AVALARA
NOTICE ON RECRUITMENT/ONBOARDING DATA PROCESSING
UNITED STATES

This Notice describes the practices of the Avalara Group company to which you are applying ("**we**" or the "**Company**"), as a data controller, with respect to the processing (such as collection, use, storage, disclosure, or erasure) of personal data that is obtained through the recruitment process and, if you are hired, the onboarding process that takes place before your employment begins ("**Personal Data**"). This Notice covers all employment candidates of Avalara, Inc., its affiliated companies, and its private equity sponsor and affiliated companies (collectively, "**Avalara Group**") and applies to you if you are a resident of the United States.

I. Categories of Personal Data

We process non-sensitive Personal Data ("**Candidate Data**") and, to the extent you provide it, certain special categories of Personal Data ("**Sensitive Candidate Data**"), to the extent required and permitted under applicable law.

We process the following Candidate Data:

- Name, address, e-mail, phone number ("**Basic Contact Data**");
- Passport, national ID or social security number, tax ID, citizenship, date of birth, birth country/location, gender, work permit and visa information, travel-related information, expense data, emergency contact information, driver's license information, bank account information to set up payroll, contributions to health insurance and pension, marital status, number of children, and similar data ("**Human Resources Data**");
- Information contained in your resume/CV, your responses to screening questions or other submissions, educational information, employment history, job qualifications, skills and experience, reference checks, background checks, training and skills checks or samples, language skills, information provided or generated by interviewers, recruiters and references, and similar data ("**Background Data**");
- Information regarding your access and use of Avalara Group facilities and computer systems, such as your username, IP address, emails, and other electronic communications, documents, files, websites accessed and log files on Avalara computer systems, security badge information, and camera and video images and recordings ("**Security and Access Control Data**").

In addition, we process the following self-reported Sensitive Candidate Data:

- Information about any disability for which the Company would need to make a reasonable adjustment during the recruitment process or during employment; and
- Health information/certificate (if required to be collected).

II. Processing Purposes

We process your Personal Data to the extent permitted or required under applicable law for the following purposes:

- Administering the recruiting process and assessing your suitability for the role for which you are applying or other roles (including setting up a job applicant HR file, managing your

application, conducting assessments, organizing interviews, arranging or reimbursing for your travel and accommodations, processing interview feedback, and conducting background checks and screening); engaging in an equal opportunity monitoring and diversity initiatives; performing analyses to better understand our applicant pool; and onboarding you as an employee, if you are hired ("**Recruiting-Related Purposes**");

- Complying with applicable employment-related laws and requirements and administration of those requirements ("**Regulatory-Related Purposes**");

- Administer and maintain the Company's operations, including for safety purposes ("**Safety Purposes**");

- Conducting internal audits and workplace investigations, and investigating and enforcing compliance with any potential breaches of Company policies and procedures ("**Investigation and Audit Purposes**");

- Facilitating and managing security and access control regarding Avalara Group offices and premises, equipment, and systems, including security activities ("**Security and Access Control Purposes**"); and

- Supporting any claim or defense that the Avalara Group could face before any jurisdictional and/or administrative authority, arbitration, or mediation panel, and cooperating with – or informing – law enforcement or regulatory authorities to the extent required by law ("**Litigation-Related Purposes**").

In addition to the above, if you are hired by the Company as an employee, we also process your Personal Data collected during the application and onboarding process to the extent permitted or required under applicable law for the following purposes:

- Managing your employment relationship with the Company (including onboarding processes, timekeeping, payroll, and expense report administration, employee benefits administration, employee training and development requirements, the creation, maintenance, and security of your online employee accounts, reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill, workers' compensation claims management, employee job performance, including goals and performance reviews, promotions, discipline, and termination, and other human resources purposes) ("**HR Purposes**");

- Performing workforce analytics, data analytics, and benchmarking ("**Analytics Purposes**");

- Marketing to existing or future clients ("**Client Marketing Purposes**");

- Maintaining commercial insurance policies and coverages, including for workers' compensation and other liability insurance ("**Insurance Purposes**"); and

- Engaging in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company ("**Corporate Transaction Purposes**").

