Last updated August 8, 2022

This DPA is incorporated into the Contract between Avalara Europe Ltd. ("***Avalara***" or "***us***" or "***our***") and Customer. If a provision of this Avalara Europe Ltd. Services Data Processing Agreement ("***DPA***") conflicts with a provision of the Contract, the provision in this DPA governs. Capitalised 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 organisations ("***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 authorised users ("***Authorised 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.

2. Security. Avalara applies technical, administrative and organisational data security measures that meet or exceed the requirements described in Exhibit 1 ("***Security***"). Avalara may update and modify Exhibit 1 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 unauthorised 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. 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=CBFCIBAA3AAABLblqZhB05c1e2iTcpxkELW8vTvPqk4U8ZyPEAzxTu9ldh7un3AHSdm8-TmV9ovhX8SMAjac. 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.

9. 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 Europe Ltd.
Lanchester House
3rd Floor
Trafalgar Place
Brighton BN1 4FU
United Kingdom

EXHIBIT 1: SECURITY

Avalara maintains the following technical and organisation 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 unauthorised 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, analyse, prioritise, and handle cyber security events and incidents to prevent, detect, and deter the unauthorised 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 authorised 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 organisation'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.