Last updated February 14, 2023

This DPA is incorporated into the Contract between Avalara, Inc. (“Avalara” or “us” or “our”) and Customer. If a provision of this Avalara, Inc. Services Data Processing Agreement (“DPA”) conflicts with a provision of the Contract, the provision in this DPA governs. Capitalized terms used and not otherwise defined in this DPA have the meanings provided in the Contract.

1. Except as amended by this DPA, the Contract will remain in full force and effect.
2. To the extent that the terms of this DPA and the Contract conflict, the terms of this DPA prevail.
3. This DPA will automatically expire on the termination or expiration of the Contract.

Avalara serves enterprises, public sector entities and other organizations (“Customer”) and protects Services Data in compliance with the terms of this DPA. Services Data means personal data relating to named or identifiable individuals that Customer’s authorized users (“Authorized Users”) provide in compliance with applicable law and our applicable service agreements or other commercial contract terms (“Contract”) when Customer uses our service offerings and related data processing services as described in our data sheets, service specifications, and other technical documentation, as amended from time to time (“Services”).

1. Control and Ownership. Customer owns and controls all Services Data. Avalara does not use Services Data, except: (a) in the interest and on behalf of Customer; (b) as necessary to provide the Services, or (c) as contemplated or directed by the Contract. Avalara returns or deletes Services Data at Customer’s request, as agreed in the Contract, or after the Contract expires or is terminated, subject to applicable law.

2. Security. Avalara applies technical, administrative and organizational data security measures that meet or exceed the requirements described in Avalara’s Technical and Organisational Measures in Exhibit 1, Annex II (“TOMs”). Avalara may update and modify its TOMs from time to time, provided that Avalara must not reduce the level of security provided thereunder, except with Customer’s consent or with 90 days prior written notice.

3. Cooperation with Compliance Obligations. At Customer’s reasonable request, Avalara will (a) reasonably assist Customer with data access, deletion, portability and other requests, subject to compensation for any custom efforts required of Avalara, and (b) enter into additional contractual agreements to meet specific requirements that are imposed by mandatory laws on Customer pertaining to Services Data and that, due to their nature, can only be satisfied by Avalara in its role as service provider or that Customer specifically explains and assigns to Avalara in an addendum or amendment to the applicable Contract, subject to additional cost reimbursement or fees as appropriate. If Customer can no longer legally use Avalara’s products due to changes in law or technology, Avalara shall allow Customer to terminate certain or all contracts and provide transition or migration assistance as reasonably required, subject to termination charges and fees as mutually agreed in good faith by the parties.

4. Submit to Audits. Avalara submits to reasonable data security and privacy compliance audits subject to reasonable precautions and safeguards for the data of other customers.

5. Notify Breaches. Avalara notifies Customer of unauthorized access to Services Data and other security breaches as required by applicable law.

6. No Information Selling or Sharing for Cross-Context Behavioral Advertising. Avalara does not accept or disclose any Services Data as consideration for any payments, services or other items of value. Avalara does not sell or share any Services Data, as the terms “sell” and “share” are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act (“CCPA”). Avalara processes Services Data only for the business purposes specified in the written Contract. Avalara does not retain, use, or disclose Services Data (a) for cross-context behavioral advertising, or (b) outside the direct business relationship with the Customer. Avalara does not combine Services Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA.

7. Personal Data subject to the GDPR or similar laws: With respect to any Services Data that is subject to the EU General Data Protection Regulation (GDPR) or similar laws of other countries as "personal data," Avalara accepts the following obligations as a data importer, processor or sub-processor of Customer and warrants that Avalara:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or EU Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32 of the GDPR (security of processing);
(d) respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controller's obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects)
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