III. Data Transfers, Recipients, and Legal Justification for Such Transfers

We share your information internally within the Company. In addition, we transfer your Personal Data in accordance with applicable law to the Avalara Group entities and third parties (e.g., service providers, governmental authorities, and external advisors).

1. External Recipients of your Personal Data

Other Avalara Group companies: In some cases, it is necessary to share Candidate Data that was collected locally within the Avalara Group. We do so to facilitate internal communication and task management to other group companies, group-wide HR planning, and administration in connection with the group's global matrix structure and to be able to fulfill the employment relationship within our global structure. Access to Candidate Data is provided only on a need-to-know basis and subject to an access concept.

In particular, Personal Data may be shared with the following Avalara Group companies:

- Avalara, Inc. (US) and Avalara Europe Ltd. (UK) for the purposes mentioned above, as various senior managers and HR functions for the Avalara Group entities in the EEA, are located in these entities; and

- Avalara, Inc. (US), Avalara Europe Ltd. (UK), and other shared services entities for the provision of shared services, for example, for data hosting and IT services, application-processing and onboarding support, travel-expense management, IT support and maintenance.

- The Avalara Group's private equity sponsor, Vista Equity Partners (US), and its affiliates, including Vista Consulting Group (US) (collectively, "**Vista**"), for administration, research, database development, workforce analytics and business operation purposes. See *Notice Regarding Vista* below.

Benefits Providers, Insurance Carriers, Professional Advisors: Benefits providers (such as payroll processors or pension plan providers), insurance carriers (such as health plan administrators and life insurance providers) and brokers, and other HR services providers may also receive information about your salary, benefits, and equity compensation as necessary to quote, administer and provide compensation, benefits and other work-related allowances, administer the workforce, comply with applicable laws and employment-related requirements, communicate with you and third parties, and respond to and comply with requests and legal demands. Those third parties are located in your country of employment and, depending on the function, in the United Kingdom, the United States and other countries.

Third-Party Service Providers: Certain third-party service providers, whether affiliated or unaffiliated, will receive your Personal Data to process such data under appropriate instructions ("**Processors**") as necessary for the processing purposes, in particular, to carry out employment background checks and certain global HR management activities or IT-related tasks (*i.e.*, for hosting or maintenance of secure global systems or the recruiting platform). The Processors will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard your Personal Data and to process your Personal Data only as instructed.

Former Employers: We may provide your Candidate Data to former employers to obtain the necessary references and background checks for you.

Government Agencies, Regulators, and Professional Advisors: We may need to transfer your Personal Data to government agencies and regulators (*e.g.*, tax authorities, courts, and government authorities) to comply with legal obligations and to external professional advisors as necessary to comply with legal obligations, communicate with you and third parties, respond to and comply with requests and legal demands and otherwise pursue legitimate interests (*e.g.*, protecting Avalara Group's legal interests). Professional advisors may be located in your country of employment or, depending on the function, in the United Kingdom, the United States, and other countries.

Sensitive Candidate Data will only be processed and transferred if permitted by applicable law.

Notice Regarding Vista. We disclose Personal Data to Vista for administration, research, database development, workforce analytics and business operation purposes, in accordance with this Notice. Vista processes and shares your Personal Data with its affiliates, including other Vista portfolio companies, on the basis of its legitimate interests in managing, administering and improving its business and overseeing the recruitment process and, if applicable, your employment relationship with the Company. If you have consented to it, your Personal Data may be shared with other Vista portfolio companies for the purpose of being considered for other job opportunities in the pooling system. A full list of all Vista portfolio companies is located at https://www.vistaequitypartners.com/companies/ and Vista's privacy policy is located at https://www.vistaequitypartners.com/privacy/. In connection with the recruitment process, your Personal Data may be transferred to iCIMS, Hirebridge, LLC, and Criteria Corp., which provide applicant tracking and evaluation services.

IV. If you Provide Personal Data of Third Parties

If you provide third parties' personal data to the Company (for instance, data of people requesting or providing personal references or data of your dependents), you must ensure that your provision of that personal data and further processing by the Company pursuant to this Notice complies with the applicable data protection laws. Where applicable, you must also authorize third parties to provide us with your personal information requested for the applicable purposes of processing indicated above (for example, a reference).

