

AVALARA

NOTICE ON RECRUITMENT/ONBOARDING DATA PROCESSING

BRAZIL

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 Brasil - Assessoria e Consultoria Tributária e Tecnológica Ltda., its affiliated companies, and its private equity sponsor and affiliates companies (collectively, "**Avalara Group**") in Brazil.

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, , 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;
- Health information/certificate (if required to be collected);
- Trade union membership (when legally required to be collected);
- Self-declaration concerning racial and ethnic origin (when legally required to be collected or, if you grant your consent, for purposes of implementation of any diversity/inclusion program).

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 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**”);
- 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 defence that the Avalara Group could face before any jurisdictional and/or administrative authority, arbitration, or mediation panel and to cooperate with – or to inform – law enforcement or regulatory authorities to the extent required by law (“**Litigation-related Purposes**”).

III. Legal Justification for the Processing of your Personal Data

Privacy law, in particular, the Brazilian General Data Protection Law (“**LGPD**”) requires any processing of Personal Data to have a legal justification. We generally rely on the following legal justifications: you have given your consent (LGPD Art. 7, (I) or Art. 11, (I)) (“**Consent**”) or the processing is necessary for (i) the performance of the employment contract (LGPD Art. 7(V) or Art.11, (II)(d) and the corresponding provisions in local data protection law for the employment relationship) (“**Contract Justification**”); (ii) compliance with a legal obligation (LGPD Art. 7(II) or Art.11, (II)(a) (“**Legal Obligation Justification**”); or (iii) pursuing our legitimate interests that do not override your interests and fundamental rights and freedoms (LGPD Art. 7(IX)) (“**Legitimate Interest Justification**”).

Generally, the processing of your Personal Data is necessary for the consideration of the employment contract. In general, you are required to provide your Personal Data in order to be considered for a position with the Company, except in limited instances when we indicate that certain data is voluntary.

We rely on the following legal justifications for the processing of your Personal Data:

FOR PROCESSING OF CANDIDATE DATA		
Processing Purposes	Categories of Candidate Data involved	Legal basis
Recruiting-related Purposes	<ul style="list-style-type: none">• Basic Contact Data• Human Resources Data• Background Data	<ul style="list-style-type: none">• Consent;• Contract Justification;• Legal Obligation Justification; or

FOR PROCESSING OF CANDIDATE DATA		
Processing Purposes	Categories of Candidate Data involved	Legal basis
		<ul style="list-style-type: none"> • Legitimate Interest Justification to appropriately administer the recruiting (and, if applicable, onboarding) process.
Regulatory-related Purposes	<ul style="list-style-type: none"> • Basic Contact Data • Human Resources Data • Background Data • Security and Access Control Data 	<ul style="list-style-type: none"> • Contract Justification; • Legal Obligation Justification; or • Legitimate Interest Justification to comply with applicable laws and employment-related requirements and administration of those requirements.
Security and Access Control Purposes	<ul style="list-style-type: none"> • Basic Contact Data • Human Resources Data • Background Data • Security and Access Control Data 	<ul style="list-style-type: none"> • Contract Justification; • Legal Obligation Justification; or • Legitimate Interest Justification to facilitate and manage security and access controls regarding Avalara Group offices and premises, equipment, and systems.
Litigation-related Purposes	<ul style="list-style-type: none"> • Basic Contact Data • Human Resources Data • Background Data • Security and Access Control Data 	<ul style="list-style-type: none"> • Legal Obligation Justification; or • Legitimate Interest Justification to support any claim or defence that the Avalara Group could face before any jurisdictional and/or administrative authority.

We conduct relevant balancing tests for data processing we carry out on the basis of our legitimate interests; further information on this exercise can be obtained from the data privacy office using the details set out above. More information on the balancing test is available upon request.

FOR PROCESSING OF SENSITIVE CANDIDATE DATA		
Processing Purposes	Categories of Sensitive Candidate Data involved	Legal basis
Recruiting Purposes, including onboarding, equal opportunity and diversity monitoring initiatives, accommodations for disabilities, and right to work checks	<ul style="list-style-type: none"> • Information on disability, where this has been provided voluntarily to us • Other health information, where required to be collected • Race or ethnicity data, where this has been provided voluntarily to us or is contained in your 	Consent (LGPLD Art. 11(I)) or The processing is necessary for the purposes of (i) carrying out the obligations and exercising our or your specific rights in the field of employment and social

FOR PROCESSING OF SENSITIVE CANDIDATE DATA		
Processing Purposes	Categories of Sensitive Candidate Data involved	Legal basis
	passport or other citizenship and right to work documentation or information collected for visa and immigration.	security and social protection law (LGPD Art. 11(II)(a)); (ii) protecting your life or physical safety as a data subject (e.g. in the case of a workplace accident) (LGPD Art. 11(II)(e));
Regulatory-related Purposes	<ul style="list-style-type: none"> • Information on disability, where this has been provided voluntarily to us • Other health information, where required • Race or ethnicity data, where this has been provided voluntarily to us or is contained in your passport or other citizenship and right to work documentation or information collected for visa and immigration. 	(iii) the assessment of the working capacity of an employee or the provision of health or social care or treatment (LGPD Art. 11(II)(a)).
Litigation-related Purposes	<ul style="list-style-type: none"> • Sensitive Candidate Data relating to claims or defences before any jurisdictional and/or administrative authority. 	The processing is necessary for the establishment, exercise or defence of legal claims (LGPD Art. 11(II)(d)).

IV. 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). Some recipients are located outside of Brazil.

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 fulfil the employment relationship within our global structure. The legal basis for such transfers is Contract Justification and Legitimate Interest Justification and our legitimate interests are the above mentioned. 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 European Economic Area 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.

