

CAMBIO TOOL, LLC — DATA PROCESSING ADDENDUM

How we handle, protect, and return Customer Data · Last updated October 30, 2026

Version 1.0 · Effective October 30, 2026 · <https://sign.cambiotool.com/legal/dpa/v/1.0>

This Data Processing Addendum (the "**DPA**") is part of the Cambio Tool Master Services Agreement (the "**MSA**") between Cambio Tool, LLC, a Wisconsin limited liability company ("**Cambio Tool**"), and the customer named on an Order Form ("**Customer**"), and applies to every Order Form under it. If this DPA conflicts with the MSA or an Order Form on how Customer Data is handled, this DPA controls. Each Party's liability under this DPA is subject to the limits in the MSA. Capitalized terms not defined here have the meanings given in the MSA.

PART 1 — TERMS FOR ALL CUSTOMERS

1. DEFINITIONS

"**Personal Information**" means Customer Data that identifies or could reasonably be linked to an individual, including "personal information" under Wis. Stat. § 134.98.

"**Regulated Data**" means Customer Data that is export-controlled under ITAR or EAR, Controlled Unclassified Information ("**CUI**"), or Covered Defense Information under DFARS 252.204-7012.

"**Security Incident**" means a confirmed unauthorized access to, or acquisition, disclosure, alteration, or loss of, Customer Data in Cambio Tool's control. Blocked log-in attempts, port scans, and similar unsuccessful attempts are not Security Incidents.

"**Subprocessor**" means a third party Cambio Tool engages to process Customer Data, listed in Schedule B.

2. OUR ROLE

2.1 Service provider, not a cloud provider. Cambio Tool provides software and managed services: it deploys, configures, operates, and supports the applications Customer uses. It does not own or operate data centers. Hosting, storage, and AI processing are performed by the Subprocessors in Schedule B, for which Cambio Tool remains responsible.

2.2 Customer's data, Customer's instructions. Customer owns and controls Customer Data. Cambio Tool will process it only to provide the Services, as Customer directs, or as the law requires (and will tell Customer first unless the law prohibits it).

2.3 What we will not do. Cambio Tool will not sell or share Personal Information, use Customer Data for any other purpose, combine it with data from other sources, or allow any AI provider to train on it. Where the California Consumer Privacy Act or a similar state law applies, Cambio Tool acts as Customer's "service provider" or "processor" and will meet the obligations that law places on it.

3. ACCESS TO CUSTOMER SYSTEMS

3.1 Read-only. Cambio Tool will only read from Customer Systems. It will never write to, change, or delete data in them.

3.2 Credentials. Customer will issue dedicated credentials limited to what the Services need. Cambio Tool will keep them in a managed secrets vault, use them only for Customer, and follow Customer's reasonable written access policies. Customer may revoke them at any time.

4. WHERE DATA IS KEPT

4.1 Private Deployment Option. Under the Private option, Customer's Services run on a private server dedicated to Customer, in a U.S. region of a hosting provider listed in Schedule B. Customer Data, including backups, stays in the United States, and no one accesses it from outside the United States without Customer's written consent.

4.2 AI providers. Cambio Tool uses only the AI providers in Schedule B, under terms that prohibit training on Customer Data and limit retention to the period stated there.

4.3 No Regulated Data under the Private option. Customer will not send Regulated Data to a Private deployment and will configure its connections to exclude it. If Regulated Data is found there, Cambio Tool may pause processing of it and will work with Customer to delete it or move it to a Government deployment.

5. SUBPROCESSORS

Customer approves the Subprocessors in Schedule B. Each is bound in writing to protect Customer Data at least as well as this DPA. Cambio Tool will email Customer at least thirty (30) days before adding a new Subprocessor. If Customer objects on reasonable data-protection grounds and the parties cannot resolve it, Customer may end the affected Services and receive a refund of prepaid fees for the unused period.

6. SECURITY

Cambio Tool will maintain the security measures in Schedule A and will not materially weaken them during Customer's current term.

7. SECURITY INCIDENTS

7.1 Notice. Cambio Tool will notify Customer of a Security Incident without unreasonable delay and within seventy-two (72) hours after confirming it (see Section 14 for the Government option). The notice will describe what happened, the data affected, the steps taken, and a contact, and Cambio Tool will update Customer as it learns more.

