Applicants must agree to the following privacy policy before submitting an employment application. Select "APPLY NOW" to continue.

EMPLOYMENT PRIVACY POLICY

LEGACY PARTNERS, Inc.

Effective as of January 1, 2023.
Last reviewed:

Our Commitment to Privacy

Legacy Partners and its subsidiaries, affiliates and related companies ("Legacy Partners," "we," or "us") are committed to protecting the Personal Information that our employees and job applicants (together referred to as "Employees," "you," or "your") entrust to us.

We use industry standard safeguards to protect the confidentiality of Personal Information we collect. All Personal Information that we collect in connection with your application or employment is accessible only by designated staff or agents of our organization who are also bound to this statement. This statement is provided to clarify our commitment to protecting the security of the Personal Information you provide.

Updates

This Notice will be reviewed annually and may be updated to reflect changes in our business, legal or regulatory obligations. The current version of the Privacy Policy is always available to Employees and Applicants by emailing your request to Privacy@legacypartners.com or visit our website at www.legacypartners.com/careers and select Employment Privacy Policy/Notice. Employees may also visit the Legacy Partners employee information portal on Dayforce Forms/Company Documents. Legacy Partners will not collect Personal Information or use already collected Personal Information in any manner other than as disclosed in this Notice without providing you with notice of our intent to do so.

Collection, Use, and Disclosure of Personal Information

Personal Information covered by this Privacy Policy

As used in this Privacy Policy, "Personal Information" means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked with a particular California resident or household. Personal Information generally does not include publicly available information, such as information shared through social media and information lawfully made available from federal, state, or local government records, except to the extent such information is associated with other Personal Information.

Please note that this Privacy Policy does not apply to your Personal Information that is already protected under other laws such as the California Financial Information Protection Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Fair Credit Reporting Act (FCRA).

In particular, we have collected the following categories of Personal Information from Employees within the last twelve (12) months:

Statutory category and Definition	Examples of what we may collect
Identifiers Real name, alias, postal address, unique personal identifier, customer number, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.	• *Full name, alias and names of family members* • *Physical address(es), telephone number(s), e-mail address(es) Business and personal contact information* • *Date of birth, place of birth*
Personal Information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) A name, signature, Social Security number, or, address, telephone number, passport number, driver's license or state identification card number, education, employment, employment history, bank account number, or any other financial information, medical information, or health insurance information.	*Financial information:* • Retirement account information, bank accounts, student loans, insurance, information regarding estate or tax planning, legal issues (e.g., child support, alimony, wage garnishments and subpoenas), and benefits information. *Medical Information* • Medical history, medical questionnaires, information regarding physical, mental and/or behavioral health, genetic information, wellness activities and subsidies, health insurance information, information regarding payment for healthcare services.
Protected Classification Characteristics Age (forty years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	*We do not intentionally collect this information but some of it may be revealed in identity data or other information we collect, such as:* ▪ age ▪ race ▪ citizenship ▪ gender ▪ disability status ▪ military service status

Commercial Information Records of personal property, products or services purchased, obtained, or considered, payment history, complaint history, service requests or other purchasing or consuming histories or tendencies.	• *Purchase History* (for example, from expenses submitted for reimbursement) • *Personal Property Records*
Biometric Information An individual's physiological, biological or behavioral characteristics, including an individual's fingerprint, faceprint, voiceprint, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	• *Fingerprints* • *Voice recognition* • *Typing cadence* • *Health, or exercise data through our wellness program*
Internet or Network Information Browsing history, search history, and information regarding a person's interaction with an Internet website, application, or advertisement.	• *Usage information* • *Search history* • *IP address* • *Mobile device identifier*
Geolocation Data Precise location, e.g., derived from GPS coordinates or telemetry data.	• *Physical location*
Sensory Information Audio, electronic, visual, thermal, olfactory, or similar information.	• *Onsite security camera recordings* • *Photographs* • *Audio recordings*
Professional or Employment Information Any information relating to a person's current, past or prospective employment or professional experience (e.g., job history, performance evaluations).	• *Salary/compensation* • *Benefits* • *Employment history* • *Performance reviews*
Non-Public Education Information Education records, degrees and vocational certifications obtained, report cards, and transcripts.	• *Information you provide in connection with hiring process or in seeking a promotion in employment*
Inferences	*May be derived from:* • *Business and personal contact information* • *Profile information*

