

Teneo Agent SDK — Public Deployment Rules

Effective: 2025-11-01

Version: 1.0.0

Applies to: All third-party agents built with the Teneo Agent Deployment SDK (the “SDK”) and made available in the Teneo Ecosystem, including the Teneo Chat Room and Data SDK.

Contractual status: These Rules form part of the binding agreement between Teneo Protocol (or relevant affiliate, “Teneo”) and each Agent Developer (“you”). By submitting or enabling an Agent, you accept these Rules.

Plain-English summary: Build safe, lawful, transparent agents; disclose what they do; get affirmative user consent for any data access; respect third-party rights and site terms; ship with strong security; don’t mislead users; and be ready for audits. Deployment is instant upon self-certification. Teneo reserves the right to delist or audit any Agent post-deployment.

1) Definitions

- **Agent:** Any autonomous or semi-autonomous software built with the SDK and deployed to the Teneo Ecosystem.
- **Developer:** The individual or entity that submits, configures, or controls an Agent.
- **User:** Any person or system invoking an Agent through Teneo products or APIs.
- **Sensitive Data:** Includes (without limitation) precise geolocation, financial account numbers, payment card data, government IDs, authentication secrets, private keys, health/biometric data, children’s data, and any data subject to heightened legal protection.
- **High-Risk Domains:** Health/medical, legal advice, financial/investment, biometric identification, surveillance, weapons, critical infrastructure.

2) Eligibility & Self-Certification

- You must be **18+** and not subject to sanctions, export restrictions, or other legal prohibitions.
- All Agents are deployed **permissionlessly** after you self-certify compliance with these Rules.
- By submitting, you confirm that your Agent meets all ethical, technical, and legal criteria herein.
- Teneo reserves the right to **audit, suspend, or delist** Agents that present safety, legal, or performance risks.

3) Ethical & Content Safety

- **No unlawful, violent, or hateful conduct;** no incitement, harassment, or discrimination.

- **No deceptive functionality:** Do not impersonate people or organizations; do not misrepresent capabilities or data provenance.
- **Clear Purpose & Limits:** Your listing must accurately describe functions, data sources, limitations, and where hallucinations may occur.
- **High-Risk Disclaimers:** Agents operating in domains such as finance, law, or health must display appropriate disclaimers (e.g., “not medical/legal/financial advice”).
- **Age-Appropriate Use:** No pornographic or harmful-to-minors content. No collection of children’s data without verifiable parental consent and explicit Teneo approval.

4) Data Privacy & User Consent

- **Lawful Basis:** You must have a lawful basis for all data processing.
- **Consent UX:** Any access to user accounts, private areas, or device resources must use an **explicit, revocable consent flow** separate from general TOS acceptance; default to least privilege.
- **Prohibited Collection:** Do **not** solicit, store, or process Sensitive Data unless your Agent is designed for that purpose and compliant with applicable law.
- **No Credential Harvesting:** Never request or store user passwords, 2FA codes, recovery phrases, or private keys.
- **Data Minimization & Retention:** Collect only what’s necessary; document retention; provide deletion options.
- **Cross-Border Transfers:** Implement safeguards for international data transfers.

5) Third-Party Terms, Rights & IP

- **Respect Platform Terms:** Agents must comply with the terms, policies, and rate limits of any third-party sites or APIs they access. Do not bypass technical restrictions or paywalls.
- **Copyright & Trademarks:** Do not infringe IP; honor takedown requests.
- **Data Provenance:** Maintain verifiable logs or references sufficient to substantiate factual claims and data sources shown to users.

6) Security Requirements

- **Secrets Handling:** Use the SDK’s secret storage; never hard-code keys. Rotate keys regularly.
- **Dependency Hygiene:** Declare dependencies; patch known critical vulnerabilities promptly.
- **Incident Response:** Notify Teneo promptly of any breach or suspected compromise affecting Users or the Ecosystem.

7) Reliability & Safety Controls

- **Operational Quality:** Agents must meet reasonable uptime and latency targets.
- **Guardrails:** Implement content filters, input validation, and safety policies.
- **Abuse Prevention:** Respect throttles and back-off signals from Teneo infrastructure.

8) Transparency & Listing Metadata

Each listing must include:

- Clear **title**, **description**, supported languages, and intended audience.
- **Capabilities & limitations**, expected error modes, and **disclaimer** language (where applicable).
- **Contact or issue-reporting link** (no direct email required).
- **Monetization** terms if any (pricing, revenue share, refunds).

9) Monitoring & Audit

- Teneo may collect operational telemetry for safety and quality.
- Operators must maintain **basic audit logs** of key events.
- Teneo may **audit or delist** Agents retrospectively at its discretion.

10) Monetization & Compliance

- Where Agents earn rewards or payments (including on-chain flows such as x402), Operators are responsible for all applicable **tax, AML, and consumer protection** compliance.
- No money laundering, sanctions evasion, or deceptive billing practices.
- Teneo may request KYC/KYB verification for monetized or high-value Agents.

11) Enforcement & Remedies

- Teneo may take immediate action—including **takedown, suspension, delisting, rate limiting, reward clawbacks, or account termination**—to address safety, legal, or operational risks.
- Operators remain responsible for **their own users and subcontractors**.

12) Liability & Indemnification

- **No Warranties**: Agents are provided “as is.” Teneo disclaims all warranties to the fullest extent permitted by law.
- **Indemnification**: You agree to **defend, indemnify, and hold harmless** Teneo and its affiliates against claims arising from your Agent, data processing, or breach of these Rules.
- **Limitation of Liability**: To the maximum extent permitted by law, Teneo and its affiliates will not be liable for any indirect, incidental, special, consequential, or exemplary damages arising out of or in connection with your use or operation of an Agent. In no event will Teneo’s total aggregate liability for any claim related to your Agent exceed the greater of (a) the amounts paid by you to Teneo (if any) in the twelve months preceding the claim, or (b) one hundred U.S. dollars (USD 100).

Nothing in these Rules limits liability for fraud, willful misconduct, or any liability that cannot legally be excluded.

13) Updates & Acceptance

- Teneo may modify these Rules; material changes will be communicated through official developer channels.
- Continued use or deployment after the effective date constitutes acceptance.