

Notice at Collection for California Employees and Applicants

Cambridge Systematics (“Company” or “We”) 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.

We will not sell the personal information, including any sensitive personal information, we collect about our employees or applicants for employment or share it with third parties for cross-context behavioral advertising.

To view our full privacy policy, visit <https://camsys.com/terms-of-use-and-privacy-policy> .

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

Personal Information Category	Retention Period	Business Purpose
<p>Identifiers:</p> <p>Full name</p> <p>Contact information</p> <p>Gender</p> <p>Date of birth</p> <p>Signature</p> <p>Social Security number</p> <p>Driver's license or state identification number</p> <p>Passport or other work authorization documentation</p> <p>Dependent(s) and Beneficiary(s) Information (full name, gender, date of birth, SSN)</p> <p>Emergency Contact(s) Information (full name, phone number, e-mail).</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks • Conduct employee onboarding (e.g. system setup, employment verification check, benefit enrollment, payroll processing). • 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

		<ul style="list-style-type: none"> • 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 • Process workers compensation claims. • Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data. • Design, implement, and promote the Company's diversity and inclusion programs. • Ensure employee productivity and adherence to Company policies. • Process immigration-related documentation such as employment-related visas and employment/sponsorship documentation, and maintain records to verify work authorization. • Perform workforce analytics, data analytics, and benchmarking. • 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.
<p>California Customer Records employment and personal information:</p>	<p>10 years following termination</p>	<ul style="list-style-type: none"> • Recruit and process employment applications, including verifying eligibility for employment and

<p>Full name</p> <p>Signature</p> <p>Social Security number</p> <p>Physical characteristics or description (Race, Disability, Veteran Status, Sexual Orientation),</p> <p>Photograph</p> <p>Address, telephone number</p> <p>Passport number</p> <p>Driver's license or state identification card number</p> <p>Insurance policy number</p> <p>Education</p> <p>Current employment</p> <p>Employment history</p> <p>Membership in professional organizations</p> <p>Licenses and certifications</p> <p>Bank account number</p> <p>Financial, medical or health insurance information.</p>	<p>unless there is a business need to retain data longer</p>	<p>conducting background and related checks</p> <ul style="list-style-type: none"> • Conduct employee onboarding (e.g. system setup, employment verification check, benefit enrollment, payroll processing). • 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 • Process workers compensation claims. • Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data. • Design, implement, and promote the Company's diversity and inclusion programs. • Ensure employee productivity and adherence to Company policies. • Process immigration-related documentation such as employment-related visas and employment/sponsorship
---	--	--

		<p>documentation, and maintain records to verify work authorization.</p> <ul style="list-style-type: none"> • Perform workforce analytics, data analytics, and benchmarking. • 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.
<p>Protected classification characteristics under California or federal law:</p> <p>Age</p> <p>Race/Ethnicity</p> <p>National origin</p> <p>Citizenship</p> <p>Marital status</p> <p>Medical condition</p> <p>Physical or mental disability</p> <p>Sex (including gender, gender identity, sexual orientation)</p> <p>Pregnancy or childbirth</p> <p>Military and/or veteran status.</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<p>Same as above.</p>
<p>Professional or employment-related information:</p> <p>Work history</p> <p>Academic and Professional qualifications</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding

<p>Educational records</p> <p>Employment references</p> <p>Interview notes</p> <p>Background checks</p> <p>Work authorization</p> <p>Performance/ Disciplinary records</p> <p>Salary, Bonus, and other compensation data</p> <p>Benefit plan enrollment/ participation</p> <p>Benefit claims information</p> <p>Leave of absence information (including religious, military and family obligations)</p> <p>Requests for accommodations (medical/ religious).</p>		<ul style="list-style-type: none"> • 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 plan beneficiaries. • Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. • Conduct pay equity audits and equal opportunity for promotions/advancement. • Perform workforce analytics, data analytics, and benchmarking. • 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. • Process workers compensation claims. • Process immigration-related documentation such as employment-related visas and employment/sponsorship documentation, and maintain records to verify work authorization. • Evaluate and provide useful feedback about job performance, facilitate
--	--	---

