WORKFORCE PRIVACY NOTICE

Effective Date: June 3, 2024
Last Updated: June 3, 2024

The Privacy Notice describes how Sterling Group Companies and affiliated entities (collectively, "Sterling" "we" and "us") processes personal information about you in the course of your employment with us.

If you have any questions, please contact us as provided below. If you have a disability and/or want to receive this Privacy Notice in a different format, please contact us at privacy@sterling.com.

BY OBTAINING EMPLOYMENT WITH US OR OTHERWISE PROVIDING US WITH YOUR PERSONAL INFORMATION, YOU ARE CONSENTING TO THIS PRIVACY NOTICE. PLEASE READ IT CAREFULLY.

Contents

Categories of Personal Information We Process

We, or our third-party vendors, may collect the following categories and types of personal information about you. Where provided by you, we may also collect this information about your dependents/beneficiaries.

- **Identifiers.** We, or our third-party vendors, may collect name, employee number, postal address, telephone number, email address, business contact information, social security number, driver's license number, government issued ID number, state identification card number, passport number, military ID (or copy), professional certification or license numbers, TSA Precheck/Global Entry Number, physical description (height, weight, hair color, eye color), tax identification number, signature, online identifiers (Facebook ID, Google ID, LinkedIn ID, Twitter ID, etc.), username or email address, combined with password or security question and answer, immigration visa information, and immigration/travel history.
- **Audio/Visual Data.** We, or our third-party vendors, may collect audio, electronic, photographic, visual or similar data including videos, photographs, and audio recordings both inside our offices

and warehouses and in our parking lots and other external areas. We may also collect text messages if you are using a company cell phone.

- **Biometric Information.** We, or our third-party vendors, may collect characteristics about you that can be used to establish your identity. For example, we may collect your fingerprint, hand or palm print to obtain government security clearances. Additionally, certain applications allow the use of face recognition for authentication and access. If you choose to enable this feature, will receive this biometric information.
- **Characteristics of Protected Classifications Under California or Federal Law.** We, or our third-party vendors, may collect race, ethnicity, national origin, citizenship, physical or mental disability, marital status, gender/gender identity, age/date of birth, veteran or military status, and pregnancy and related information.
- **Financial Information.** We, or our third-party vendors, may collect bank account number, credit card number, Swift/BIC number, and payroll records.
- **Geolocation Data**. If you use your personal device to access our systems or access applications, We, or our third-party vendors, may collect information such as your GPS coordinates and location.
- **Internet or Electronic Usage Data.** We, or our third-party vendors, may collect browsing history, search history, cookie data, online identifier, device identifier, and IP address. We may also collect PW, PW hints, and other information for access, authentication, and security.
- **Health Insurance Information.** We, or our third-party vendors, may collect health insurance information such as your policy number, insurance application information, claims history, spouse or dependent information, insurance group ID, insurance plan member ID, and insurance policy number if applicable.
- **Medical Information.** To the extent permitted by applicable laws, we, or our third-party vendors, may collect information about your medical treatment, diagnosis, dates of service, and your ability to perform certain tasks or to work, about physical screenings or drug test results.
- **Sensitive Personal Information.** We, or our third-party vendors, may collect credit history/credit score, drug test results, criminal records, and health information.
- **Professional or Employment Information.** We, or our third-party vendors, may collect pre-employment information such as resumes, employment applications, references, social media profiles, and other information we do through independent research. We may also collect employee evaluations, feedback, comments, suggestions, ideas, etc. and other information provided via forms, surveys, questionnaires, etc.
- **Inferences.** We, or our third-party vendors, may use information from the categories of personal information described above in order to create inferences about you, to reflect your preferences and intelligence or aptitudes.

