



PRIVACY NOTICE FOR CALIFORNIA OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, CONTRACTORS AND JOB APPLICANTS

The California Consumer Privacy Act ("CCPA" or "Act") grants California residents ("you") certain privacy rights in their personal information. The CCPA requires a business that collects personal information from California residents to disclose at or before the point of collection, the categories of personal information to be collected, the purposes for which that information is to be collected or used, whether that information is sold or shared for cross-context behavioral purposes, and the length of time a business intends to retain that information. If sensitive personal information is to be collected, the Act requires a business to disclose the purposes for which it is collected or used and whether such information is sold or shared. This Privacy Notice is intended to meet these requirements.

Effective January 1, 2023, the CCPA applies to the personal information a business collects from job applicants, employees, owners, directors, officers or independent contractors of the business. This Privacy Notice only applies to residents of the State of California.

The CCPA defines various terms used in this Privacy Notice such as: consumer, sale, share, cross-context behavioral advertising and the definitions of those terms are incorporated herein.

If you are a job applicant or independent contractor, additional information about your rights under the CCPA can be found in our Firm's Online Privacy Policy at: https://www.hinshawlaw.com/privacy_policy.html. Additional information for our lawyers and staff about your CCPA rights can be found in our California Privacy Rights Statement in the Policy Store on the Firm's intranet, Compass.

Personal Information

The CCPA defines personal information as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA also has recognized a category personal information called "sensitive personal information" which is listed in the chart below.

Personal information under the CCPA, however, does not include:

- Deidentified or aggregated consumer information.
- Publicly available information from federal, state or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer, or from widely distributed media, or made available by a person to whom the

consumer has disclosed the information without restricting the information to a specific audience. Personal information also does not include lawfully obtained, truthful information that is a matter of public concern.

The CCPA further excludes certain types of information from its definition of personal information:

- (i) Medical or health information covered by the Health Insurance and Portability and Accountability Act of 1966 (“HIPAA”) and the California Confidentiality of Medical Information Act (“CMIA”) and certain types of clinical trial or biomedical research study data.
- (ii) Personal information covered by certain specific privacy laws such as the Fair Credit Reporting Act (“FCRA”), the Gramm-Leach-Bliley Act (“GLBA”), or California Financial Information Privacy Act (“FIPA”) and the Driver’s Privacy Protection Act of 1994.

The chart immediately below identifies categories or examples of personal information and sensitive personal information covered by the CCPA some of which we collect:

Category	Examples	Collected
A. Identifiers	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.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code §1798.80(e))	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Note: Some personal information included in this category overlap with other categories.	YES
	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or	

C. Protected classifications under California or federal law	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).	YES
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information	Physiological, behavioral, and biological characteristics, including DNA, that is or intended to be used either alone or in combination with other identifying data to establish individual identity, and includes other identifying information, such as, imagery of the iris or retina, fingerprint, face, hand, palm, vein patterns and voice recordings from which an identifier template or a voice print can be extracted, also includes, keystroke or gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	NO
F. Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data	Physical location or movements.	YES
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	NO
I. Professional or employment related information	Current or past job history or performance evaluations.	YES
J. Non-public education information (per the Family Educational Rights	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules,	

and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99))	student identification codes, student financial information, or student disciplinary records.	YES
K. Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.	NO
L. Sensitive Personal Information	Personal information that reveals a person's: social security, driver's license, state identification card or passport number, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password or credentials allowing access to the account; precise geolocation, race or ethnic origin, religious or philosophical beliefs, union membership, contents of a person's mail, email and text messages unless the business is the intended recipient; genetic data; processing biometric information for the purpose of uniquely identifying a person; information collected and analyzed concerning a person's health, sex life or sexual orientation. Note: Sensitive personal information does not include information that is "publicly available" as defined in 1798.140(v)(1)(L).	YES

Business Purposes For Which Your Information Will Be Used

Please note:

- 1) We do not and will not sell your personal information.
- 2) We will not share your personal information with third parties for cross-context behavioral advertising purposes.
- 3) We will not use your personal information to make any automated decisions affecting you.

We will use and process any personal information we receive to:

- To evaluate your eligibility or suitability for any type of engagement or association with the Firm, or your eligibility or suitability for employment, partnership or any continuation thereof, including but not limited to confirming employment, educational and military histories when applicable, check references and make background checks;
- To calculate your salary and any withholding for state or federal taxes, social security payments or any benefits offered or required by the Firm;
- To make salary payments, other payments, direct deposits or necessary calculations;
- To evaluate and permit your participation in any retirement plan offered by the firm in which you are eligible to participate under the terms of that plan and to administer your participation in and payments made to or from any plan;
- To administer our personnel policies and to assess risk management issues;
- To evaluate or administer any type of benefits offered by the Firm for which you or a family member may be eligible, and to pay and or dispute claims;
- For possible inclusion in any affirmative action programs including programs for veterans or individuals with disabilities;
- To track the use of vacation, sick days, disability or leave policies;
- To notify a person you designate in the event of an emergency;
- To comply with any legal obligation imposed upon us by law;
- To provide legal advice or services you may request that we agree to provide;
- To defend or prosecute a lawsuit, administrative proceeding, or any type of legal, regulatory or administrative claim, challenge or dispute which may include responding to discovery requests involving your information;
- To negotiate, conduct due diligence, document, settle or close a deal, transaction, contract or legal dispute, including the issuance of opinions to third parties in connection with the foregoing;
- To communicate with you or a related third party such as our insurer, any benefits or claims administrator or your agent, broker or a claim administrator about the status, developments or the outcome or our legal analysis of any claim or dispute;