Avalara, Inc. or Avalara Europe Ltd. acts as a Processor (as further described below) for some Personal Data (for example, it is hosting the global human resources information system) and acts as Controller with respect to other Personal Data.

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. To the extent these providers do not act as Processors (as below), the legal basis for such transfer is Contract Justification and Legitimate Interest Justification.

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. A list of currently engaged Processors can be provided upon request to dataprivacy@avalara.com.

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. The legal basis for such transfer is the Legal Obligation Justification and Legitimate Interest Justification.

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

Potential Acquirors or Partners: We may need to share your Personal Data with companies or professional advisors of companies that may be interested in acquiring all or part of Avalara’s participation or assets, during a due diligence and negotiation process. Such companies and individuals may be located in Brazil or abroad.

In connection with the data transfers described above, Personal Data may in some cases be transferred onwards to recipients (i) in a country benefitting from an adequacy decision, (ii) bound by standard contractual clauses or other binding instrument ensuring the same level of data protection as standard contractual clauses, (iii) where such onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings, (iv) where it is necessary in order to protect life or physical safety of the data subject or another natural person, (v) you have provided consent to such onward transfer, or (vi) the recipient otherwise ensures appropriate safeguards.

2. Cross-Border Data Transfers

We transfer Personal Data to Avalara Group companies, service providers, customers, business partners, regulators and advisors located inside or outside Brazil, such as Avalara, Inc. in the United States, only if necessary for the purposes listed above. To the extent your Personal Data is transferred to countries that do not provide for an adequate level of data protection from a Brazilian legal perspective, we will base the respective transfer on appropriate safeguards, such as standard contractual clauses, where this is required under applicable law. You can ask for a copy of such appropriate safeguards by contacting dataprivacy@Avalara.com.

V. Retention periods for and deletion of your Personal Data

We and our service providers store your Personal Data to the extent necessary for the performance of our obligations and for the time necessary to achieve the purposes for which the information is collected, in accordance with applicable data protection laws. When we no longer need to store or use your Personal Data to comply with contractual, statutory or regulatory obligations to which we are subject (for example, statutory retention periods or if we need it to preserve evidence within legal statutes of limitation) or for other purposes in accordance with applicable law (for example, if you consent to our keeping your information on file for purposes of contacting you about other job opportunities), we will remove it from our systems and records or take steps to properly anonymize it so that you can no longer be identified from it.

VI. Your statutory rights

Individuals have a number of rights in relation to their personal data processed as described in this Notice. These are summarised below. Please note that exercising these rights is subject to certain requirements and conditions as set forth in applicable laws.

These rights may also be limited in certain circumstances, for example if fulfilling a request would reveal personal information about another person, where they would infringe the rights of another (including the Company), or if an individual asks us to delete information which we are required by law or have compelling legitimate interests to keep. Relevant exemptions are included in both the LGPD and other applicable local laws. We will inform individuals of any relevant exemptions it on which we rely upon when responding to any request received.

- 1. Right of access:** You have the right to obtain from the Company confirmation as to whether your Personal Data is being processed, and, where that is the case, to request access to the Personal Data. The access information includes – inter alia – the purposes of the processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data have been or will be disclosed.

You have the right to obtain a copy of the Personal Data undergoing processing. Subject to applicable law, we may charge a reasonable fee for copies, based on administrative costs.

2. **Right to rectification:** You have the right to obtain from the Company the rectification of inaccurate Personal Data concerning you. Depending on the purposes of the processing, you may have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.
3. **Right to erasure:** You have the right to ask the Company to erase your Personal Data.
4. **Right to restriction of processing:** You have the right to request restriction of processing of your Personal Data, in which case and if the requirements are met, it would be marked and processed by the Company only for certain purposes.
5. **Right to data portability:** You have the right to receive your Personal Data which you have provided to us in a structured, commonly used and machine-readable format and you have the right to transmit the Personal Data to another entity without hindrance from us.
6. **Right to object:** *You may have the right to object, on grounds relating to your particular situation, at any time to the processing of your Personal Data by us and we can be required to no longer process your Personal Data. If you have a right to object and you exercise this right, your Personal Data will no longer be processed for such purposes by us. Exercising this right will not incur any cost. Such a right to object may not exist, in particular, if the processing of your Personal Data is necessary to take steps prior to entering into a contract or to perform a contract already concluded.*
7. **Right to withdraw consent at any time.** For processing relying on consent, you have the right to withdraw your consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.
8. **Right to anonymize your Personal Data.** You may request that your Personal Data be anonymized so that it no longer identifies you. In some circumstances we will not be able to comply with such request.
9. **Right to Petition to Public Authorities and to Exercise Your Rights in Court.** Whenever you feel that any of your rights have been violated, you have the right to file administrative and judicial claim.
10. **Request review of automated decisions made on the basis of Personal Data collected:** We will provide you with the opportunity to review a decision made automatically by Avalara's systems based on your Personal Data, if applicable.
11. **Right to request information from public and private parties with whom we have shared your Personal Data.** In this document, we set out the categories of third parties with whom may share your Personal Data. If you wish, you may request that we disclose the identity of the third parties with whom we have shared your Personal Data.

If you wish to exercise these rights, or if you have questions or comments regarding this Notice, or to get the physical address of the Avalara Group company to which you are applying, please contact your Avalara hiring entity contact (or the applicable data protection officer, where appointed) or Avalara's global data privacy office at dataprivacy@avalara.com.

VI. 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. For instance, you should inform the third parties of the purposes and means of the processing of their personal data and obtain their consent to the processing, as required by the applicable data protection law. 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).

VII. Updates and notices

If we update this Notice, we will provide you with a new notice. We may also notify you in other ways from time to time about the processing of your personal data.

Last updated: May 30, 2023