

1290 WORLD LLC

TWELVE NINETY CONNECTIONS

TNC Privacy Notice

Version 1.1

Document ID	TNC-STD-PRIVACY-2026-08-18-001
Entity	1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections ("TNC")
Audience	All TNC ecosystem participants and site users
Effective Date	Upon valid acceptance after TNC designates this exact version for controlled external use.

This document is part of the TNC Ecosystem Standard Protocol. It must be presented with the exact incorporated versions identified in the acceptance receipt. A visible portal state without a durable receipt is not acceptance.

1. SCOPE AND CONTROLLER

This Privacy Notice explains how TNC collects, uses, discloses, retains, and protects personal information in connection with public websites, accounts, Network Portals, recruiting, services, communications, events, relationship programs, and authorized technology-assisted workflows.

The responsible entity is **1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections (“TNC”)**. An applicable Network term or action instrument may provide additional privacy information for a specific relationship.

This Notice is a disclosure, not a substitute for a separate consent when law requires one.

2. PERSONAL INFORMATION WE MAY COLLECT

Depending on the relationship and function, TNC may collect:

- identity and contact information, including name, preferred name, email, telephone number, address, and time zone;
- account, authentication, verification, device, session, and security information;
- organization, role, title, authority, ownership, billing, and account-administration information;
- professional, education, credential, résumé, work-history, skills, compensation, availability, location, and career-interest information;
- recruiting and relationship information, including jobs, searches, candidate source, communications, interviews, offers, placements, onboarding, guarantee, and follow-up records;
- service, transaction, invoice-reference, payment-status-reference, contract, authorization, receipt, and support information;
- communications, messages, meeting details, notes, attachments, and authorized recordings or transcripts;
- public-profile and professional information from sources the participant or applicable law permits TNC to use;
- website, portal, browser, device, log, cookie, analytics, and interaction information;
- preferences, accessibility requests, language, notification settings, and relationship context;
- information supplied by clients, candidates, partners, references, service providers, or other authorized sources;
- inferences or recommendations derived from authorized information; and
- sensitive information only when necessary, lawfully authorized, and subject to appropriate restrictions.

TNC does not require unnecessary protected-trait, medical, financial-account credential, or government-identifier information. Participants should not upload sensitive information unless TNC specifically requests it through an approved secure channel.

3. SOURCES OF INFORMATION

TNC may receive information:

- directly from the participant or an authorized representative;
- from an organization, client, candidate, partner, reference, or service provider involved in the relationship;
- from public professional sources and lawful research;
- from TNC websites, portals, communications, and technology systems;
- from connected providers the participant or organization authorizes; and
- from source records preserved for provenance, correction, reconciliation, fraud prevention, or audit.

TNC does not silently merge conflicting source values. Source, date, and status should remain distinguishable until validated.

4. PURPOSES OF PROCESSING

TNC may process personal information to:

- create, authenticate, secure, and administer accounts and Network relationships;
- verify identity, organization, authority, eligibility, consent, and source;
- provide recruiting, relationship, portal, services, communications, support, and transaction functions;

- match and route authorized opportunities, candidates, services, and relationships;
- manage searches, submissions, interviews, offers, placements, onboarding, guarantees, and follow-up;
- prepare, deliver, execute, and preserve agreements, notices, authorizations, approvals, receipts, and records;
- communicate account, security, relationship, service, recruiting, billing, legal, support, and promotional information as permitted;
- personalize the participant's experience and maintain context continuity;
- analyze, summarize, compare, classify, retrieve, and improve authorized information and workflows;
- prevent fraud, misuse, duplicate identity, unauthorized access, discrimination, harassment, and operational failure;
- comply with law, enforce agreements, preserve evidence, and respond to lawful requests;
- conduct research, quality assurance, accessibility, security, and product improvement consistent with disclosed purposes; and
- create aggregated, statistical, or de-identified information where appropriate.

TNC will not use personal information for a materially incompatible purpose without an applicable notice, authorization, or legal basis.

5. TECHNOLOGY-ASSISTED PROCESSING AND HUMAN REVIEW

TNC may use technology-assisted tools for research, drafting, summarization, comparison, classification, retrieval, fraud detection, workflow routing, and decision support. TNC remains responsible for appropriate human review of consequential TNC actions.

TNC does not make an employer's final employment decision. TNC will not intentionally use protected characteristics as a substitute for lawful, job-related criteria. Participants may request correction of inaccurate source information and may ask for human review of a material TNC decision where required by law or TNC policy.