7.2 Response. Cambio Tool will contain and fix the problem and give Customer what it needs to meet its own obligations. Customer decides whether to notify affected individuals under Wis. Stat. § 134.98 or other laws. Cambio Tool will not name Customer publicly without consent unless the law requires it, and notice of an incident is not an admission of fault.

8. REQUESTS FROM INDIVIDUALS AND GOVERNMENTS

Cambio Tool will forward to Customer any request from an individual about their Personal Information and will reasonably help Customer respond. If a government authority demands Customer Data, Cambio Tool will refer it to Customer and notify Customer promptly unless the law prohibits it.

9. SECURITY REVIEWS

Once a year, or after a Security Incident, Customer may send a reasonable security questionnaire, which Cambio Tool will answer within thirty (30) days. An on-site audit is available only if required by law, a regulator, or Customer's government contract, or after a Security Incident the questionnaire does not adequately address; it is limited to once a year, on thirty (30) days' notice, during business hours, at Customer's expense. Audit information is confidential.

10. END OF SERVICE

For thirty (30) days after an Order Form ends, Customer may request an export of its Customer Data and Insights in a commonly used format. Cambio Tool will then delete Customer Data within a further thirty (30) days and certify the deletion in writing on request. Copies in routine backups are deleted on the normal backup cycle and stay protected by this DPA until then.

PART 2 — GOVERNMENT DEPLOYMENT OPTION

Part 2 applies only to Order Forms for the Government Deployment Option, and for those it controls over Part 1.

11. HOW THE GOVERNMENT OPTION WORKS

11.1 Customer owns the enclave. Customer establishes and owns an AWS GovCloud (US) account (the "Enclave") under its own agreement with Amazon Web Services ("AWS"). AWS is Customer's cloud service provider under DFARS 252.204-7012. Cambio Tool installs, operates, and supports the applications inside the Enclave using access Customer grants and can revoke.

11.2 Cambio Tool is an external service provider. For CMMC purposes, Cambio Tool is an external service provider (ESP), not a cloud service provider, under 32 CFR § 170.19. It does not run a cloud service of its own for Regulated Data.

11.3 Regulated Data stays in the Enclave. Cambio Tool will not store or send Regulated Data anywhere outside the Enclave, including its own systems, email, support tickets, code repositories, or test environments.

11.4 AI processing. AI runs on Anthropic Claude models through Amazon Bedrock inside the Enclave, using only model versions AWS has authorized in GovCloud at FedRAMP High and DoD Impact Level 4 or 5 (recorded in writing at kickoff). No Regulated Data goes to commercial cloud regions or to any AI provider directly. If no authorized model remains available, either Party may end the affected Order Form with a refund of prepaid fees for the unused period.

12. CMMC AND NIST SP 800-171

12.1 Shared responsibility. Cambio Tool's services fall within Customer's CMMC assessment scope. Before Regulated Data is loaded, Cambio Tool will deliver a service description and a customer responsibility matrix (summarized in Schedule C) for Customer's System Security Plan, and will implement the NIST SP 800-171 requirements the matrix assigns to it.

12.2 Assessment support. Cambio Tool will support Customer's self-assessment, third-party certification, or government assessment with evidence and personnel. Up to 16 hours a year are included; additional time is billed at Cambio Tool's standard rate.

12.3 Certification and flowdowns. Cambio Tool does not currently hold a CMMC certification. If Customer's contracts require Cambio Tool to hold one or to accept DFARS 252.204-7012 or 252.204-7021, the parties will record that requirement, its timing, and any cost in the Order Form. Customer remains responsible for its own compliance, SPRS submissions, and affirmations.

13. PEOPLE AND EXPORT CONTROL

Only Cambio Tool personnel who are U.S. persons (22 CFR § 120.62), located in the United States, background-checked, and trained in CUI handling will access the Enclave. Access ends the same business day a person leaves or changes roles. Customer determines and marks the export classification of its data; Cambio Tool will not export or release Regulated Data except as Customer directs in writing and the law allows.

14. CYBER INCIDENTS

Cambio Tool will report any cyber incident affecting Regulated Data or the Enclave to Customer within twenty-four (24) hours after discovery, so Customer can meet its own seventy-two (72) hour reporting deadline to the Department of Defense. Cambio Tool will preserve relevant images and logs for at least ninety (90) days, give Customer (and DoD through Customer) access for forensic analysis, and report directly to DoD if the Order Form flows DFARS 252.204-7012 down to Cambio Tool.

15. SUBPROCESSORS AND END OF SERVICE

Other than AWS under Customer's own agreement, no Subprocessor will handle Regulated Data without Customer's written consent. Because Regulated Data stays in Customer's own account, Section 10 applies as follows: on exit, Cambio Tool provides a data export, removes its access, and certifies that it holds no Customer Data. The applications in the Enclave remain Cambio Tool's property; Customer will allow their removal and will not keep using them unless the parties agree on a transition license.

SCHEDULE A — SECURITY MEASURES

Values in brackets to be confirmed before use.

AREA	MEASURE
Separation	A dedicated server or Enclave for each customer; no shared databases.

AREA	MEASURE
Encryption	TLS 1.2+ in transit; AES-256 at rest using the hosting provider's key management service. Government option: FIPS-validated encryption.
Access	Least-privilege, role-based access; multi-factor authentication for all Cambio Tool personnel; Cambio Tool-managed, encrypted devices only; access reviewed quarterly.
User sign-in	Customer's identity provider (Microsoft 365 or Google) where supported.
Logging	Administrative and access logs kept at least 12 months and monitored.
Patching	Critical patches within 14 days; high-severity within 30 days.
Backups	Encrypted, U.S.-only (Government option: within the Enclave), kept 30 days, restore-tested annually.
Development	Code review before release; no Customer Data in development or test environments.
People	Confidentiality agreements; security training at hire and annually; documented incident response plan.

SCHEDULE B — PROCESSING DETAILS AND SUBPROCESSORS

ITEM	DESCRIPTION
Purpose	Read data from Customer Systems and produce reports and AI-assisted insights through the applications Customer uses.
Data	Business and operational records (orders, quotes, production, scheduling, shipping, financials); user account data (names, emails, roles); employee work data (names, shifts, assignments); business contacts at Customer's customers and suppliers. No sensitive personal information unless agreed in writing.
People	Customer's employees, contractors, and users, and contacts at its customers and suppliers.
Duration	The term of each Order Form plus the return and deletion period in Section 10.

SUBPROCESSOR	ENVIRONMENT	SERVICE	LOCATION / AI RETENTION
Vultr	Private	Dedicated server hosting and backups	United States / N/A
Anthropic	Private	AI processing via enterprise API	United States / up to 30 days
Amazon Web Services	Government	GovCloud hosting and Bedrock AI, under Customer's own AWS agreement	AWS GovCloud (US) / per AWS terms

SCHEDULE C — GOVERNMENT OPTION SHARED RESPONSIBILITY SUMMARY

Government option only. A summary; the full customer responsibility matrix delivered under Section 12.1 controls.

AREA	AWS	CAMBIO TOOL	CUSTOMER
Access control	Infrastructure	Roles and least privilege for Cambio Tool staff and apps	Grants and revokes access; manages its users
Identity	Infrastructure	MFA for Cambio Tool staff; app sign-in via Customer's identity provider	Identity provider and MFA for its users
Logging and monitoring	Logging services	Configures and reviews Enclave logs	Owns logs; reviews alerts
Configuration and patching	Infrastructure	Secure baselines, change control, OS and app patching	Approves changes affecting its SSP
Incident response	Cloud provider duties under DFARS 7012	Detection, 24-hour reporting, preservation (Section 14)	Reporting to DoD; overall plan
Personnel	AWS staff	U.S. person, screening, training, offboarding	Its own staff
Physical and media	Data centers and media	Its offices and devices; no CUI off the Enclave	Its facilities and endpoints
Encryption and network	FIPS endpoints, network	FIPS settings, segmentation within the Enclave	Its network boundary and connections
Assessment	FedRAMP authorizations	Matrix, evidence, assessment support	SSP, POA&M, SPRS score, affirmations

SHA-256 of version 1.0 source: a893d35c897f941b4bb56ae48d2a37cd9773620b485dfa2100e0b615e3ed561a