		<p>better working relationships, and for employee professional development.</p> <ul style="list-style-type: none"> • Exercise or defend the legal rights of the Company and its employees. • Provide professional qualifications of workforce in proposals to potential clients and respond to client contract documentation requests.
<p>Non-public education information:</p> <p>Education records</p> <p>Degrees and certifications</p> <p>Transcripts.</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company. • Provide professional qualifications of workforce in proposals to potential clients and respond to client contract documentation requests. • Process immigration-related documentation such as employment-related visas and employment/ sponsorship documentation, and maintain records to verify work authorization.
<p>Internet or other similar network activity:</p> <p>All activity on the Company's information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords).</p> <p>All activity on communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and</p>	<p>Up to 10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • 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. • Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policy.

search history, mobile email communications, and other information regarding an employee's use of company-issued devices).		<ul style="list-style-type: none"> • Exercise or defend the legal rights of the Company and its employees, customers or contractors.
<p>Commercial information:</p> <p>Employment Verification Requests from third-party Financial details</p>	10 years following termination unless there is a business need to retain data longer	<ul style="list-style-type: none"> • Verify employment status, salary information, etc. for various requests from third-party administrators for transactions such as personal loan processing. • Respond to law enforcement requests and as required by applicable law or court order.
<p>Inferences drawn from other personal information to create a profile or summary:</p> <p>Personality traits and behaviors</p>	10 years following termination unless there is a business need to retain data longer	<ul style="list-style-type: none"> • 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.
<p>Geolocation data:</p> <p>Physical location, such as the time and physical location related to use of an internet website, application, or device.</p> <p>GPS location data from mobile devices of employees.</p>	Up to 10 years following termination unless there is a business need to retain data longer	<ul style="list-style-type: none"> • Prevent unauthorized access, use, or loss of the Company property. • 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, customers and contractors.

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 CCPA 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	Retention Period	Business Purpose
<p>Government identifiers: Social Security number Driver's license/ State identification card Passport/Visa information Immigration status and documentation</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks. • Process and administer payroll and employee benefit plans, including enrollment. • Maintain personnel records and comply with state and federal record retention requirements. • Provide employees with human resources management services and employee data maintenance and support services. • 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. • Process immigration-related documentation such as employment-related visas and employment/ sponsorship documentation, and maintain records to verify work authorization. • Process workers compensation claims.

<p>Complete account access credentials:</p> <p>User names</p> <p>Required access/security code or password</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • 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
<p>Racial or ethnic origin:</p> <p>Race/Ethnicity</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Comply with federal and state equal employment opportunity and affirmative action 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.
<p>Religious or philosophical beliefs:</p> <p>Religious beliefs</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Review and process religious reasonable accommodation requests. • Exercise or defend the legal rights of the Company and its employees.
<p>Health information:</p> <p>Job restrictions/ accommodations (medical/religious)</p> <p>Workplace Illness/ Injury Information.</p>	<p>10 years following termination unless there is a business need to retain data longer</p>	<ul style="list-style-type: none"> • Investigate and process workers' compensation claims. • Process health insurance claims. • Ensure equal access to benefit programs to same-sex spouses. • Ensure equal family leave policies and insurance coverage.
<p>Sexual orientation information:</p>	<p>10 years following</p>	<ul style="list-style-type: none"> • Ensure equal access to benefit programs to same-sex spouses.

Sexual Orientation	termination unless there is a business need to retain data longer	<ul style="list-style-type: none"> • Ensure equal family leave policies and insurance coverage. • Design, implement, and promote the Company's diversity and inclusion programs.
<p>Precise geolocation:</p> <p>Physical access to a Company office location, or the location of a delivery, sales, or other employee in the field.</p>	Up to 10 years following termination unless there is a business need to retain data longer	<ul style="list-style-type: none"> • Prevent unauthorized access, use, or loss of the Company property. • 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, customers and contractors.

If you have any questions about this Notice or need to access this Notice in an alternative format due to having a disability, please contact privacy_tos@camsys.com and/or 888.265.1825.

June 12, 2023