V. CCPA/CPRA Disclosures for candidates in California

Pursuant to the California Civil Code §1798.100 and 1798.130(c) and the corresponding regulations from the California Attorney General and California Privacy Protection Agency, candidates in California receive additional disclosures as follows:

We do not sell or share for cross-context behavioral advertising any of the categories of personal information we collect about California resident job applicants. These disclosures do not reflect our collection, use, or personal information handling practices with respect to California residents' personal information where an exception or exemption applies under the California Consumer Privacy Act for 2018, as amended, including by the California Privacy Rights Act of 2020 and its implementing regulations ("**CCPA**"). If you have a visual disability, please contact our HR department for accommodations.

We collect and process the following categories of personal information for the following purposes:

Categories of Personal Information	Processing Purposes
Identifiers such as real name, alias,	• Regulatory-Related

Categories of Personal Information	Processing Purposes
postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.	Purposes. • Recruiting-Related Purposes. • HR Purposes. • Security and Access Control Purposes. • Investigation and Audit Purposes. • Corporate Transaction Purposes. • Insurance Purposes. • Analytics Purposes. • Safety Purposes. • Client Marketing purposes. • Litigation-Related Purposes.
Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including but not limited to his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information, but excluding publicly available information that is lawfully made available to the general public from federal, state, or local government records. (the categories of personal information described in the California Customer Records Act (Cal. Civ. Code § 1798.80(e)) that Avalara collects)	• Regulatory-Related Purposes. • Recruiting-Related Purposes. • HR Purposes. • Security and Access Control Purposes. • Investigation and Audit Purposes. • Corporate Transaction Purposes. • Insurance Purposes. • Analytics Purposes. • Safety Purposes. • Client Marketing purposes. • Litigation-Related Purposes.
Characteristics of protected classifications under California or federal law.	• Regulatory-Related Purposes. • Investigation and Audit Purposes. • Corporate Transaction Purposes. • Insurance Purposes. • Analytics Purposes. • Client Marketing

Categories of Personal Information	Processing Purposes
	purposes. • Litigation-Related Purposes.
Internet or other electronic network activity information, including but not limited to browsing history, search history, and information regarding a consumer's interaction with an internet website application or advertisement.	• Regulatory-Related Purposes. • HR Purposes. • Security and Access Control Purposes. • Investigation and Audit Purposes. • Safety Purposes. • Litigation-Related Purposes.
Professional or employment-related information. Specifically, job information, contact information, work history.	• Regulatory-Related Purposes. • Recruiting-Related Purposes. • HR Purposes. • Corporate Transaction Purposes. • Analytics Purposes. • Safety Purposes. • Client Marketing purposes. • Litigation-Related Purposes.
Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 USC Sec. 1232g; 34 CFR Part 99). Specifically, education history.	• Regulatory-Related Purposes. • Recruiting-Related Purposes. • HR Purposes. • Corporate Transaction Purposes. • Analytics Purposes. • Safety Purposes. • Client Marketing purposes. • Litigation-Related Purposes.
Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Specifically, inferences regarding characteristics, attitudes, abilities, and aptitudes regarding job and	• Regulatory-Related Purposes. • Recruiting-Related Purposes. • HR Purposes. • Analytics Purposes.

Categories of Personal Information	Processing Purposes
culture fit.	
Social security, driver's license, state identification card, or passport number.	• Regulatory-Related Purposes. • HR Purposes. • Insurance Purposes.
Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. Specifically, account log-in, credentials allowing access to an account.	• HR Purposes. • Security and Access Control Purposes. • Investigation and Audit Purposes. • Analytics Purposes. • Safety Purposes. • Litigation-Related Purposes.
Racial or ethnic origin, religious or philosophical beliefs, or union membership. Specifically, racial or ethnic origin.	• Regulatory-Related Purposes. • HR Purposes. • Corporate Transaction Purposes. • Analytics Purposes. • Safety Purposes. • Client Marketing purposes. • Litigation-Related Purposes.
The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication. Specifically, email messages.	• Regulatory-Related Purposes. • Investigation and Audit Purposes. • Analytics Purposes. • Safety Purposes. • Litigation-Related Purposes.

Effective Date: January 1, 2023