Sources of Personal Information

We collect personal information in the following ways:

- **Directly from you.** We may collect identifiers, biometric information, personal characteristics or traits, financial information, health insurance information, medical information, professional or

employment information, education information, and sensitive personal information that you provide directly to us. This included when you are interacting with products, services, systems, applications, etc. For example, when you are interacting with a digital person, artificial human, or avatar, or with a system/application for security, authentication, access purposes.

- **When you visit our locations.** When you visit our offices, warehouses, or parking lots, we may collect audio/visual data from security cameras at our facilities.
- **Automatically.** We may collect geolocation data and internet or electronic usage data relating to your use of our IT systems including your website activity and IP address in accordance with our internal policies.
- **From third-parties including vendors and service providers.** We may collect identifiers, audio/visual data, biometric information, personal characteristics or traits, financial information, geolocation data, internet or electronic usage data, health insurance information, medical information, professional or employment information, education information, sensitive personal information, and inferences from third parties including vendors and service providers.

Purposes for Collecting Personal Information

We use personal information for the following business and commercial purposes:

- **Onboarding.** We use identifiers, audio/visual data, personal characteristics or traits, medical information, professional or employment information, education information, and sensitive personal information to complete our contract with you, enroll you in our databases, provide communication services, provide you access to our facilities and IT systems, and administer your engagement and personnel records.
- **Benefits.** We use identifiers, audio/visual data, personal characteristics or traits, health insurance information, medical information, professional or employment information, education information, and sensitive personal information to create benefits packages and provide and administer benefits.
- **Payroll.** We use identifiers, biometric information, financial information, geolocation data, and sensitive personal information to track your time and attendance and absences and to pay you and reimburse you for professional expenses.
- **Leave and Accommodation Requests.** We use identifiers, personal characteristics or traits, health insurance information, medical information, professional or employment information, and sensitive personal information to evaluate and process time off, leaves of absence, or accommodation requests.
- **Resource Planning and Consultant Management.** We use identifiers, professional or employment information, education information, and inferences for performance and talent management, disciplinary and grievance procedures, and reviews and assessments.
- **Business Operations.** We use identifiers, audio/visual data, biometric information, personal characteristics or traits, financial information, geolocation data, internet or electronic usage data, health insurance information, medical information, professional or employment information, education information, sensitive personal information, and inferences for guiding our recruiting, hiring, and onboarding efforts, maintaining records, planning, budgeting, calibration, headcount, training, competency, professional development, increasing employee engagement, assessing

performance, promoting employee health and safety, database administration, diversity metrics, surveys, evaluations, reports, legal claims, compliance, regulatory, audit, investigative and disciplinary purposes (including disclosure of such information in connection with legal process or litigation),ethics and compliance reporting and tools, and support our business operations.

- **Analytical Purposes.** We use identifiers, audio/visual data, personal characteristics or traits, professional or employment information, education information, sensitive personal information, and inferences to analyze trends and statistics, including analyzing and monitoring the equality, diversity, and inclusivity of our consultant workforce (as permitted by applicable law). We may do so in order to better understand our workforce, to prevent discrimination in the workplace, comply with our legal, contractual, and other compliance obligations, and/or to respond to allegations or claims.
- **Maintenance and Improvement of our Systems.** We use identifiers, geolocation data, and internet or electronic usage data to improve our systems, provide and maintain functionality on our systems, and help us diagnose technical and service problems and administer our systems. Maintenance of our systems includes activities such as applying security controls for company systems, providing new system implementations, applying change management processes, and providing IT Service Desk / Help Desk Support.
- **Security and Fraud Prevention.** We use identifiers, audio/visual data, biometric information, personal characteristics or traits, financial information, geolocation data, internet or electronic usage data, health insurance information, medical information, professional or employment information, education information, sensitive personal information, and inferences to: (i) protect our websites, premises, assets, systems, products, services and intellectual property; (ii) protect us, our employees, our carriers and others from fraud, theft and other misconduct; (iii) enforce our policies or the policies of our clients; and (iv) detect and prevent fraud, theft, and misconduct including by verifying the identity of those we are conducting business with.
- **Legal.** We use identifiers, audio/visual data, biometric information, personal characteristics or traits, financial information, geolocation data, internet or electronic usage data, health insurance information, medical information, professional or employment information, education information, sensitive personal information, and inferences to comply with our legal obligations, contractual obligations, customer and partner requirements, company policies and procedures, and other compliance obligations, including reporting requirements, and defend ourselves against allegations, complaints, claims and in legal proceedings, and protect our company and our property, employees, and others through legal proceedings.
- **Other Purposes.** We may use identifiers, audio/visual data, biometric information, personal characteristics or traits, financial information, geolocation data, internet or electronic usage data, health insurance information, medical information, professional or employment information, education information, sensitive personal information, and inferences for other reasons we may describe to you.