For example, a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.	• *Behaviors, attitudes or aptitudes* • *Hobbies*

How We Collect Personal Information

We collect Personal Information from the following categories of sources:

- **Directly from You** – We may collect information you provide to us, or that you authorize a third party to provide to us, such as information from a recruiting agency or related to administration of benefits or special accommodations for employment.
- **Business Partners** – We may collect information provided to us in connection with our recruiting efforts.
- **Automatic Collection** – We may use data collection technologies to collect information about you (see Automatic Data Collection Technologies below).
- **Public Sources** – Such as social media profiles and online forums. We may combine information collected from a public profile with non-public information and subsequently treat such information as Personal Information.

Use of Personal Information

We may use or disclose the Personal Information we collect for one or more of the following purposes:

- Manage workforce activities and personnel generally, including for recruitment, background screening, performance management, career development, payments administration, employee training, leaves and promotions;
- Perform identity verification, accounting, audit, and other internal functions, such as internal investigations;
- Administer hiring, promotion, and discipline;
- Manage payroll, wages, tax forms and filing, expense reimbursements, and other awards such as stock options, stock grants and bonuses, and provide healthcare, pensions, savings plans and other benefits;
- Calculate insurance and other employee benefits;
- Notify family members in case of an emergency;
- Maintain and secure our facilities, equipment, systems, and infrastructure;
- Protect the health and safety of our workforce and others, and conduct risk and security control and monitoring;
- Conduct research, analytics, and data analysis to assist in planning succession and to ensure business continuity, as well as to design employee retention programs and diversity initiatives;
- Provide an efficient means for personnel to obtain the contact information of their colleagues so they may contact them;
- Monitor use of IT infrastructure, internet access, and electronic communication for unauthorized, unlawful, or inappropriate use;
- Record phone calls for training, quality assurance, and legal compliance purposes;
- Operate and manage IT and communications systems and facilities, allocate company assets and human resources, and undertake strategic planning and project management;

- Obtain legal advice and establish, exercise or defend legal rights, and act on collection and discovery requests in the context of litigation, government investigations or regulatory audits or inquiries; and
- Comply with law, legal process, investigations, internal policies and other requirements such as income tax deductions, monitoring, record-keeping and reporting obligations.

Sharing of Personal Information

We do not sell or rent your Personal Information or share your Personal Information with other people or nonaffiliated companies, except with your permission, or under the following circumstances:

- We may provide your Personal Information to our service providers, who work on our behalf under confidentiality agreements. Service providers may include payroll processing, benefit providers, training providers and companies that assist in any pre-employment verifications and background checks.
- We may provide your Personal Information to our professional advisors, including insurance providers and legal counsel, who work on our behalf under confidentiality agreements.
- We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims;
- We believe it is necessary to share information in order to investigate, prevent, or act regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of the Web site terms of use, or as otherwise required by law.
- We transfer information about you if this company is acquired by or merges with another company.

Your Rights and Choices

Where required by federal, state, or local law, including the California Consumer Privacy Act of 2018 and California Privacy Rights Act of 2020 with respect to California residents, Employees have the rights listed below. However, these rights are not absolute, and we may decline your request as permitted by law.

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection and use of your Personal Information over the past 12 months (the "right to know"). Once we receive your request and confirm your identity (see Exercising Your Rights to Know or Delete), we will disclose to you:

- The categories of Personal Information we collected about you.
- The categories of sources for the Personal Information we collected about you.
- Our business or commercial purpose for collecting or selling that Personal Information.
- The categories of third parties with whom we share that Personal Information.

- If we sold or disclosed your Personal Information for a business purpose, two separate lists disclosing: sales, identifying the Personal Information categories that each category of recipient purchased; and disclosures for a business purpose, identifying the Personal Information categories that each category of recipient obtained.
- The specific pieces of Personal Information we collected about you (also called a data portability request).

Right to Delete

You have the right to request that we delete any of your Personal Information that we collected from you and retained, subject to certain exceptions (the "right to delete"). Once we receive your request and confirm your identity (see Exercising Your Rights to Know or Delete), we will review your request to see if an exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Maintain records with respect to past and/or current Employees; take actions reasonably anticipated within the context of our ongoing business and/or employment relationship with you, or otherwise exercise our rights, or perform our obligations, including, without limitation, with respect to any contract, law or regulation, in connection with your employment or application for employment.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.) or other applicable federal, state, or local laws and regulations.
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify Personal Information not subject to an exception from our records and will direct our service providers to take similar action.

