

Please note that these Service-Specific Supplemental Terms will apply to your Avalara Service upon any renewal, upgrade, or Service purchase made on or after September 25, 2026.

These Versori by Avalara Service-Specific Supplemental Terms ("**Versori Terms**") govern Customer's purchase and use of Versori by Avalara. These Versori Terms apply where Versori by Avalara is purchased as an add-on to another Avalara Service. These Versori Terms are in addition to and incorporate by reference the Avalara Service Terms and Conditions located at <https://www.avalara.com/terms> (the "**Terms**"). Any capitalized terms used in these Versori Terms and not defined have the meaning given in the Terms.

1. Definitions.

- a. "Connected System"** means any third-party or Customer-owned application, API, database, or service that Customer integrates with through the Service.
- b. "Connector"** means a software component within the Service that enables connectivity between the Service and a specific Third-Party Application or API endpoint.
- c. "Integration"** means a configured data flow or workflow within the Service that connects two or more applications or systems through one or more Connectors and transformation logic.
- d. "Integration Configurations"** means the Integrations, data mappings, transformation logic, and configurations the Service generates for Customer, whether Avalara creates them or Customer configures them. They do not include Connectors, templates, or other components of general application, which are Avalara Technology however and whenever developed, Customer Data, or Customer Output.
- e. "Project"** means an Integration between two endpoints. Each additional endpoint adds to the number of Projects.
- f. "Tenant"** means an end-customer environment Customer provisions on the Service to serve its own downstream customers.
- g. "Versori Documentation"** means the materials located at <https://docs.versori.com> (or a successor site Avalara may designate). Documentation includes the Versori Documentation.
- h. "Versori Platform"** means the integration platform, Connectors, pre-built integration templates, APIs, webhooks, data transformation logic, and the runtime, together with all know-how and learnings about how third-party systems and APIs operate. Avalara Technology includes the Versori Platform.

2. The Services.

- a. Customer Responsibilities.** In addition to Customer's responsibilities in the Terms, Customer will only configure credentials, API keys, and similar access data that Customer is authorized to use and remains responsible for those credentials and for the systems they access. Customer will obtain and maintain all rights, consents, and permissions necessary for Customer Data to be accessed, transformed, and delivered through the Service. Customer will validate that each Integration Configuration produces the intended results before deploying it to production. Customer is responsible for its Tenants' use of the Service as though it were Customer's own, and will impose terms on its Tenants that are at least as protective of Avalara as the Agreement.
- b. Additional Restrictions.** In addition to the restrictions in the Terms, Customer will not use the Service to build a competing product or service, or to serve Tenants beyond the capacity set out in the Order Document.

3. Usage and Rework.

- a. Usage.** Customer must subscribe to each Avalara Service that an Integration connects to. Usage of the Service is calculated under, and counts against Customer's usage tier for, that Avalara Service as set out in its Service-Specific Supplemental Terms. The Service does not have a separate usage tier.

b. Rework. The subscription fee does not cover rework or additional development needed because a Connected System or other third party changed its API. Avalara may provide that work as a chargeable change request or additional Project at Avalara's then-current rates.

4. Data Processing Agreement. The DPA governs Avalara's processing of Personal Information in connection with the Service. For the Service, Exhibit A replaces the DPA's technical and organizational measures, Exhibit B replaces the DPA's description of transfer, and Exhibit C supplements the DPA's list of subprocessors wherever referenced. Avalara may update Exhibit A as provided in the DPA. The DPA is modified so that Avalara's obligations under it do not extend to Customer Data that Customer submits in breach of Section 6(d). The DPA is not otherwise modified.

5. Proprietary Rights.

a. Ownership. As between the parties, Avalara owns Avalara Technology and the Integration Configurations, including all improvements and derivative works.

b. Customer's License. Avalara grants Customer a perpetual, nonexclusive, nontransferable, worldwide license to use, copy, and modify the Integration Configurations for Customer's business, including after the Agreement ends. Customer may run them on another runtime and is responsible for any rework that takes. Customer's license covers any Avalara Technology contained in what Customer exports, solely for use with the exported Integration Configurations, but gives Customer no other rights in Avalara Technology. Customer's right to access and use Avalara's runtime ends when the Subscription Term for the Service ends. Avalara's warranties and indemnification obligations under the Terms stop applying to an Integration Configuration once Customer modifies it or runs it outside the Service.