How We Disclose Personal Information

We disclose personal information in the following circumstances:

- **Service Providers.** We may share personal information with vendors and service providers who support the operation of our products, services, Site, and our business and who need access to

such information to carry out their work for us (including, for example, cloud hosting providers, OEMs, suppliers and distributors, lawyers, bankers, tax consultants, auditors, insurers, payment processors, financial institutions, email delivery vendors, internet service providers, operating systems and platforms, recruiting vendors, maintenance and customer support services). In some cases, the vendor or service provider may directly collect the information from you on our behalf.

- **Marketing/Analytics/Advertising Partners.** We may share personal information with third-party marketing, analytics or advertising partners, including social media platforms and networks, who provide analytics or marketing and advertising services to us.
- **Government Entities.** We share information with regulatory and government entities including government, administrative, law enforcement and regulatory agencies; tax authorities; and other public agencies or authorities if we think we should in order to comply with any applicable law, regulation, legal process or other legal obligation. This includes cooperating with law enforcement when we think it is appropriate, obtaining legal remedies or limiting our damages, responding to subpoenas, and to enforcing or protecting our contracts, legal rights or the rights of others, including by responding to claims asserted against us.
- **Corporate Transaction Recipients.** We may share information with potential investors, purchasers, merger partners, and their advisors in the event we: (i) sell or transfer, or are considering selling or transferring, all or a portion of our business or assets; or (ii) are considering or engaging in any reorganization, conversion, merger, sale, joint venture, assignment, transfer or disposition of all or any portion of our ownership interest, business or operations; or (iii) are soliciting or accepting investments.
- **Other Reasons.** We may disclose personal information for other reasons we may describe to you, including if you consent to the disclosure or direct us to disclose your information.

How Long We Keep Personal Information

We will retain and use your information for as long as we need it to administer your employment, or as long as necessary to comply with our legal obligations, contractual obligations, and other compliance obligations, resolve disputes, and enforce our agreements. We use the following criteria to determine retention periods:

- how long the information is needed to provide our services and operate our business;
- whether there are contractual or legal obligations that exist that require us to retain the information for period of time;
- whether any law, statute, or regulation allows for a specific retention period;
- whether an individual has agreed to a longer retention period;
- whether the data is considered to be sensitive data; and
- what the expectation for retention was at the time the data was provided to us.

Security

We follow generally accepted industry standards to protect the personal information submitted to us and have implemented reasonable technical, organization, administrative and physical measures to protect personal information. No method of transmission over the Internet, or method of electronic storage, is

100% secure, however. Therefore, we cannot guarantee its absolute security and encourage you to use website and share information with caution.

Processing in the United States

Please be aware that information we obtain about you will be processed in the United States by our service providers or us. You acknowledge your personal information may be transferred to and processed in jurisdictions outside your own as described in this Privacy Policy. Please be aware that the data protection laws and regulations that apply to your personal information transferred to the United States or other jurisdictions may be different from the laws in your country of residence. The United States may not afford the same level of protection as laws in your own country.

California Privacy Rights

This section applies to residents of California.