8. EU Standard Contractual Clauses: For Services Data that is subject to the GDPR, Avalara complies with the EU Standard Contractual Clauses for international transfers in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (EU SCCs) for the transfer of personal data outside the European Economic Area (EEA), Modules 1-3 as noted below, in Exhibit 1. Under such EU SCCs, Customer will act as data exporter. Customer may be based within or outside the EEA. Customer may receive personal data from the EEA as a controller and as a processor under separate agreements. Avalara is based outside the EEA, acts as data importer, provides services to data exporter under separate commercial agreement(s) and agrees to the EU SCCs as a processor or sub-processor under Modules 2 and 3. Data exporter will provide all relevant instructions under Module 2 (as the controller) and under Module 3 (on the controller's behalf). Customer instruct Avalara to provide Avalara's standard services as described in Avalara's commercial terms and service descriptions. For limited business contact information concerning individual representatives who provide instructions to Avalara, Avalara agrees to the EU SCCs as a controller under Module 1.

9. Switzerland: For transfers of Services Data from Switzerland, Avalara agrees to the EU SCCs as set out in Section 8 subject to the following amendments: The Federal Data Protection and Information Commissioner is the competent supervisory authority in so far as the data transfer falls under Swiss law. Switzerland is also to be considered as a Member State within the meaning of the EU SCCs so that data subjects can file claims according to clause 18c of the EU SCCs at their habitual residence in Switzerland. Until the revised Swiss Federal Act on Data Protection enters into force that does no longer protect data of legal persons but only data of natural persons, the EU SCCs also applies to data of legal persons.

10. United Kingdom: With respect to transfers of Services Data from the United Kingdom of Great Britain and Northern Ireland to countries not deemed to have adequate data protection regimes under all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the United Kingdom of Great Britain and Northern Ireland, Avalara agrees to the EU SCCs as set out in Section 8 and the International Data Transfer Addendum to the EU SCCs in Exhibit 2. Any conflicts between the EU SCCs and the International Data Transfer Addendum to the EU SCCs shall be resolved as provided in the International Data Transfer Addendum to the EU SCCs.

11. Integration. This DPA is binding after a Contract has been signed between Avalara and Customer, and Customer may collect a signed copy of this DPA at here or

https://avalara.na1.echosign.com/public/esignWidget?wid=CBFCIBAA3AAABLblqZhD8qGCX455w96VKreWqVy5W0RbQ_E1XtKdKuZpn1hVkh8z3XJDKKePI-McnHEXenqA*. This DPA shall not create third party beneficiary rights. Avalara does not accept or submit to additional requirements relating to Services Data, except as specifically and expressly agreed in writing with explicit reference to the Contract and this DPA.

12. Notice. Avalara shall provide Customer with legal notices in writing by email, mail, or courier to the address provided by Customer. Except as otherwise specified in the Agreement, all notices to Avalara must be in writing and sent as follows:

Email: DataPrivacy@avalara.com
Attn: Legal Department
Avalara, Inc.
Suite 1800
255 South King Street
Seattle, WA 98104, USA

EXHIBIT 1:

STANDARD CONTRACTUAL CLAUSES

The EU SCCs, modules 1-3, available at Standard Contractual Clauses (SCC) | European Commission (europa.eu) or on a successor website designated by the EU commission, are incorporated herein by reference. Customer will provide all instructions under these EU SCCs as the controller and on the controller's behalf.

Where the EU SCCs require that the parties make an election, the parties make the elections reflected below. Any optional clauses in the EU SCCs not expressly selected below are omitted from this DPA.

1. for purposes of Clause 9 of the EU SCCs, Option 2 ('General authorization') shall apply and Avalara shall inform customer in writing of any intended changes to sub-processors at least 30 days in advance;
2. in Clause 11 (a) of the EU SCCs, the optional language shall be deleted; and
3. for purposes of Clause 17 and Clause 18 of the EU SCCs, the Member State for purposes of governing law, forum and jurisdiction shall be Luxembourg.

Annex I

A. LIST OF PARTIES

For purposes of Annex 1.A (List of Parties) of the EU SCCs: (i) Avalara processes personal data to provide Services to Customer and Avalara shall be the 'data importer'; and (ii) Customer shall be the 'data exporter'. Avalara can be contacted through the Avalara Global Privacy Office at dataprivacy@avalara.com. Customer provides personal data to Avalara to obtain Avalara's Services and can be contacted through the contact information provided by Customer to Avalara.