c. Copy on Termination. If Customer asks within 60 days after a Project ends, Avalara will give Customer a readable copy of that Project's Integration Configurations. Avalara does not promise the copy will run outside the Service and does not have to provide source code for Avalara Technology, migration services, or support.

d. Know-How. Avalara owns the know-how and learnings from Customer's use of the Service, from inputs Customer provides, and from Avalara's support of Customer, and may use them to improve and train the Service, including Avalara's own agents, skills, and models. Avalara may reuse Avalara Technology for any customer or purpose.

e. No Warranty of Title. Avalara does not warrant title in, or the validity or enforceability of, any Integration Configuration. If an Integration Configuration is not protected by any Intellectual Property right, Avalara will not assert one against Customer's use of it.

f. Customer Information and Materials. Avalara claims no ownership of Customer's business rules, processes, or requirements, or of anything Customer or a third party engaged by Customer builds outside the Service. Where an Integration Configuration reveals Customer's non-public business information, that information is Customer's Confidential Information under the Terms and the parties treat it as disclosed by Customer. Avalara's rights under Section 5(d) do not let Avalara give another customer the business rules, logic, or data in Customer's Integration Configurations. Work Avalara does for others that is similar to Customer's Integration Configurations is not a breach of the Agreement.

6. Connected Systems; Deviations from the Terms.

a. Disclaimer. Without limiting the disclaimer of implied warranties in the Terms, Avalara does not warrant that an Integration Configuration will be compatible with any third-party application, system, or service, that any Third-Party Application or Connected System API will remain available, that a Connector will stay compatible with future versions of a Third-Party Application, or the accuracy or completeness of data transformations beyond correct execution of the transformation logic Customer configured. Customer is responsible for compatibility with the systems its Integration Configurations interact with.

b. Availability. For purposes of Avalara's availability obligations under the Terms, an outage or API change at a Third-Party Application or Connected System is a circumstance beyond Avalara's reasonable control. If a Connected System provider changes its API so that a Connector can no longer function, Avalara will use commercially reasonable efforts to update the Connector, and

Section 3(b) (Rework) governs the fees for that work. Avalara owes no credit, refund, or other financial remedy for disruptions caused by third-party API changes.

c. Third-Party Claims. Avalara's indemnification obligations under the Terms do not cover any claim by a third party, including a Connected System provider or a counterparty of Customer, based on an error in the availability, accuracy, or timeliness of any Integration or data transformation the Service processes.

d. Prohibited Customer Data. Customer will not submit to the Service any special categories of personal data, or data relating to criminal convictions or offences, as those terms are used in applicable data protection law, or any payment card data, government-issued identification numbers, or biometric data. Avalara's data protection, security, and breach notification obligations do not apply to, and Avalara is not liable for, any claim, loss, or incident arising from Customer Data that Customer submits in breach of Section 2(a), this Section 6(d), or the restrictions on Customer Data in the Terms.

Exhibit A – Technical and Organizational Measures

Technical and Organisational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Avalara uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and the Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	The Agreement between the Customer and Avalara contains strict confidentiality obligations. Additionally, Avalara requires all subprocessors to follow substantially similar processes and controls, which shall be verified by either (i) a signed agreement; or (ii) receipt of a declaration of compliance issued by an independent entity authorised by a standardising body such as, but not limited to, a SOC 2 Type II report. Avalara has undergone a SOC 2 Type II audit that requires compliance to the Security Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily, weekly and monthly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Avalara has undergone a SOC 2 Type II audit that requires compliance to the Security Trust Service Criteria. Avalara uses secure access protocols & processes and follows industry best-practices for authentication, including Multi Factor Authentication and Single Sign On (SSO). All

Measures for user identification and authorisation	production access requires the use of two-factor authentication. Network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services, and unauthorised network traffic.
Measures for the protection of data during transmission	Avalara has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Avalara only uses recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)
Measures for the protection of data during storage	Encryption-at-rest is automated using GCP's "Default encryption at rest", which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by GCP. https://cloud.google.com/docs/security/encryption/default-encryption
Measures for ensuring physical security of locations at which personal data are processed	All Avalara processing occurs in physical data centres that are managed by GCP. https://cloud.google.com/trust-center/security
Measures for ensuring events logging	Avalara monitors access to applications, tools, and resources that process or store the Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Avalara adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Avalara maintains a set of controls and policies in line with SOC 2 Type II, which includes administrative, organisational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of the Customer Data.