Shine The Light. The California Shine the Light law (Cal. Civ. Code § 1798.83) permits residents of California to request certain details about how their information is shared with third parties for the third parties' direct marketing purposes. If you are a California resident and would like to make such a request, please contact us at privacy@sterling.com and include "CA Shine the Light" in the subject line of your email.

California Consumer Privacy Act ("CCPA").

Sale or Sharing of Personal Information. In the preceding 12 months, we have not "sold" or "shared" (as those terms are defined in the CCPA) any personal information that we process in connection with your employment with us. We do not knowingly sell or share the personal information of minors under the age of 16.

Use or Disclosure of Sensitive Personal Information. In the preceding 12 months, we have not used or disclosed sensitive personal information for purposes to which the right to limit use and disclosure applies under the CCPA.

Disclosures for a Business Purpose. In the 12 months preceding the last updated date above, we have collected and disclosed the following categories of personal information to these categories of recipients for a business purpose:

- Identifiers: service providers, professional advisors, and government entities.
- Biometric Information: service providers and professional advisors.
- Characteristics of Protected Classifications Under California or Federal Law: service providers and government entities.
- Geolocation Data: service providers, professional advisors, and government entities.
- Audio/Visual Data: service providers and professional advisors.
- Education Information: service providers, professional advisors, and government entities.
- Professional or Employment Information: service providers, professional advisors, and government entities.
- Sensitive Personal Information: service providers, professional advisors, and government entities.

- Inferences: service providers, professional advisors, and government entities.

Your Rights Under the CCPA. Subject to certain exceptions and limitations, the CCPA affords California consumers the following rights:

- You have the right to request that we tell you (i) what personal information we have collected about you, (ii) the sources of that information, (iii) the business or commercial purposes for collecting, selling or sharing the personal information; and (iv) the categories of third-parties to whom we have disclosed personal information.
- You have the right to request that we provide you with a copy of your personal information.
- You have the right to request that we delete your personal information.
- You have the right to opt-out of the sale of your personal information.
- You have the right to opt out of the sharing of your personal information for cross-context behavioral advertising
- You have the right to direct us to limit the use or disclosure of your sensitive personal information to only the purposes specified in the CCPA.
- You have the right to correct inaccurate personal information that we hold about you.
- You have the right to not be discriminated against for exercising any of your CCPA rights. We will not discriminate against you, deny you services, charge you a different price, or provide you with a lesser quality of services if you exercise any of your CCPA rights.

Exercising Your Rights. To exercise any of your rights, please use our webform (available at https://www.sterling.com/privacyrequest) or call us toll free at 866-219-2874. For all requests, you must provide us with your name, email address, phone number, and mailing address. We will verify your identity by matching the information we have collected against the information you have provided. Failure to provide the foregoing information may prevent us from processing your request. If you have requested that we correct your personal information, we may contact you to request additional information about the personal information that you believe is inaccurate, including supporting documentation. In order to designate an authorized agent to act on your behalf, you must send a signed, written authorization to us.

Virginia Privacy Rights

This section applies to residents of Virginia.

Your Rights. Subject to certain exceptions and limitations, the Virginia Consumer Data Protection Act ("VCDPA") affords Virginia consumers the following rights:

- You have the right to request that we confirm whether or not we are processing your personal data and to access your personal data.
- You have the right to obtain a copy of your personal data in a portable and, to the extent technically feasible, readily usable format that allows data portability.
- You have the right to correct inaccurate personal data that we hold about you, taking into account the nature of the personal data and the purposes of the processing of the data.
- You have the right to request that we delete personal information that we have collected from you or obtained about you.

- You have the right to opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) automated decision-making or profiling in furtherance of decisions that produce legal or similarly significant effects concerning you.