B. DESCRIPTION OF TRANSFER

For the details of the processing of personal data required for Annex 1.B of the EU SCCs, see below:

MODULE ONE: **Transfer controller to controller**

Categories of data subjects whose personal data is transferred

Individual employees and representatives of data exporter who instruct data importer, send purchase orders, process invoices, arrange for payment, make support calls, use data importer's services, and otherwise do business with data importer.

Categories of personal data transferred

Business contact information, service usage, payment status and other information relating to how data exporter uses data importer's services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

Sensitive data is not transferred on a controller-to-controller basis.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous as initiated by customer in each case as part of each tax or regulatory audit period during which customer contracts for Avalara's Services.

Nature of the processing

Data importer uses data as a controller to do business with data exporter, sell services, issue invoices, provide technical support, perform services, address customer questions, improve services and develop new services and offerings.

Purpose(s) of the data transfer and further processing

Communications and business collaboration between data exporter and data importer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the term of the contract and so long as data importer markets additional services to data exporter.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Same as above.

MODULE TWO AND THREE: **Transfer controller and processor to processor**

Categories	Tax Calculation	Return Preparation	Tax Identification Registration	Fiscal Representation	D
Categories of data subjects whose personal data is transferred	Customer's customers	Customer if it is a sole traders/proprietor using personal contact information for its business; Customer's Authorized Users	Customer's owners and directors	Customer's owners and directors	
Categories of personal data transferred	Delivery addresses, tax identifiers for sole traders/proprietorships, names, access credentials	Tax identifier for sole traders/proprietorship, names and contact details, access credentials for Authorized Users	Names and contact details of owners and directors as required by regulatory authorities, including proof of identification and date of birth	Names and contact details, proof of identification, tax identifiers for sole traders/proprietorships	
Sensitive data transferred (if	None	None	Passport images, which could	Passport images, which could include racial, ethnic, or	

applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.			include racial, ethnic, or religious information; access to data is subject to roles-based access controls	religious information; access to data is subject to roles-based access controls
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous as initiated by customer in each case as part of each tax or regulatory audit perio customer contracts for Avalara's Services.			
Nature of the processing	Calculating various types of tax	Preparing and filing tax returns	Registering Customer to collect and remit various tax types	Providing Fiscal Representation services
Purpose(s) of the data transfer and further processing	Assist Customer in complying with tax obligations	Assist Customer in complying with tax obligations	Assist Customer in complying with tax obligations	Assist Customer in complying with tax and financial obligations

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Unless deletion is requested by the controller, the data will be processed until the end of appl audit periods.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Processor uses subprocessors for certain hosting, support, logging, monitoring, warehousing analytics purposes

C. COMPETENT SUPERVISORY AUTHORITY

For purposes of Clause 13 and Annex 1.C of the EU SCCs, where no competent supervisory authority is identified through the rules of such Clause 13, the competent supervisory authority is the authority in Luxembourg.

Annex II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

For the purposes of Annex 2 of the EU SCCs, the technical and organizational measures implemented by Avalara are as described below.

Avalara maintains the following technical and organization measures:

1. Avalara maintains a written security program under which Avalara periodically evaluates risks to Customer Data and maintains commercially reasonable technical, and physical safeguards to protect Customer Data against accidental or unauthorized access, disclosure, loss, destruction, or alteration. Avalara regularly evaluates the scope and coverage of the Security Program.
2. Avalara teams classify and handle data using technical controls described below to ensure its integrity, availability, and confidentiality.
3. Avalara maintains a central inventory of assets where the asset custodian is responsible for classifying and maintaining the asset and ensuring the use of the asset complies with the security program.
4. Avalara maintains standards for user authentication, access provisioning, de-provisioning, performing periodic access reviews and restricting administrative access to ensure access is granted based on the principle of least privilege.
5. Avalara maintains standards for segregation of network services and devices to ensure unrelated portions of the network are isolated from each other.
6. Avalara maintains network zones and applies ingress and egress standards for the protection of

data.

