Applicant/Employee Privacy (CCPA/CPRA) Notice

About This Notice. This notice describes the categories of personal information ("PI") collected by Granite Construction Incorporated, its subsidiaries, successors, and affiliated companies over which it has operating control ("Company") and how the Company collects and uses PI about you in compliance with our obligations under the California Consumer Privacy Act of 2018 ("CCPA"), as amended by the California Privacy Rights Act of 2020 ("CPRA"). This Notice supplements the Company's California Privacy Policy, Privacy Policy, Terms of Use, and Cookie Policy.

Please read this notice carefully as it contains important information on the PI that we collect, why we collect it, how long we keep it, and whether it is sold to or shared with third parties. This notice will be updated regularly. The day the last update was performed is provided at the bottom of this document for your reference.

Key Terms. The following key terms are used in this notice:

a. **We, us, our, the Company**. Granite Construction Incorporated and its subsidiaries, successors, and affiliated companies over which it has operating control.
b. **Personal information**. Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with a particular individual.
c. **Sensitive personal information**. Personal information revealing an individual's social security number, driver's license and passport numbers, account numbers and credentials, precise geolocation, racial or ethnic origin, religious beliefs, or union membership, personal information concerning a consumer's health, sex life, or sexual orientation, contents of a consumer's mail, email and text messages where the business is not the intended recipient, genetic data, and biometric information.
d. **Biometric Information**. An individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

Other terms used but not defined will have the meaning set forth in the CCPA, as amended by the CPRA, Cal. Civ. Code §§ 1798.100—1798.199.100, and accompanying regulations set forth under Cal. Code Regs. tit. 11, § 7000 et seq., as such may be amended.

Personal Information We Collect About You and How and Why We Use Your Personal Information. We may collect and use the following categories of personal information about you and use your personal information for the following purposes:

Categories of Personal Information Collected	Purposes Personal Information is Used
Identifiers and Contact information. This category includes without limitation names, aliases, addresses, telephone	• Collecting and processing employment applications, including confirming identity, eligibility for

numbers, mobile numbers, email addresses, unique personal identifiers, online identifiers, internet protocol addresses, dates of birth, social security numbers, employee identification numbers, driver's license or state identification numbers, passport numbers, employment eligibility verification documents, benefit eligibility verification documents, insurance policy numbers, bank account numbers, credit card or debit card numbers and other financial information, travel information, bank account numbers, credit card numbers, and debit card numbers and other financial information, medical information, health insurance information, and other similar contact information and identifiers.	employment, background and related checks, and onboarding • Processing payroll and employee benefit plan and program administration including enrollment, claims handling, account statements, confirmations, responses to inquiries, and notifications about changes to plans and services • Maintaining personnel records and record retention requirements • Communicating with applicants and employees and/or their emergency contacts and plan beneficiaries • Complying with applicable state and federal labor, employment, tax, benefits, worker's compensation, disability, equal employment opportunity, workplace safety, and related laws • Preventing unauthorized access to or use of the Company's property, including the Company's information systems, electronic devices, network, and data • Ensuring employee productivity and adherence to the Company's policies, procedures and code of conduct • Facilitation of event registration and management for online and in-person events • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure or code of conduct • Monitoring compliance with Company policies, procures and code of conduct, use of Company resources, and any other monitoring activities permitted by applicable law • Managing other Human Resources Functions* • For Everyday Business Purposes**
Protected classification information. This category includes without limitation characteristics of protected classifications under California or federal law.	• Complying with applicable state and federal Equal Employment Opportunity laws • Designing, implementing, and promoting the Company's diversity and inclusion programs • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure or code of conduct • Managing Human Resources Functions* • For Everyday Business Purposes**
Internet or other electronic network activity information. This category includes without limitation:	• Facilitating the efficient and secure use of the Company's information systems

• 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 • all activity on communications systems including phone calls, call logs, voice mails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an individual's use of company-issued devices	• Ensuring compliance with Company information systems policies and procedures • Complying with applicable state and federal laws • Preventing unauthorized access to, use, or disclosure/removal of the Company's property, records, data, and information • Enhancing employee productivity • Monitoring compliance with Company policies, procures and code of conduct, use of Company resources, and any other monitoring activities permitted by applicable law • Compliance with legal and regulatory obligations, court or other government directives, and Company policies, procedures and code of conduct • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure, or code of conduct • Managing Human Resources Functions* • For Everyday Business Purposes**
Geolocation data. This category includes without limitation GPS location data from company-issued mobile devices and company-owned vehicles.	• Improving safety of employees, customers and the public with regard to use of Company property and equipment • Preventing unauthorized access, use, or loss of Company property • Improving efficiency, logistics, and supply chain management • Monitoring compliance with Company policies, procures and code of conduct, use of Company resources, and any other monitoring activities permitted by applicable law • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure, or code of conduct • Managing Human Resources Functions* • For Everyday Business Purposes**
Biometric information. This category includes without limitation fingerprint scans and related information, and certain wellness metrics.	• Providing benefit plan offerings to promote health and prevent disease • Improving safety of employees, customers, and the public with regard to use of Company property and equipment • Identification of employees and their devices • Preventing unauthorized financial transactions • Enhancing physical security • Monitoring compliance with Company policies, procures and code of conduct, use of Company

