

CALIFORNIA APPLICANT/EMPLOYEE PRIVACY POLICY

This California Privacy Policy provides you with information regarding SullivanCurtisMonroe's ("SCM," "we," "us," and "our") treatment of personal information relating to you as either an employee, director, officer, independent contractor, or part-time worker of SCM, or as an applicant for one of those positions (collectively, "Employee").

Your Rights

Under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, "CCPA"), California residents have the following rights:

- The right to know what personal information we've collected about you, including the categories of personal information; categories of sources from which we collected the personal information; the purpose for our collection, selling, or sharing of your personal information; the categories of parties to whom we disclose personal information; and the specific pieces of personal information we have collected about you;
- The right to delete personal information we have collected from you, subject to certain exceptions;
- The right to correct inaccurate personal information that we maintain about you; and
- The right to not receive discriminatory treatment for exercising your privacy rights.

How to Submit a Request to Know, Access, Correct, or Delete

If you are a California resident and you would like to submit a request to know, access, correct, or delete your personal information, you can email your request to ccpa@sullicurt.com, call us toll-free at 833-214-5105, or submit the webform available at https://sullivancurtismonroe.com/wp-content/uploads/2020/07/ccpa-request-form_07012020-1.pdf.

What Happens After You Submit a Request to Know, Access, Correct, or Delete?

Following receipt of a request to know, access, correct, or delete your personal information, we will take commercially reasonable steps to verify your identity, including verifying you via your existing password-protected account with us or asking you to provide us with information to confirm your identity (e.g., your zip code, email address, phone number, or dates of employment). If you are an agent authorized to make a request on a California resident's behalf, please indicate that when submitting your request. Agents must generally provide a signed authorization evidencing their authority to act on behalf of another individual.

We will make good faith efforts to evaluate and act on your request, but there may be circumstances in which we do not grant your request. For example, we are not required to delete personal information needed (i) to provide a service we are contracted to provide, (ii) to detect fraudulent or illegal activity, (iii) for bookkeeping or tax purposes, or (iv) for legal purposes. Also, we are not required to provide access or deletion where

your identity could not be verified, where the information would compromise others’ privacy or other legitimate rights, such as intellectual property rights, or where the information contains legally privileged material. If we determine that your request should be restricted in any particular instance, we will provide you with an explanation of why that determination has been made and a contact point for any further inquiries.

Any requests that can be processed by us will be done so within 45 days from the date we receive your request, unless we notify you that an extension is required. In case of an extended completion period, we will process your request within 90 days from the date of your original request. Employees are limited to two requests to know or access within a 12-month period.

Personal Information Collected, Used, and Disclosed Within the Past 12 Months

Below you will find a chart that generally describes the categories of personal information we have collected, where that information came from, the purpose for the collection of that information, the categories of parties to whom that information was disclosed, and the purpose for that disclosure, all within the past 12 months from the effective date of this notice and as it relates to Employees. Please note that these are categories of personal information as they are set forth under California law. We did not necessarily collect all of the specific pieces of personal information listed for any given person.

We do not sell any of the personal information we obtain from Employees, nor do we use it to track you across websites and target advertising to you (known as “sharing” under California law). We only use your sensitive personal information as necessary to process your application to work with us and manage and administer that relationship (e.g., to verify your eligibility to work with us, administer your benefits, pay you, and/or comply with legal requirements), or as otherwise permitted by law. If you do not provide us with certain personal information when requested, we may not be able to perform certain functions, such as considering your application for employment, hiring you, or paying or providing a benefit to you.

What Personal Information Do We Collect?	Where Do We Get It?	Why Do We Collect It?	To Whom Do We Disclose It?	Why Do We Disclose It?
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, including	<ul style="list-style-type: none"> • The Employee • Background check providers • Recruiters 	<ul style="list-style-type: none"> • Collecting or processing employment applications, including confirming eligibility, performing background checks, and onboarding • For payroll and employee benefit plan and program administration purposes, including enrollment and claims handling 	<ul style="list-style-type: none"> • Service providers (e.g., information technology (“IT”) support, background check and benefit providers) • Financial institutions • State or federal government entities 	<ul style="list-style-type: none"> • Administering benefits • Facilitating work • Paying Employees • Training • Monitoring and supporting our IT system