Measures for certification/assurance of processes and products Measures for ensuring data minimisation	Avalara undergoes annual SOC 2 Type II audits. Avalara's customers unilaterally determine what data they route through the Services. As such, Avalara operates on a shared responsibility model. Avalara gives Customer control over exactly what data enters the platform. Additionally, Avalara has built in self-service functionality to the Services that allows the customers to delete and suppress data at their discretion.
Measures for ensuring data quality	Avalara has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) API design and strong typing to enforce a strict contract between official clients and API services. Avalara applies these measures across the board, both to ensure the quality of any usage data that Avalara collects and to ensure that Avalara's software services are operating within expected parameters. Avalara ensures that data quality is maintained from the time a customer sends/the data is pulled into the platform until the customer data is presented or exported.
Measures for ensuring limited data retention	Avalara's customers unilaterally determine what data they route through the Services. As such, Avalara operates on a shared responsibility model. If a customer is unable to delete personal data via self-service functionality, then Avalara deletes such personal data upon the customer's written request, within the timeframe specified in the DPA and in accordance with applicable data protection law. All personal data is deleted from the Services following service termination.
Measures for ensuring accountability	Avalara has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting personal data breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, Avalara conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	Personal data submitted to the Services by the customer may be deleted by the customer or at the customer's request. Personal data is incidental to Avalara's Services. Based on Privacy by Design and Data Minimization principles, Avalara severely limits the instances of personal data collection and processing within the Services. Most use cases for porting personal data from Avalara are not applicable. However, Avalara will respond to all requests for data porting in order to address the Customer needs.

Technical and organisational measures of sub-processors	Avalara enters into Data Processing Agreements with its subprocessors with data protection obligations substantially similar to those contained in the DPA.
--	---

Exhibit B – Details of Processing

Annex I category	1. Platform Access & Accounts	2. AI Build & Design	3. System Connection & Credentials	4. Integration Execution (data flow)	5. Monitoring, Logs & Support
Categories of data subjects	Customer's authorised users (employees, contractors, agents)	Customer's users writing prompts; individuals referenced in example/config data	Customer's users; system/service accounts	End customers' individual customers; individuals in connected systems (contacts, employees, message/call participants)	Customer's users; individuals appearing in log/error data
Categories of personal data	Names, emails, job titles, sign-in identity, org membership	Prompts, requirements, example/config data, generated code & assets (may contain personal data)	API keys, OAuth tokens, usernames, connection endpoints	Integration payloads (contact, order/transaction, message/ticket content); KV-store identifier mappings; vector embeddings; prompt/response data sent to LLMs	IP addresses, activity & system logs, telemetry, error diagnostics
Sensitive data (+ safeguards)	None	None	None	Could incidentally include special-category data depending on Customer's Connected Systems; prohibited categories per Section 6(d) of the Versori Terms; per-org namespace isolation and access controls apply	None
Frequency of transfer	Continuous, as initiated by the customer's use	Continuous, when the customer prompts the AI	On connection setup and each authenticated request	Continuous — each workflow run, webhook, or scheduled job	Continuous, generated automatically during operation

Nature of processing	Authentication, account & organisation management	AI-assisted integration design and code generation (incl. RAG over embeddings and third-party LLM calls)	Secure storage and use of connection credentials	Transfer and transformation of data between connected systems; durable workflow execution; short-term persistence	Logging, tracing, performance monitoring, automated error diagnosis
Purpose	Provide access to the Services per Customer instructions	Help the Customer build and maintain integrations	Enable secure connectivity to the Customer's systems	Run the Customer's integrations as configured	Keep the Services running, secure, and supportable
Retention period	Duration of the account	Build artefacts for the project's life; LLM prompt data ~30 days at provider	Duration of the connection	Integration data auto-deleted after 30 days; KV state & embeddings exist independently of a Project and are deletable by the Customer at any time or on termination	Monitoring data (logs, metrics) retained 30 days

Exhibit C – Subprocessors

Supplemental subprocessors for the Service are listed at <https://trust.versori.com/subprocessors>.