Updated January 13, 2026

StepStone Group Job Applicant Privacy Notice (California)

In this Job Applicant Privacy Notice (California), we, StepStone Group LP, StepStone Group Real Estate LP, StepStone Group Real Assets LP, StepStone Group Private Wealth LLC, StepStone Group Private Debt LLC, and their subsidiaries and affiliates (collectively "**StepStone**"), address disclosure requirements towards you, a job applicant residing in California, under the California Consumer Privacy Act of 2018 and its regulations ("**CCPA**") at or before the point of collection. These disclosures do not reflect our personal information handling practices with respect to California residents' personal information where an exception or exemption applies under the CCPA.

This notice applies to you if you are a California resident who has applied for a job with StepStone as an employee, contractor, consultant, temporary worker, intern, or apprentice ("**Job Applicant**"). Nothing in this notice shall change a job applicant's employment status with StepStone.

1. WHAT CATEGORIES OF PERSONAL INFORMATION DO WE COLLECT?

The list below sets out the categories of personal information and sensitive personal information (as defined by the CCPA) that we collect from our job applicants (in the following bullets, a "consumer" means a job applicant residing in California).

Non-Sensitive Personal Information:

- Identifiers such as a real name, alias, 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.
- 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, 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.
- Characteristics of protected classifications under California or federal law.
- 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.
- Geolocation data.
- Audio, electronic, visual, or similar information, including data relating to your use of computers, software, networks, communications devices, and other similar systems that: (i) we or our affiliates own or make available to you; or (ii) you connect to or use for the purposes of providing services to us or our affiliates; and
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

- Inferences drawn from any personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Sensitive Personal Information:

- A consumer's social security, driver's license, state identification card, or passport number.
- A consumer's 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.
- A consumer's precise geolocation.
- A consumer's racial or ethnic origin, religious or philosophical beliefs.
- Personal information collected and analyzed concerning a consumer's health.
- Personal information collected and analyzed concerning a consumer's sexual orientation.

2. FOR WHAT PURPOSES DO WE COLLECT AND USE PERSONAL INFORMATION?

We use non-sensitive personal information about our job applicants:

- To comply with applicable laws and regulatory requirements, including applicable work-related laws and requirements and administration of those requirements.
- To administer and process your application.
- To assess your skills, qualifications, suitability for the work or role for which you applied or for similar roles in the Company, and eligibility to work in the jurisdiction.
- To communicate with you about the recruitment process and, to the extent permitted by applicable law, future roles and opportunities.
- If your application progresses, carry out reference and/or background checks where applicable.
- To conduct internal audits and workplace investigations, as well as investigate and enforce compliance with any potential breaches of Company policies and procedures.
- To comply with various monitoring and reporting requirements.
- To comply with applicable legal or regulatory requirements, such as employment-related requirements, statutory reporting requirements, and export control restrictions.
- To protect the health and safety of our personnel as well as visitors to our facilities.
- To respond to lawful requests, court orders, and legal processes.
- To support any claim or defense that we or our affiliates could face before any jurisdictional and/or administrative authority, arbitration, or mediation panel, as well as cooperate with or inform law enforcement or regulatory authorities to the extent required by law.
- To keep records related to our hiring processes.
- If you are offered and accept a position with us, complete the on-boarding or new hire process.

We use sensitive personal information about our job applicants:

- To perform the services reasonably expected by our job applicants, including those services that are reasonably necessary for us to administer and process job applications.
- To comply with diversity monitoring and reporting requirements.
- To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information, including in or via our premises, computers, software, networks, communications devices, and other similar system.
- To resist malicious, deceptive, fraudulent or illegal actions directed at us and to prosecute those responsible for those actions.
- For short-term, transient use.
- To verify or maintain the quality or safety of our services and products.
- To perform functions that are required under laws that apply to us.
- To collect or process it where such collection or processing is not for the purpose of inferring characteristics about a consumer.

3. WHAT CRITERIA DO WE CONSIDER WHEN RETAINING PERSONAL INFORMATION?

We retain each of the categories of personal information for as long as necessary for the purposes for which it was collected, including any additional time periods necessary for the compliance with laws, exercise or defense of legal rights, and archiving, back-up, and deletion processes.

4. ADDITIONAL INFORMATION

This notice is not intended to create any rights for anyone except us and our affiliates or qualify any other notices or consents of us or our affiliates in any way. For more information, please contact **privacy@stepstonegroup.com**, fill out our **Contact Us** form on our website, or call +1-888-995-0350. Our CCPA Privacy Disclosures are available **here**.