	resources, and any other monitoring activities permitted by applicable law • Managing Human Resources Functions* • For Everyday Business Purposes**
Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information. This category includes without limitation: • Photographs • Video images • Audio recordings • Voicemails	• Authentication of identity • Publication and marketing purposes • For premises security purposes and loss prevention • Monitoring compliance with Company policies, procures and code of conduct, use of Company resources, and any other monitoring activities permitted by applicable law • Compliance with legal and regulatory obligations, court or other government directives, and Company policies, procedures and code of conduct • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure, or code of conduct • Managing Human Resources Functions* • For Everyday Business Purposes**
Children's Information. This category includes without limitation: • Information about children listed as beneficiaries of Company benefits • Information about children provided by individuals in relation to Company-sponsored benefit plans and services	• For providing information, benefits, or services requested • Managing Human Resources Functions* • For Everyday Business Purposes**
Professional and employment-related information. This category includes without limitation: • data submitted with employment applications, employment history, prior employer, references, employment recommendations • background check and criminal history • work authorization • fitness for duty data and reports • performance and disciplinary records • qualifications, skills and experience • human resources data • salary and bonus data • benefit plan enrollment, participation, and claims information • emergency contact information • leave of absence information	• Collecting and processing employment applications, including confirming eligibility for employment, background and related checks, and onboarding • Employee benefit plan and program design and administration, including leave of absence administration • Maintaining personnel records and complying with record retention requirements • Communicating with applicants and employees and/or their emergency contacts and plan beneficiaries • Complying with applicable state and federal labor, employment, tax, benefits, worker's compensation, disability, equal employment opportunity, workplace safety, and related laws • Business management • Preventing unauthorized access to or use of the Company's property, including the Company's

	information systems, electronic devices, network, and data • Ensuring employee productivity and adherence to the Company's policies, procedures and code of conduct • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy, procedure, or code of conduct • Managing other Human Resources Functions* • For Everyday Business Purposes**
Education information. This category includes without limitation education history, education information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.	• Evaluating an individual's appropriateness for a particular position at the Company, or promotion to a new position • For Everyday Business Purposes*
Compliance information. This category includes without limitation: • Compliance program data, including screening records, individual rights requests, consents, and other records maintained to demonstrate compliance with applicable laws, such as tax laws, Office of Foreign Assets Control (OFAC), anti-money laundering (AML), Foreign Corrupt Practices Act (FCPA) • Occupational and environmental safety records • Records maintained in conjunction with legal matters or litigation or that are subject to legal holds • Records relating to complaints and internal investigations, including compliance hotline reports • Records of privacy and security incidents, including any security breach notifications	• For complying with and demonstration of compliance with applicable laws • For legal matters, including litigation and regulatory matters, including for use in connection with civil, criminal, administrative, or arbitral proceedings, or before regulatory or self-regulatory bodies, including service of process, investigations in anticipation of litigation, or execution or enforcement of judgments and orders • Managing Human Resources Functions* • For Everyday Business Purposes**
Inferences drawn from the PI in the categories above.	• Communicating with applicants and employees and/or their emergency contacts and plan beneficiaries • Complying with applicable state and federal labor, employment, tax, benefits, worker's compensation, disability, equal employment opportunity, workplace safety, and related laws • Business management • Preventing unauthorized access to or use of the Company's property, including the Company's information systems, electronic devices, network, and data

	• Ensuring employee productivity and adherence to the Company's policies, procedures, and code of conduct • Investigating complaints, reports of wrongdoing, grievances, and suspected violations of Company policy • Evaluating an individual's appropriateness for a particular position at the Company, or promotion to a new position • Engaging in human capital analytics, including, but not limited to, identifying certain correlations about individuals and success on their jobs, analyzing data to improve retention, and analyzing employee preferences to inform HR policies, programs, and procedures. • Managing Human Resources Functions[*] • For Everyday Business Purposes[**]

In the preceding twelve (12) months, we have disclosed the above categories of personal information for a business purpose.

Whether Personal Information Will Be Sold or Shared. The Company does not sell or share your personal information. To carry out the purposes outlined above, the Company may share information with third parties, such as background check vendors, third-party human resources and information technology vendors, outside legal counsel, and state or federal governmental agencies. The Company may add to the categories of PI it collects and the purposes it uses PI. In that case, the Company will inform you.

How Long Your Personal Information Will Be Kept. Personal information will not be kept for longer than is necessary for the business purpose for which it is collected and processed and will be retained in accordance with our internal retention policies, procedures, and schedule. We will keep your personal information:

- To respond to any questions, complaints or claims made by you or on your behalf;
- To show that we treated you fairly; or
- To keep records required by law.

The Company will not retain your personal information for longer than necessary for the purposes set out in this notice. Different retention periods apply for different types of personal information. For details on retention periods, see the Company's retention policies, procedures, and schedule, as such may be amended from time to time.

Anti-Discrimination and Retaliation; Contact. In accordance with the CCPA, as amended by the CPRA, Cal. Civ. Code §§ 1798.100—1798.199.100, and accompanying regulations set forth under Cal. Code Regs. tit. 11, § 7000 et seq., as such may be amended, the Company will not discriminate against anyone because they exercised their rights under the CCPA, as amended by the CPRA, Cal. Civ. Code §§ 1798.100—1798.199.100, and accompanying regulations set forth under Cal. Code Regs. tit. 11, § 7000 et seq., as such may be amended. If you have questions

about the Company's privacy policies and procedures, rights you may have concerning your personal information, you may contact us, toll-free, at (844) 353-4998 or CCPA@gcinc.com.

---

[*] Managing Human Resource Functions includes the following purposes for which PI may be collected and used:

- Workforce planning
- Recruiting, hiring, and onboarding
- Performing background or credit checks
- Implementing diversity and inclusion initiatives
- