TRIBAL TECHNOLOGY

RFP Addendum:

Data & AI Protection Requirements

A model addendum for sovereign tribal nations issuing RFPs for technology products and services involving data or artificial intelligence.

Provided free of charge by Tribal Technology · tribal-technology.com

HOW TO USE THIS ADDENDUM

Attach this document as a required addendum to any RFP for software, platforms, AI tools, data services, or managed IT. Require vendors to respond in writing to each question. Evaluate responses before scoring proposals. Any red-flag answer should trigger follow-up or disqualification. All responses should be incorporated by reference into the final contract.

These questions cover five protection domains. All apply to AI-heavy systems. For simpler IT purchases, use Sections 1–3 at minimum.

SECTION 1

Data Ownership & Control

These questions establish who legally owns data generated by or entered into the vendor's system, and whether the tribe can access, export, and delete it without vendor interference.

QUESTION 1.1

Who owns the data entered into or generated by your system by tribal users?

Why this matters: Vendors sometimes claim joint ownership or broad licensing rights to data processed by their platform. The tribe must retain sole ownership of all tribal data at all times.

■ **Red-flag answer:** Any answer claiming vendor ownership, co-ownership, or broad licensing rights over tribal data.

QUESTION 1.2

Can the tribe export a complete copy of all its data at any time, in a non-proprietary format, at no cost?

Why this matters: Data portability is essential to sovereignty. Tribes must be able to leave a vendor without losing data.

■ **Red-flag answer:** Export requires vendor assistance, incurs fees, is limited to certain data types, or only available in proprietary formats.

QUESTION 1.3

What happens to tribal data if the contract is terminated — by either party? Provide your data return and deletion timeline.

Why this matters: Tribes need a guaranteed window to retrieve data before deletion, and confirmation it is fully purged from vendor systems.

■ **Red-flag answer:** No defined timeline, vague language like "may retain for operational purposes," or retention periods exceeding 30 days post-termination.

QUESTION 1.4

Does your system store tribal data in a way that allows it to be subpoenaed, audited, or accessed by third parties without tribal consent?

Why this matters: Tribal data stored on vendor infrastructure may be subject to federal or state legal processes. Tribes need to understand this exposure.

■ **Red-flag answer:** Vendor cannot provide a clear answer, or confirms data is subject to third-party access without tribal notification.

SECTION 2

AI & Automated Decision-Making

If the vendor's system uses AI, machine learning, or algorithmic scoring in any form — including recommendations, fraud detection, eligibility screening, or content moderation — these questions apply.

QUESTION 2.1

Does your system use artificial intelligence, machine learning, or algorithmic decision-making in any feature? If yes, describe each use case.

Why this matters: AI is often embedded in features that appear routine — fraud flags, eligibility determinations, document routing. Full disclosure is required to evaluate risk.

■ **Red-flag answer:** Vendor cannot clearly describe where AI is used, or discloses AI use only when pressed.

QUESTION 2.2

Has your AI system been trained on data from tribal nations, Indigenous communities, or federally recognized tribes? If yes, describe the source and whether consent was obtained.

Why this matters: AI trained on tribal data without consent is a direct violation of data sovereignty. This includes models trained on tribal language, health records, or enrollment data.

■ **Red-flag answer:** Yes, without consent — or vendor cannot confirm whether tribal data was used in training.

QUESTION 2.3

Can the tribe opt out of any AI-driven features and still use the core system functionality?

Why this matters: Tribes must retain the ability to decline AI features they have not evaluated or approved, without losing access to the system they purchased.

■ **Red-flag answer:** AI features are inseparable from core functionality, or opting out voids the contract or support agreement.

QUESTION 2.4

When your system makes or influences a decision affecting an individual (eligibility, benefits, flags, scores), is a human review step available?

Why this matters: Automated decisions affecting tribal members must have a human review path. This is both ethical and legally prudent.

■ **Red-flag answer:** No human review is available, or review is only triggered after adverse action has already been taken.

QUESTION 2.5

How do you test your AI systems for bias, particularly against Indigenous populations? Provide your most recent bias audit results.

Why this matters: AI trained on majority-population data frequently performs poorly on Indigenous populations. Vendors must demonstrate they have tested for this.

■ **Red-flag answer:** No bias audits conducted, audits do not include Indigenous subgroups, or results are withheld as proprietary.