Exercising Your Rights to Know or Delete

To exercise your rights to know or delete described above, please submit a request by either:

- Calling our Privacy Line at (833) 329-0076
- Emailing us at Privacy@legacypartners.com

Only you, or someone legally authorized to act on your behalf, may make a request to know or delete related to your Personal Information.

You may only submit a request to know twice within a 12-month period. Your request to know or delete must provide sufficient information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative and describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with Personal Information if we cannot verify your identity or authority to make the request and confirm the Personal Information relates to you.

Changes to Our Privacy Policy

We reserve the right to amend this privacy policy at our discretion and at any time. When we make changes to this privacy policy, we will post the updated notice and update the notice's effective date.

Contact Information

If you have any questions or comments about this Policy, the ways in which Legacy Partners collects and uses your information described here, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Phone: (833) 329-0076 or **Email:** Privacy@legacypartners.com

If you need to access this Policy in an alternative format due to having a disability, contact Privacy@legacypartners.com or (833) 329-0076.

Or Postal Address:
Legacy Partners, Attn: Human Resources
950 Tower Lane, Suite 900
Foster City, CA 94404

EMPLOYMENT PRIVACY NOTICE

NOTICE AT COLLECTION
LEGACY PARTNERS

Effective Date: January 1, 2023

Last Reviewed:

Legacy Partners and its subsidiaries, affiliates and related companies (the "Company") collects and uses your personal information, including sensitive personal information, for human resources, employment, benefits administration, health and safety, and business-related purposes and to be in legal compliance. We are committed to properly handling the personal information collected or processed in connection with your employment relationship with us.

To view our Employment Privacy Policy, please email your request to Privacy@legacypartners.com or visit www.legacypartners.com/careers select "Employment Privacy Policy/Notice."

We may collect the personal information and sensitive personal information categories listed in the tables below. The tables also list, for each category, our collection and use purposes.

Personal Information Category	Business Purpose
Identifiers Real name, alias, postal address, unique personal identifier, customer number, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.	• Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks. • Conduct employee onboarding. • Maintain and administer payroll and employee benefit plans, including enrollment and claims handling. • Maintain personnel records and complying with record retention requirements. • Provide employees with human resources management services and employee data maintenance and support services. • Communicate with employees and their emergency contacts and plan beneficiaries. • Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to Company policies.

	• Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy. • Respond to law enforcement requests and as required by applicable law or court order. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Personal Information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) A name, signature, Social Security number, or, address, telephone number, passport number, driver's license or state identification card number, education, employment, employment history, bank account number, or any other financial information, medical information, or health insurance information.	• Same purposes as for identifiers category.
Protected Classification Characteristics Age (forty years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	• Comply with federal and state equal employment opportunity laws. • Design, implement, and promote the Company's diversity and inclusion programs. • Perform workforce analytics, data analytics, and benchmarking. • Conduct internal audits, grievances, and suspected violations of Company policy. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Commercial Information Records of personal property, products or services purchased, obtained, or considered, payment history, complaint history, service requests or other purchasing or consuming histories or tendencies.	• Manage payroll, wages, tax forms and filing, and expense reimbursement. • Respond to law enforcement requests and as required by applicable law or court order.

Biometric Information An individual's physiological, biological or behavioral characteristics, including an individual's fingerprint, faceprint, voiceprint, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	• Fingerprinting for a criminal background check after an initial offer of employment is made. Criminal background checks protect the company, mitigate risk, and avoid potential negligent hiring lawsuits. • Administer and design health wellness programs. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Internet or Network Information Browsing history, search history, and information regarding a person's interaction with an Internet website, application, or advertisement.	• Facilitate the efficient and secure use of Company information systems. • Ensure compliance with Company information systems policies and procedures. • Comply with applicable state and federal laws. • Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information. • Enhance employee productivity. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Geolocation Data Precise location, e.g., derived from GPS coordinates or telemetry data.	• Improve safety of employees, customers, and the public regarding use of the Company property and equipment. • Prevent unauthorized access, use, or loss of the Company property. • Improve efficiency, logistics, and supply chain management. • Ensure employee productivity and adherence to the Company's policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company's policy.
Sensory Information Audio, electronic, visual, thermal, olfactory, or similar information.	• Comply with applicable state and federal laws, including on workplace health and safety. • Prevent unauthorized access, use, or loss of the Company property.

	• Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Professional or Employment Information Any information relating to a person's current, past or prospective employment or professional experience (e.g., job history, performance evaluations).	• Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding. • Design and administer employee benefit plans and programs, including for leaves of absence. • Maintain personnel records and comply with record retention requirements. • Communicate with employees and their emergency contacts and plan beneficiaries. • Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of the Company's property, including its information systems, electronic devices, network, and data. • Ensure employee productivity and adherence to the Company policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy. • Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Non-Public Education Information Education records, degrees and vocational certifications obtained, report cards, and transcripts.	• Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company.
Inferences For example, a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.	• Engage in human capital analytics, including to identify correlations about individuals and job success, analyze data to improve retention and productivity, and analyze employee preferences to inform human resources policies and procedures • Conduct applicant reference checks to assist in hiring decisions

Sensitive personal information is a subtype of personal information consisting of specific information categories. While we collect information that falls within the sensitive personal information categories listed in the table below, the California Privacy Rights Act of 2020 does not treat this information as sensitive because we do not collect or use it to infer characteristics about a person.

Sensitive Personal Information Category	Business Purpose
Government Identifiers Social Security number, driver's license, state identification card, and passport and visa information, and immigration status and documentation.	• Manage workforce activities and personnel generally, including for recruitment, background screening, performance management, career development, payments administration, employee training, leaves and promotions. • Process and administer payroll and employee benefit plans, including enrollment and claims handling. • Maintain personnel records and comply with record retention requirements. • Provide employees with human resources management services and employee data maintenance and support services. • Communicate with employees and their emergency contacts and plan beneficiaries. • Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data. • Respond to law enforcement requests and as required by applicable law or court order.
Complete Account Access Credentials User names, account numbers, or card numbers combined with required access/security code or password.	• Manage workforce activities and personnel generally, including for recruitment, background screening, performance management, career development, payments administration, employee training, leaves and promotions. • Provide employees with human resources management services and employee data maintenance and support services. • Prevent unauthorized access to or use of the Company information systems, electronic devices, network, and data.

Precise Geolocation Physical access to a Company office location, or the location of a delivery, sales, or other employee in the field.	• Improve safety of employees, customers, and the public regarding use of the Company property and equipment. • Prevent unauthorized access, use, or loss of the Company property. • Improve efficiency, logistics, and supply chain management. • Ensure employee productivity and adherence to the Company's policies. • Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company's policy. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Racial or Ethnic Origin	• Comply with federal and state equal employment opportunity laws. • Design, implement, and promote the Company's diversity and inclusion programs. • Perform workforce analytics, data analytics, and benchmarking. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy.
Religious or Philosophical Beliefs	• Review and process religious reasonable accommodation requests. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Mail, Email, or Text Messages Contents Not Directed to the Company	• Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Genetic Data	• Investigate and process workers' compensation claims. • Process health insurance claims. • Conduct and process employment testing.
Unique Identifying Biometric Information	• Fingerprinting for a criminal background check after an initial offer of employment is made. Criminal background checks protect the company, mitigate risk, and avoid potential negligent hiring lawsuits.

	• Ensure accurate time records. • Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.
Health Information Job restrictions and workplace illness and injury information.	• Investigate and process workers' compensation claims. • Process health insurance claims. • Conduct and process employment testing. • Ensure equal access to retirement programs and fertility planning by same-sex spouses. • Ensure equal family leave policies and insurance for transgender surgeries.
Sex Life Or Sexual Orientation Information	• Process health insurance claims. • Ensure equal access to retirement programs and fertility planning by same-sex spouses. • Ensure equal family leave policies and insurance for transgender surgeries.

Retention

Legacy Partners will retain the Personal Information, including sensitive Personal Information, listed above, as long as we need this information to fulfill the business purpose for which it was collected or as long it is required by applicable laws or regulation.

If you have any questions about this Notice or need to access this Notice in an alternative format, please contact Privacy@legacypartners.com or leave a message at (833) 329-0076.