<p>emergency contact details and information regarding your dependents.</p>		<ul style="list-style-type: none"> • Communicating with Employees and their emergency contacts and/or plan beneficiaries • Monitoring employee performance and policy adherence • Loss prevention • Investigating complaints, grievances, and potential policy violations • Maintaining employment records • Legal compliance 	<ul style="list-style-type: none"> • Dispute resolution bodies 	<ul style="list-style-type: none"> • Contract execution • Investigating complaints • Accounting • Resolving legal disputes • Legal compliance
<p>Any personal information described in subdivision (e) of Section 1798.80.</p>	<ul style="list-style-type: none"> • The Employee • Background check providers • Employee benefit providers • Insurers 	<ul style="list-style-type: none"> • Collecting or processing employment applications, including confirming eligibility, performing background checks, and onboarding • For payroll and employee benefit plan and program administration purposes, including enrollment and claims handling • Maintaining employment records • Communicating with Employees and their emergency contacts and/or plan beneficiaries • Monitoring and preventing unauthorized access or use of our property and/or systems • Loss prevention • Monitoring employee performance and policy adherence • Workplace safety 	<ul style="list-style-type: none"> • Service providers (e.g., IT support and benefit providers) • Financial institutions • Insurers • State or federal government entities • Dispute resolution bodies 	<ul style="list-style-type: none"> • Administering benefits • Evaluating Employees • Paying Employees • Facilitating work • Training • Contract execution • Monitoring and supporting our IT system • Accounting • Investigating complaints • Claims handling • Resolving legal disputes • Legal compliance

		<ul style="list-style-type: none"> Investigating complaints, grievances, and potential policy violations Legal compliance 		
Characteristics of protected classifications under California or federal law (e.g., gender, race, sex, age, religious or philosophical beliefs, marital status, and military or veteran status).	<ul style="list-style-type: none"> The Employee 	<ul style="list-style-type: none"> Legal compliance Providing employee benefits Our diversity and inclusion program Investigating compliance, grievances, and potential policy violations 	<ul style="list-style-type: none"> Service providers (e.g., benefit providers) State or federal government entities 	<ul style="list-style-type: none"> Administering benefits Diversity efforts Legal compliance
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.	<ul style="list-style-type: none"> The Employee 	<ul style="list-style-type: none"> Providing, supporting, monitoring, and protecting our information systems and property Enhancing employee productivity and communication Investigating complaints, grievances, and potential policy violations Ensuring policy and legal compliance 	<ul style="list-style-type: none"> IT service providers 	<ul style="list-style-type: none"> Providing, supporting, monitoring, and protecting our information systems and property Enhancing employee productivity and communication Investigating complaints, grievances, and potential policy violations Ensuring policy and legal compliance
Geolocation data, such as time and physical location related to use of an internet	<ul style="list-style-type: none"> The Employee 	<ul style="list-style-type: none"> Providing, supporting, monitoring, and protecting our 	<ul style="list-style-type: none"> IT service providers 	<ul style="list-style-type: none"> Monitoring and protecting our

website, application, device, or physical access to a company office location.		information systems and property		information systems
Professional or employment-related information (e.g., employment history, performance and disciplinary records, salary and bonus data, and benefit plan enrollment, participation, and claims information)	<ul style="list-style-type: none"> • The Employee • Employees' prior employers • Others to whom Employees refer us 	<ul style="list-style-type: none"> • Evaluating employment applications, including confirming eligibility, performing background checks, and onboarding • Administering our employee benefit plan and program • Maintaining personnel records • Communicating with Employees and/or their emergency contacts and beneficiaries • Employee monitoring to ensure productivity and policy adherence • Recruiting • Training • Investigating complaints, grievances, and potential policy violations • Legal compliance 	<ul style="list-style-type: none"> • Employee benefit providers and administrators • State or federal government entities • HR and training service providers • Others, as directed by the Employee 	<ul style="list-style-type: none"> • Providing benefits • Considering Employees for promotion • Recruiting and retaining Employees • Employment verification • Training • Claims handling • Accounting • Legal compliance
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).	<ul style="list-style-type: none"> • The Employee 	<ul style="list-style-type: none"> • Evaluating Employee applications 	N/A	N/A
Personal information collected and analyzed	<ul style="list-style-type: none"> • The Employee 	<ul style="list-style-type: none"> • Benefit administration • Claims management 	<ul style="list-style-type: none"> • Employee benefit providers, 	<ul style="list-style-type: none"> • Administering employee benefits

concerning your health and benefits	<ul style="list-style-type: none"> • Health providers to whom Employees refer us 	<ul style="list-style-type: none"> • Workplace safety • Legal compliance 	<ul style="list-style-type: none"> administrators, and consultants • Insurers 	<ul style="list-style-type: none"> • Claims handling • Legal compliance
-------------------------------------	---	--	---	---

Document Retention

We will not retain your personal information for longer than reasonably necessary for the purpose(s) we collected it. How long we retain your personal information depends on a number of criteria, including whether we hire you, your employment status with us, how long it’s been since we employed you, the nature of our relationship with you, and legal considerations.

Additional Information or Questions

If you have any questions about our privacy policy or exercising the rights described above, please visit <https://sullivancurtisonroe.com/privacy-policy/> and/or <https://sullivancurtisonroe.com/california-online-privacy-policy/>. You can also email us at ccpa@sullicurt.com or call us at 833-214-5105.

Effective Date

This California Privacy Policy is effective as of January 1, 2023, and was last updated on January 27, 2023.