- To comply with any legal demands or lawful orders issued in an administrative proceeding, by a tribunal or court of law such as subpoenas, warrants, or other legal process, or to comply with a regulatory obligation imposed by a governmental or regulatory agency or official, which could include meeting various compliance, screening, or recordkeeping requirements, anti-money laundering, financial and credit checks, fraud and crime prevention requirements, and which may require manual or automated checks of your personal information against various databases and lists;
- To respond for requests for proposals (“RFPs”), to highlight your knowledge, background, experience for marketing purposes, for making pitches to clients, to respond to client inquires or questionnaires, or in business development and marketing efforts to attract new clients or business and/or to retain existing clients and business;
- For any other lawful purpose necessary to further the legitimate interests of our Firm;
- To comply with federal, state or local laws and regulations including but limited to tax, civil rights and ERISA.
- To meet or fulfill the reasons you provided us the information, including to process offerings or requests, complete transactions, to make payments or refunds, to provide necessary information and to prevent transaction fraud;
- To help maintain the safety, security, and integrity of our websites, products, services, applications, databases, networks, and other technical assets;
- Debug, identify, rectify, or mitigate errors or vulnerabilities in our website, systems, applications, technologies, hardware, software, servers or equipment;
- To evaluate, confirm compliance with, and enforce firm policies, procedures;
- To evaluate, confirm compliance with and enforce outside counsel guidelines issued by our clients;
- To audit, improve, develop, modify or support our websites, products and services, to update and maintain contact, visitor or email lists and for other internal purposes;

- To send invitations, announcements, and information about Firm publications, programs, events, seminars, conferences, events, newsletters, publications, blogs social media feeds or to provide CLE or CE information.
- To confirm an attorney's licensure status, standing and admission to the bar of any state, jurisdiction, court of law or tribunal.
- To respond to lawful requests for information through court orders, subpoenas, warrants and other legal process, obligations or governmental regulations;
- To protect the operations of our law firm, or the safety, security and privacy of our Firm, our lawyers and staff, our clients or third parties. This potentially includes sharing information with others for purposes of fraud protection, information security, and related matters;
- To review, confirm and evaluate the identity of a person making a request concerning information in our possession.
- To evaluate and resist malicious, deceptive, fraudulent or illegal actions directed at our firm or the information in our possession and to prosecute anyone responsible.
- For any purpose related to any of the foregoing.

Categories of Third Parties With Whom We May Share Your Personal Data

We may share personal data received when necessary to administer background checks, our payroll, benefits or plans with vendors or other service providers with whom we contract to assist in the provision of those benefits or payments. This may require that we share your information with vendors like ADP, or others such as accountants, actuaries, insurers or third-party administrators or consultants used by an insurer, benefit provider, or vendors we retain to assist us when necessary to accomplish any of the purposes noted above. Information from the firm's equipment or your use of the firm's network, systems or equipment may be shared with vendors, who provide data and cybersecurity to our firm. When necessary information may be shared with court reporters, videographers, notaries, trial consultants, judges, courts, tribunals, arbitrators, lawyers and mediators involved in the resolution of a dispute. When relevant to our marketing and business development efforts, we may share your information with existing or potential clients.

We may also share your personal information with courts of law, law enforcement authorities, governmental officials or regulators, attorneys or other third parties when it is reasonably necessary for the establishment, exercise or defense of a legal or equitable claim, or for purposes of an alternative dispute resolution process; to investigate or prosecute the

violation of any law or regulation, to recover our applications, software, hardware, equipment or assets, to comply with a subpoena or court order, legal process, or other legal requirement or when we believe in good faith that such disclosure is necessary to comply with the law, to prevent physical harm or financial loss, to investigate, prevent or take action concerning illegal activities, suspected fraud, threats to our Firm, any of its lawyers or our property; or as necessary in connection with an investigation of fraud, intellectual property infringement, piracy or other unlawful activity.

Data Retention

The length of time we retain information depends on the nature of the information and the context in which it was received. We strive to retain information in accordance with our record retention schedule. For employment related information such as resumes and job applications, for instance, our record retention schedule requires that we retain that information for seven years from the time of submission.

Questions

We welcome any questions about our privacy practices and this notice. If you have any questions, please contact our Firm's General Counsel, Steven Puiszis. Mr. Puiszis can be reached by phone at 312-704-3243, via email at spuiszis@hinshawlaw.com or you can write him at: Hinshaw & Culbertson LLP, 151 North Franklin Street, Suite 2500, Chicago, Illinois 60606.