Exercising Your Rights. To exercise any of your rights, please use our webform (available at https://www.sterling.com/privacyrequest) or call us toll free at 866-219-2874. For all requests, you must provide us with your name, email address, phone number, and mailing address. We will verify your identity by matching the information we have collected against the information you have provided. Failure to provide the foregoing information may prevent us from processing your request. If you have requested that we correct your personal information, we may contact you to request additional information about the personal information that you believe is inaccurate, including supporting documentation. In order to designate an authorized agent to act on your behalf, you must send a signed, written authorization to us.

Appealing Our Decision. If we refuse to take action on your request, you may appeal our decision within a reasonable period of time, not to exceed 90 calendar days from the date of your receipt of our response. You may exercise your appeal rights by emailing us at privacy@sterling.com.

Please include your full name, the basis for your appeal, and any additional information to consider.

United Kingdom Privacy Rights

This section applies to residents of the United Kingdom.

Controller. The controller of your personal information is Sterling Group Companies.

Representative. Our UK Representative is Olivier Willocx. Our UK Representative may be contacted at info@edpo.com.

Disclosure and Cross-Border Transfer. Personal information that is shared with affiliates and third parties as described in this Privacy Policy is done pursuant to contracts that include the requisite protections under applicable data protection laws. In accordance with these laws, transfers of personal information outside of the United Kingdom are conducted in accordance with compliant arrangements such as international data transfer agreements or legally recognized certifications and adequacy decisions. In certain circumstances, courts, law enforcement agencies, regulatory agencies or security authorities in those other countries may be entitled to access your personal information.

Lawful Basis for Processing Personal Information. The lawful basis for our collection and use of your personal information described in this Privacy Policy is that the processing is (i) necessary for our legitimate interests in carrying out our business, provided those interests are not outweighed by your rights and interests; (ii) necessary to perform a contract with a third-party or with you; (iii) necessary to comply with a legal obligation; or (iv) based, when necessary and appropriate, on your consent.

Special Categories of Data. Unless we specifically authorize you to do so, do not send us any Special Categories of Data, which is defined under applicable data protection laws as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric characteristics, health, or sexual orientation.

Segmentation and Automated Decision Making. We do not use segmentation or automated decision-making without human intervention, including profiling.

Your Rights Over Your Personal Information**.** Subject to certain exceptions and limitations, you have the right to:

- Ask us to confirm whether we are processing your personal information.
- Ask us to provide you or a third party that you designate with certain of your personal information in a commonly used, machine readable format. Please note, however, that data portability rights apply only to personal information that we have obtained directly from you and only where our processing is based on consent or the performance of a contract.
- Request that we update or correct your personal information when it is inaccurate or incomplete.
- Request that we delete your personal information in certain circumstances.
- Request that we limit processing or stop processing your personal information in certain circumstances including for marketing activities and profiling for marketing activities and profiling for statistical purposes and, subject to certain exceptions, where such processing is based on our legitimate business interests.
- Withdraw or revoke consent previously granted to the extent permitted by law.

Exercising Your Rights. To exercise any of your rights, please use our webform (available at https://www.sterling.com/privacyrequest) or call us toll free at 866-219-2874. We will respond to all such requests within 30 days of our receipt of the request, unless there are extenuating circumstances, in which event we may take up to 60 days to respond. We will inform you if we expect our response to take longer than 30 days. Please note, however, that certain personal information may be exempt from such rights pursuant to applicable data protection laws. In addition, we will not respond to any request unless we are able to appropriately verify the requester's identity.

You also have the right to lodge a complaint with the Information Commissioner's Office. The ICO's complaint procedures may be found at https://ico.org.uk/make-a-complaint/.

Contact Us

If you have any questions about this Notice or our data practices, please email us at privacy@sterling.com.

Updates to Our Privacy Notice

This Privacy Notice is reviewed and updated annually to ensure that it accurately captures our practices and procedures. We will notify you of any material changes to this Privacy Notice as required by law. The "Last Updated" legend above indicates when this Privacy Notice was last revised.