

California employee and applicant privacy notice

The California Consumer Privacy Act of 2018 (CCPA) imposes specific obligations on businesses processing personal information of California residents. Pursuant to the CCPA, Sentry (“Sentry,” “we,” or “us”) is required to provide its employees and applicants for employment who are California residents (“California Persons”) a notice, at or before the point of collection of such personal information, that identifies the categories of personal information that may be collected and the purposes for which the information will be used.

This California Employee and Applicant Privacy Notice (“Notice”) provides California Persons with the required Notice, and unless separately defined in the Notice, any terms defined in the CCPA, or the implementing regulations, have the same meaning when used in the Notice. Sentry will not collect additional categories of personal information or use personal information already collected for additional purposes without providing a new Notice. Sentry reserves the right to amend the Notice at any time.

Personal information we collect

Listed below are the categories of personal information that Sentry may collect:

Identifiers, including real name, alias, postal address, physical address, unique personal identifiers, email, account name, social security number, date of birth, driver’s or other license number or identifier, passport number, mobile device identification number or other similar identifiers.

Characteristics or protected classifications under California or federal law, including race, color, religion, sex, national origin, religion, ancestry, physical or mental disabilities, medical condition, marital status, age, sexual orientation, and other protected characteristics protected by law.

Biometric information, Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns.

Internet or other electronic network activity information, including browsing history, search history, application access location; mobile device security status, information regarding an employee's interaction with an internet or intranet website, application or advertisement; and time and geolocation data related to use of an internet or intranet website, application, or physical access to a Sentry location.

Audio, electronic, visual, or similar information, including photographs, video interviews, and recorded phone calls.

Professional or employment-related information, including job-related data maintained as part of the employment relationship, that is present in information within a job application, resume, video interview, employment contract, contractor agreement, performance review, disciplinary record, or photo; information from employee expenses; internet browsing, and search history; payroll and benefits-related data; internal and external contact information; or information recorded or otherwise captured from video, audio, computer, other electronic systems, or other forms of monitoring or surveillance.

Education information, including information not publicly available about an employee's educational background, such as education records, internal learning and training, and transcripts.

Inferences, including any information drawn from any of the personal information categories referenced above to create a profile about an employee reflecting the employee's characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Sources of personal information

Sentry has obtained the categories of personal information listed in the previous section from a variety of sources:

Directly from you, for example, we may receive personal information

from forms, applications, or materials you submit, written documents you submit, or from our communications with you.

Indirectly from you, for example, we may get information from you based on your usage of our websites and mobile apps, or through cookies.

Social Networks, for example, we may get application and applicant information through social networking sites.

Others, for example, we may get information from service providers or third parties like job boards, recruiters, screening providers, credit reporting agencies, or customer due diligence providers.

Purposes for using personal information

Sentry uses the personal information identified above for the purposes listed below:

To recruit employees, we may collect employment applications, resumes, work history, MVR records, applicant assessment information, and performance evaluation information to conduct employment-related background screening and checks.

To administer benefits, such as medical, dental, optical, and retirement benefits, including recording and processing eligibility of dependents, absence and leave monitoring, insurance and accident management, and providing online total reward information and statements.

To pay for and reimburse expenses, including salary administration, payroll management, payment of expenses, and to administer other compensation-related payments, including assigning amounts of bonus payments to individuals and bonuses.

To conduct performance-related reviews, including performance evaluation, career planning, skills monitoring, job moves, promotions, and staff re-structuring.

To monitor work-related licenses and credentials, including provisioning software licenses for use in the course of an employee's work-related responsibilities, ensuring compliance, training,

examination, and other requirements are met with applicable regulatory bodies.

To provide our employees with human resources management services, including providing employee data maintenance and support services; administration of separation of employment, approvals, and authorization procedures; administration and handling of employee claims; and travel administration.

To maintain your contact information, including altering your details across relevant entities within the Sentry group of companies (for example: personal information, other employment, and information about prior roles).

To assist you in case of personal or business emergency, including maintenance of contact details for you, your emergency contacts, and your dependents.

To monitor eligibility to work in the U.S., which means monitoring and ensuring compliance of your ability to work in the U.S.

To conduct healthcare-related services, including conducting pre-employment and employment-related medical screenings for return-to-work processes and medical case management; determining medical suitability for particular tasks; identifying health needs of employees to plan and provide appropriate services, including operation of sickness policies and procedures; and providing guidance on travel risk.