6. DISCLOSURES OF PERSONAL INFORMATION

TNC may disclose personal information, subject to purpose, confidentiality, consent, and access controls, to:

- clients, employers, candidates, talent participants, partners, service customers, or World Connections participants involved in an authorized relationship or action;
- hosting, communications, authentication, payment, scheduling, document, security, analytics, and other service providers acting for TNC;
- professional advisers, auditors, insurers, and legal representatives;
- regulators, courts, law enforcement, or other persons when required or permitted by law;
- a successor or transaction participant in a merger, reorganization, financing, or transfer, subject to appropriate protection; and
- the public only as permitted by the Public & Commercial Participation Terms and any separate authorization required for identifiable or restricted material.

TNC does not disclose Candidate Data, confidential searches, private compensation, security credentials, medical information, or restricted communications merely because a general relationship exists.

7. SALE, SHARING, TARGETED ADVERTISING, AND PROFILING

TNC does not intend to sell personal information for money. If a TNC activity is legally treated as a sale, sharing, targeted advertising, or regulated profiling, TNC will provide the notice and choice required by applicable law before or at the time the activity occurs.

TNC does not use a participant's refusal of an optional regulated activity as permission to proceed.

8. COOKIES, ANALYTICS, AND SIMILAR TECHNOLOGIES

TNC may use necessary technologies for authentication, security, preferences, routing, and service operation. TNC may use analytics or measurement technologies to understand use and improve quality.

Before deploying nonessential advertising, cross-site, or similarly regulated tracking, TNC must classify the technology, update the applicable notice, implement required controls, and honor legally required preferences. Browser or device signals are honored where required by applicable law and supported by the released implementation.

9. RETENTION

TNC retains personal information only as reasonably necessary for the disclosed purpose, relationship continuity, contractual obligations, source protection, legal requirements, security, audit, disputes, and records management.

Retention depends on the information category, source authority, relationship status, applicable contract, legal limitation period, consent state, security need, and whether the information remains necessary. TNC may preserve a minimal record of a prior acceptance, transaction, source, correction, opt-out, dispute, or security event after other information is deleted.

A detailed retention schedule and deletion workflow must control production implementation. A participant may request information about applicable retention criteria.

10. SECURITY

TNC uses administrative, technical, and organizational safeguards appropriate to the information and risk. Safeguards may include access controls, authentication, encryption in transit, provider controls, logging, monitoring, backups, secure disposal, incident response, and least-privilege access.

No system is perfectly secure. Participants must protect credentials and promptly report suspected compromise. TNC will provide legally required notices of a qualifying security incident and will not represent an unverified incident state as confirmed.

11. INTERNATIONAL AND CROSS-BORDER PROCESSING

TNC is based in the United States. Information may be processed in the United States or another location where TNC or an authorized provider operates. Before activating a cross-border relationship subject to additional transfer requirements, TNC must implement the applicable notice, agreement, transfer mechanism, or restriction.

12. PRIVACY RIGHTS

Depending on applicable law, a participant may have rights to:

- know or access personal information;
- correct inaccurate information;
- delete information, subject to lawful exceptions;
- obtain a portable copy;
- opt out of sale, sharing, targeted advertising, or regulated profiling;
- limit certain uses of sensitive information;
- withdraw consent where processing depends on consent;
- appeal a denied request; and
- receive equal service and nonretaliation for exercising a right.

TNC may verify identity, authority, and jurisdiction before completing a request. An authorized agent may be required to provide proof of authority. TNC may deny or limit a request where permitted by law, including to protect another person, preserve legal claims, maintain security, or comply with a contract or legal duty. TNC will explain a denial when required.

13. 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 Communications Notice. Transactional, security, legal, billing, and active-relationship notices may continue as permitted by law.

14. RECORDINGS, TRANSCRIPTS, AND MEDIA

Recording or transcription is governed by the Recording & Transcription Notice and applicable just-in-time notice or consent. Identifiable public use of a voice, image, testimonial, or private communication requires the applicable authorization and confidentiality controls.

15. CHILDREN AND MINORS

TNC services are not directed to children under 13. TNC does not knowingly collect personal information from a child under 13 without a lawful basis and required parental authorization. A minor who is permitted to use a TNC function may require a parent, guardian, or authorized representative.

16. 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. TNC evaluates providers appropriate to the function and risk but does not represent that every third-party service has identical practices.

17. CHANGES TO THIS NOTICE

Material changes must be versioned and presented as required by law, contract, risk, or TNC policy. Prior notices, acceptances, and receipts remain preserved. A new notice does not silently rewrite an earlier consent or authorization.

18. CONTACT AND REQUESTS

Privacy questions and requests may be submitted through the authenticated portal or to:

Terrance Sullivan

Founder | Twelve Ninety Connections

Office: (316) 832-7700 ext. 1290

Direct: (702) 670-1290

Email: tsullivan@1290worldconnections.com

The request should state "Privacy Request" and identify the participant, relationship, jurisdiction, and requested action. A dedicated privacy-request address may be designated in the exact release copy or portal.