

POLICY BRIEF ONE-PAGER – TRANSLATOR CONTRACT TERMS

Scenario

To protect client data security and maintain translation quality, you're thinking of banning your translators from using AI tools.

Response

Fearing that unchecked AI will compromise client data or translation quality is completely understandable, but a blanket "No AI" policy is a strategic dead end.

A ban alienates your most professional, forward-thinking translators who use secure AI tools and methods. Tying their hands while the market demands faster, cheaper results forces them to work below their capabilities. Ultimately, you lose your best talent and degrade your delivered quality—an unsustainable combination.

Worse, blanket bans don't work anyway. They encourage "shadow AI," where vendors secretly use unsecure public tools. Trying to fight this with Big Brother surveillance destroys mutual trust and starts you down the road to blind automation, which is incompatible with your boutique LSP human-first advantages.

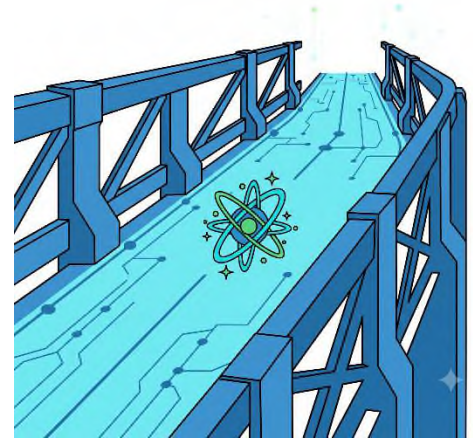
You cannot win with a policy that denies market reality just so you can have a false sense of security. Instead of banning AI, implement a framework that builds trust, boosts productivity, and places the responsibility squarely on the translator to deliver secure, premium work—just as your standard vendor agreements have always done.

Here is a ready-to-use clause you can drop into your contractor agreement today:

Use of Machine Translation and Artificial Intelligence Tools

The Translator may use machine translation and/or artificial intelligence tools in the performance of the services, provided that such use complies with the workflow criteria established by the Client, as outlined below:

1. *The Translator shall not input confidential information (personal data, client source text, or any other proprietary information) into public or consumer-grade AI tools, including free or publicly accessible generative AI platforms (e.g. ChatGPT).*
2. *Prior to delivery, the Translator or other previously agreed professional must thoroughly review, edit, and validate all content generated, translated, or assisted by MT or AI tools to ensure accuracy, fluency, project requirement compliance, and consistency.*
3. *Any AI or MT tool used must operate in a secure environment and demonstrate an adequate level of data security maturity (e.g., ISO 27001, SOC 2 Type II, GDPR compliance). If a tool is locally installed, the Translator shall ensure the host device is protected by up-to-date security software (e.g., antivirus).*
4. *Only AI tools offered under corporate or enterprise (B2B) terms of use, which expressly guarantee data confidentiality and non-retention for training purposes, may be used. Upon request, the Translator must provide a full list of the specific AI and MT tools used.*



Take the AI burden off your translators.

Instead of worrying about which tools your vendors are using, let me power your workflows securely behind the scenes as your **Outsourced LangOps Engineer**. Through my 12-Step **GAIT-Augmented MT & MTPE** process, I deliver machine output that is of such high quality, your translators won't need to retranslate it with other tools. Learn more at:

<https://cotranslatorai.com/langops>

Let's compare notes: Do these contract terms work for you? Do you have a different strategy for this scenario? Email me at sbammel@koreanconsulting.com—I'd love to hear your feedback, pushback, or success stories.