To facilitate a better working environment, which includes conducting staff surveys, providing senior management information about the workforce, and conducting training.

To ensure a safe and efficient working environment, which includes Sentry actions relating to disciplinary actions and code of conduct processes and investigations.

To maintain security on Sentry websites and internet-connected assets, which includes hosting and maintenance of computer systems and infrastructure; management of Sentry software and hardware computer assets; systems testing, such as development of new systems and end-user testing of computer systems; training; and monitoring email and Internet access.

To comply with applicable law or regulatory requirements, such as legal (state and federal) and internal company reporting obligations, including headcount, management information, demographic, and OSHA reporting (if applicable).

Disclosures of personal information

In the preceding twelve (12) months, Sentry may have disclosed your personal information to the following categories of third parties:

Professional advisors and service providers, for example, Sentry may disclose personal information to comply with applicable laws and regulations, to obtain professional advice and services, and to help deliver benefits and services related to your prospective or actual employment.

Legal and regulatory authorities, for example, Sentry may disclose personal information to comply with legal and regulatory obligations, financial and tax obligations, law enforcement and judicial requests such as a subpoena, or other obligations with federal, state, and local authorities.

Marketing firms, for example, Sentry may disclose personal information to third-party marketing vendors in connection with marketing efforts, which may include the production and use of online identifiers to deliver relevant ads to you and others across various employment websites and applications.

Sentry does not sell your personal information and has not sold your personal information in the last 12 months.

We impose contractual obligations on service providers and contractors to ensure that they can only use your personal information for appropriate purposes.

Privacy rights for California residents

The California Consumer Privacy Act (CCPA) provides you with specific rights regarding your personal information. This section describes your CCPA rights and explains how to exercise those rights.

The right to know and access your information: You have the right to request that Sentry disclose certain descriptions and categories of the personal information we collect, use, share, disclose, and sell about you. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you
- The categories of sources from which personal information was collected
- Our business or commercial purpose for collecting or sharing personal information
- The categories of third parties to whom we disclosed the personal information
- The specific pieces of personal information we collected and/or disclose about you

The right to request deletion: You have the right to request that Sentry delete any of your personal information that we have collected or maintained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers and contractors to delete) your personal information from our records, unless an exception applies. We may no longer be able to provide certain products or services if you exercise your right to delete.

The right to request correction: You have the right to correct your personal information. Once we receive and confirm your verifiable request, we will use reasonable efforts to update your information, unless an exception applies. We will also ask any service providers or contractors to whom we have disclosed inaccurate information to correct it.

The right to opt-out of the sharing of personal information: You have the right to opt out of specific sharing of personal information that we have collected from you. You have several options to exercise this right. You may:

- Turn on opt-out preference signals as described in more detail in the Opt-out preference signals section below
- Complete an [online request form](#)
- Call us, toll-free, at 877-788-4012
- Email us at privacy@sentry.com

If we have actual knowledge that you are less than 13 years old, we will not share your personal information without the consent of a parent or guardian.

The right to opt-out of the selling of personal information: We do not sell your personal information.

The right to limit the use of your sensitive personal information: We do not use your sensitive personal information except as allowed by the CCPA.

Exercising your rights: To exercise the rights described above, please submit a verifiable consumer request by calling us toll-free at 877-788-4012 or making an [online request](#). You may make up to two requests in any 12-month period. Making a verifiable consumer request does not require you to create an account with us.

Only you, or a person that you authorize to act on your behalf (an “Authorized Agent”), may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

When you submit a request, you will need to provide us with:

- Enough information to identify you (such as your first and last name, email address, physical address, and phone number)
- A description of what right you want to exercise and the information to which your request relates

We will be unable to fulfill 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. With few exceptions, we will only fulfill a request from your Authorized Agent if:

- You grant the Authorized Agent written permission to make a request on your behalf;
- You or the Authorized Agent provides us notice of that written permission; and
- We are able to verify your identity in connection with that notice and the request

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Opt-out preference signals: If you have an opt-out preference signal enabled (such as a "Do Not Track" signal or global privacy control), your preferences are being honored. You do not need to take any additional action. The signal applies to the browser you are using. To enable an opt-out preference signal, look for Privacy or Security settings in your browser. Options may vary by browser and may change periodically.

Contact information

To view our full privacy notice online, please visit sentry.com/privacy

If you have any questions about this Notice, please contact Human Resources at 715-346-6550 or askhr@sentry.com.