risk of the information. Safeguards may include identity and access controls, multi-factor authentication, least privilege, encryption in transit, encryption at rest where supported, provider controls, logging, monitoring, backups, secure disposal, vulnerability management, incident response, and recovery procedures.

No system is perfectly secure. Participants must protect credentials, use approved channels, avoid submitting secrets through unapproved methods, and promptly report suspected compromise.

TNC will assess suspected incidents and provide notices of qualifying security incidents as required by applicable law. TNC will not represent an unverified incident state as confirmed or claim a control that has not been implemented and tested.

18. INTERNATIONAL AND CROSS-BORDER PROCESSING

TNC is based in the United States. Personal Information may be processed in the United States or another jurisdiction where TNC or an authorized provider operates.

Before activating processing subject to additional cross-border transfer restrictions, TNC must implement the required notice, agreement, transfer mechanism, risk assessment, provider terms, localization, or restriction. If TNC cannot lawfully support the jurisdiction or activity, TNC may decline, limit, or pause it.

Where applicable, TNC may rely on contractual necessity, consent, legal obligation, legitimate interests, or another lawful basis recognized by the governing law. The applicable jurisdictional supplement will identify any additional controller details, representative, supervisory authority, or transfer mechanism required for released use.

19. CHILDREN AND MINORS

TNC's general-audience services are not directed to children under 13, and TNC does not knowingly create independent Accounts for or collect Personal Information online from children under 13 outside an expressly approved process that complies with applicable parental-notice and consent requirements.

If TNC learns that it collected Personal Information from a child under 13 without the required authority, TNC will restrict the Account or processing and take appropriate steps to delete or otherwise handle the information as required by law.

A minor who is permitted to use a TNC function may require a parent, guardian, or other legally authorized representative and may be restricted from functions inappropriate for the person's age or legal capacity.

20. PRIVACY RIGHTS AND CHOICES

Depending on the person's jurisdiction, relationship, and information, rights may include:

- confirming whether TNC processes Personal Information;
- accessing or obtaining a copy of Personal Information;
- correcting inaccurate Personal Information;
- deleting Personal Information, subject to lawful exceptions;
- obtaining a portable copy where required;
- opting out of sale, sharing, targeted advertising, or certain profiling;
- limiting certain uses or disclosures of Sensitive Information;
- withdrawing consent where processing depends on consent;
- requesting human review or exercising rights relating to regulated automated decisionmaking where applicable;
- appealing a denied request where applicable; and
- receiving equal service and nonretaliation for exercising a privacy right.

TNC may verify identity, authority, relationship, and jurisdiction before fulfilling a request. Verification must be proportionate to the request and risk. TNC may deny or limit a request where permitted by law, including to protect another person,



preserve security, detect fraud, maintain legal claims, honor a contract, preserve required records, or comply with another legal duty.

An authorized agent may be required to provide signed permission, power of attorney, organization authority, or other evidence. TNC will explain a denial and provide an appeal method when required.

21. CALIFORNIA AND OTHER U.S. STATE DISCLOSURES

To the extent a U.S. state comprehensive privacy law applies, the categories described in Section 3 are the categories TNC may collect and may have collected during the preceding 12 months; the sources are described in Section 4; the business and commercial purposes are described in Section 5; and the recipient categories are described in Sections 8 and 9.

TNC does not intend to sell Personal Information for money. If a covered use is legally treated as a sale, sharing, targeted advertising, or profiling, TNC will provide the required notice and choice. TNC will honor legally recognized universal opt-out mechanisms where required by the applicable state law and released implementation.

California residents may have rights to know, access, correct, delete, opt out of sale or sharing, limit certain uses of Sensitive Personal Information, and receive non-discriminatory treatment. Other state laws may provide similar rights and may also require consent for Sensitive Information, data-protection assessments, and appeal processes.

TNC is not representing in this Notice that every state comprehensive privacy law applies to every TNC activity. Applicability depends on thresholds, exemptions, context, residency, and actual processing. TNC will maintain a jurisdiction and activity matrix and provide the additional notice or process required where a law applies.

22. EXERCISING PRIVACY RIGHTS

Privacy questions and requests may be submitted through the applicable authenticated portal or by emailing tsullivan@1290worldconnections.com with the subject "Privacy Request." Office: (316) 365-5546. Direct: (316) 374-4159.

A request should identify the requester, relationship, jurisdiction, request type, and the information reasonably necessary to locate and verify the relevant records. Do not send passwords, secret keys, full payment-card data, or unnecessary Sensitive Information by email.

TNC will acknowledge, verify, respond, and provide an appeal or explanation within the period required by applicable law. A request, verification, response, denial, appeal, correction, deletion, export, restriction, opt-out, and withdrawal should each create a durable source-tagged record.

A physical privacy-notice address, authorized-agent method, and any jurisdiction-specific contact required for external release will be provided through the public Legal Center or applicable supplement before the covered use is activated.

23. COMMUNICATION CHOICES

Promotional email may be unsubscribed through the message or an approved preference center. Promotional SMS may be stopped using STOP or another reasonable method stated in the TNC Communications Notice. TNC will maintain suppression records as required.

Transactional, security, legal, billing, account, service, recruiting, Event, and active-relationship notices may continue as permitted by law even after a promotional opt-out. Opting out of promotions does not necessarily close the underlying relationship.

24. THIRD-PARTY SITES AND SERVICES

A third-party site or service may have its own privacy practices. This Notice does not control an unrelated third party outside TNC's direction. Participants should review the third party's terms and privacy notice before using it.

TNC evaluates providers appropriate to the function and risk but does not represent that every provider has identical practices or that third-party availability is uninterrupted.

25. CHANGES, NOTICE, AND REACCEPTANCE

TNC may update this Privacy Notice. Material changes must be versioned and presented through the notice, acknowledgment, consent, or reacceptance process required by law, contract, risk, or TNC policy.



A new Notice does not silently rewrite an earlier consent, authorization, audience election, privacy request, or receipt. Prior versions and records remain preserved.

Where a change materially affects a purpose, category, recipient, regulated use, Sensitive Information, automated decisionmaking, retention, transfer, or right, the affected processing must remain blocked or limited until the required notice or authorization is complete.

26. CONTACT

Privacy questions and requests may be submitted through the applicable authenticated portal or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.

CONTACT

Questions may be submitted through the applicable authenticated portal or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.