7. Avalara systems encrypt data at rest and in transit between the Avalara networks and its customers to ensure integrity, security, and confidentiality of customer data.
8. Avalara maintains processes to securely generate, store and manage encryption keys that prevent loss, theft, or compromise.
9. Avalara maintains physical access controls to restrict entry to Avalara facilities. Physical controls may include badge readers, security personnel, staff supervision, video cameras, and other tools.
10. Avalara maintains processes for retaining and securely deleting data no longer than necessary to provide its services.
11. Direct database access is restricted using the corporate VPN. This can only be accessed via Avalara issued computing equipment.
12. Avalara has disabled the ability to write data to USB mass storage devices on all Avalara issued computing equipment.
13. Avalara maintains a Software Management Standard that defines software and services which are approved, acceptable, or prohibited to be used by Avalara personnel.
14. Avalara monitors its applications and systems for vulnerabilities on a periodic basis. Identified vulnerabilities are remediated by taking actions to close them in a timely manner.
15. Avalara maintains an incident response program to detect, analyze, prioritize, and handle cyber security events and incidents to prevent, detect, and deter the unauthorized access, loss, compromise, disclosure, modification, or destruction of Avalara's electronic data assets and information, including personal information.
16. Avalara performs root cause analyses for incidents based on the nature of the incident, to identify, document, and eliminate the cause of an incident and to prevent the issue from recurring. Changes to the Avalara Incident Response Plan and standard operating procedures is also part of this review.
17. Security and audit logs are fed to the SIEM daily and retained for a period of one year. These logs cannot be modified by anyone.
18. Daily recoverable backups of critical data are configured to be performed and replicated to a secondary location.
19. Avalara maintains a Security Infraction Management Policy that describes how Avalara treats security incidents that result from deviations from Avalara's security policies, standards, and procedures.
20. Avalara maintains standards for making changes to applications, including customer-facing applications, by ensuring they are tested and approved by appropriate individuals before they are moved to production. Access to make production changes is restricted to authorized individuals.
21. Avalara has established logical separation between production and lower environments.
22. Avalara ensures test data is selected and handled in accordance with the technical controls specified in this document.
23. All Avalara personnel must undergo the mandatory security awareness training at least annually.
24. The Avalara Service Terms and Conditions along with the Vendor Security terms document are in place to communicate security commitments with vendors.
25. The Avalara Security team periodically performs assessments of different systems by conducting phishing simulations, vulnerability scans, and penetration tests.
26. The Avalara Compliance team periodically performs assessments of key systems. Remediation plans are defined as appropriate for the areas of non-compliance establishing clear ownership and

accountability.

27. The Avalara Risk Management Team periodically conducts risk assessments to identify risks arising from internal and external sources throughout the year to evaluate the organization's control environment. Risk treatment plans are defined, as appropriate, for identified risks including establishing clear ownership and accountability. Risks are monitored to acceptable mitigation according to the Avalara Security Risk Assessment Standard and Process.

28. Avalara maintains standards for Vendor Risk Management to define requirements for vendor selection, risk assessments with roles and responsibilities, contract lifecycle, exception handling and terminations.

Annex III

LIST OF SUB-PROCESSORS

MODULE TWO: **Transfer controller to processor**

MODULE THREE: **Transfer processor to processor**

The controller has provided general authorisation for the engagement of subprocessors from an agreed list, available at Subprocessors (avalara.com).

Exhibit 2

The International Data Transfer Addendum to the EU SCCs ("UK addendum"), available at International data transfer agreement and guidance | ICO or on a successor website designated by the UK ICO, are incorporated herein by reference.

The parties are as reflected in the signature block to this DPA.

The parties select the version of the approved EU SCCs referenced in section 8 of this DPA including the appendix information which is as described in Exhibit 1.

The appendix information in table 3 of the UK addendum is as set out in the annexes to the EU SCCs in Exhibit 1.

The list of sub processors is as provided at Subprocessors (avalara.com).

Either party may end the UK addendum as set out in section 19 of the same.