SECTION 3

Data Sharing & Third Parties

Vendors routinely share data with subprocessors, analytics partners, and affiliates. These questions surface that network and establish consent requirements.

QUESTION 3.1

Provide a complete list of all third parties — subprocessors, analytics vendors, cloud providers, affiliates — that will have access to tribal data.

Why this matters: Data sovereignty requires knowing exactly who touches tribal data. A vendor's privacy policy often buries this in vague language.

■ **Red-flag answer:** Vendor provides a vague list, refuses to disclose subprocessors, or states the list "changes frequently" without a notification process.

QUESTION 3.2

Will any tribal data be used to train, fine-tune, or improve your AI models, either now or in the future? This includes anonymized or aggregated data.

Why this matters: Anonymized data can often be re-identified, especially in small tribal communities. Tribes must explicitly prohibit use of their data for model training.

■ **Red-flag answer:** Yes, data is used for model improvement — or vendor cannot confirm it is not.

QUESTION 3.3

Does your contract include a provision prohibiting the sale, licensing, or transfer of tribal data to any third party?

Why this matters: Data brokerage is a growing risk. Without an explicit contractual prohibition, tribal data can be sold or transferred as part of a business acquisition.

■ **Red-flag answer:** No such prohibition exists, or it contains carve-outs for "aggregated," "de-identified," or "operational" data.

SECTION 4

Security & Breach Response

Tribal data — especially enrollment, health, and financial records — is high-value. These questions evaluate vendor security maturity and incident response obligations.

QUESTION 4.1

What security certifications does your system hold (SOC 2 Type II, FedRAMP, HIPAA BAA, etc.)? Provide current certification documentation.

Why this matters: Certifications indicate that security controls have been independently verified. Self-attestation is not equivalent.

■ **Red-flag answer:** No independent certifications, certifications are expired, or vendor refuses to provide documentation.

QUESTION 4.2

In the event of a data breach involving tribal data, what is your notification timeline? Who is notified, by what method, and within how many hours?

Why this matters: Tribes need to be notified before the vendor notifies regulators or the public. 72 hours is a common standard; anything longer is a concern.

■ **Red-flag answer:** Notification exceeds 72 hours, tribe is not the first party notified, or breach notification is not contractually guaranteed.

QUESTION 4.3

Where is tribal data stored geographically? Is it stored or processed outside the United States?

Why this matters: Data stored outside the US may be subject to foreign government access. Tribal data should remain on domestic infrastructure unless the tribe explicitly approves otherwise.

■ **Red-flag answer:** Data is stored or processed outside the US, or vendor cannot confirm data residency.

SECTION 5

Sovereignty & Jurisdiction

These questions address the legal and jurisdictional dimensions of the vendor relationship — ensuring tribal law governs the contract and the tribe retains authority to modify or exit.

QUESTION 5.1

Will you accept tribal law as the governing law for this contract, or agree to dispute resolution under a tribal forum?

Why this matters: Vendors typically default to their home state's jurisdiction. Sovereign nations should assert their own legal authority in contracts where possible.

■ **Red-flag answer:** Vendor refuses any tribal jurisdiction and requires disputes to be resolved in their home state only.

QUESTION 5.2

Does your contract include any clause that would require the tribe to waive sovereign immunity?

Why this matters: Sovereign immunity waivers can expose tribal governments to legal liability in non-tribal forums. Any such waiver requires Tribal Council review.

■ **Red-flag answer:** Contract includes a blanket sovereign immunity waiver, or vendor cannot confirm no such language exists.

QUESTION 5.3

If we determine your system poses unacceptable risk to tribal data or sovereignty after deployment, can we terminate the contract immediately without penalty?

Why this matters: Tribes must retain the right to exit a vendor relationship if new information reveals unacceptable risk. Multi-year lock-in without exit rights is a sovereignty concern.

■ **Red-flag answer:** No early termination right exists, or termination triggers significant financial penalties that function as a lock-in.

EVALUATING RESPONSES

A strong vendor response is specific, documented, and willing to be made contractual. Vague answers, references to future roadmap items, or refusals to put commitments in writing are all warning signs. Require that all responses to this addendum be incorporated by reference into the final contract.

Need help evaluating vendor responses or drafting contract language? Contact us at info@tribal-technology.com