Updated January 13, 2026

StepStone Group Worker Privacy Notice (California)

In this Worker 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, our workers 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 StepStone's directly-hired employee, contractor, consultant, temporary worker, intern, apprentice, or secondee, or employed by a third-party contracting/consulting company or staffing agency and are dispatched to work for StepStone ("**worker**"). Nothing in this notice shall change an individual's employment status.

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 workers (in the following bullets, a "consumer" means a worker of ours 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, 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.
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products or services purchased or other purchasing or consuming histories or tendencies. 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
    - Information relating to your activities on our or our affiliates' premises.
- 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.
- The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
- The processing of biometric information for the purpose of uniquely identifying a consumer.
- 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 workers:

- To comply with applicable laws and regulatory requirements, including applicable work-related laws and requirements and administration of those requirements;
- To manage your work relationship with us (including onboarding processes; timekeeping; payroll; compensation including equity-based compensation; expense report administration; worker benefits administration; worker training and development requirements; the creation, maintenance, and security of your online worker accounts; communicating with you, other personnel, and third parties; reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill; workers' compensation claims management; worker job performance, including goals and performance reviews, promotions, discipline, and termination; and other human resources purposes);
- To communicate with you and enable communications with you for purposes of business continuity;
- To facilitate and manage security and access control regarding our and our affiliates' offices and premises, equipment, and systems, including security activities such as security screenings to the extent permitted by applicable law;
- To conduct internal audits and workplace investigations, as well as monitor, investigate, and enforce compliance with applicable laws, regulatory requirements, and our policies and procedures;
- To engage in corporate transactions requiring review of worker records, such as for evaluating potential mergers and acquisitions of us;

- To comply with corporate financial responsibilities;
- To process and report on worker expenses;
- To contact and search for you in an emergency;
- To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
- To perform workforce analytics, data analytics, and benchmarking;
- To administer and maintain our operations, including for safety purposes and managing corporate information technology;
- To protect the health and safety of our personnel as well as visitors to our facilities;
- To conduct marketing and business development, including via social media and un response to client requests, as appropriate;
- To respond to lawful requests, court orders, and legal processes; and
- 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.

We use sensitive personal information about our workers:

- To perform the services or provide the goods reasonably expected by our workers in their role as our workers, including those services and goods that are reasonably necessary for us to administer the work relationship and for our workers to perform their duties;
- 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;
- To ensure the physical safety of natural persons;
- For short-term, transient use;
- To perform services on behalf of us;
- To verify or maintain the quality or safety of our services and products;
- To improve, upgrade, or enhance our services and products;
- To perform functions that are required under laws that apply to us; and
- To collect or process it where such collection or processing is not for the purpose of inferring characteristics about a consumer.

3. YOUR USE OF OUR PREMISES AND COMPUTER SYSTEMS

NO PRIVACY: **You have no expectation of privacy when you work on our premises, use any computer systems we own or connect to any networks we operate. Your actions and communications are observed, monitored, recorded, tracked, filtered, deleted, and otherwise processed for the purposes described in this notice.**

Monitoring: We monitor, collect, observe, record, track, filter, delete, and otherwise process information about your actions and communications on our premises and on Computer Systems ("**Monitored Data**") for the purposes described in Section 2 above. "**Computer Systems**" means 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. Such systems may include, but are not limited to, computer desktops/laptops, tablets, portable storage devices, instant messaging programs (*e.g.*, Microsoft Teams, etc.), web mail and pages viewed through our devices or networks, StepStone email accounts, telephones, facsimile, and smart phones, printers, network devices and equipment.

Tracking, Wiping, and Blocking Computer Systems: We may track and locate your Computer Systems, including, but not limited to, in the event devices with company information are lost or stolen. To ensure the confidentiality of business information and preserve its interests, we may remotely delete any data which may be stored on a Computer Systems. This may include, but is not limited to, deleting Monitored Data at the end of your work relationship with us, and deleting Monitored Data of a Computer System that is lost, stolen or retired. We may delete any and all data, including but not limited to any professional information and personal information you may have stored on your Computer Systems. This may affect devices you own and use for work purposes, as well as private information that you have stored on devices; you should regularly back-up data on devices in compliance with applicable company policies. We reserve the right – but do not assume any obligation – to monitor, access, retrieve, review, intercept, block, and delete, to the greatest extent permitted by applicable law, any and all activities, including, but not limited to, phone calls, emails, instant messages or chats, files or documents created, sent, received, accessed or stored while using Computer Systems. Only to the extent required by mandatory laws will we take preliminary steps (such as collection of aggregate data to pinpoint irregularities, issuing collective warnings) before engaging in these actions.

Inform others of limited privacy: Make sure that everyone who you may be communicating with on Computer Systems are also aware that if they are communicating with you through Computer Systems, their written and oral communications may be monitored, recorded, tracked, filtered and otherwise processed.

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

In general, we retain each of the categories of personal information and sensitive personal information described in this notice for the longer of: (i) four years following the end of your work with us; (ii) any duration necessary for compliance with laws; or (iii) for as long as necessary for the exercise or defense of legal rights and archiving, back-up, and deletion processes.

5. 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. If you have a visual disability, please contact your HR department for accommodations. Our CCPA Privacy Disclosures are available **here**.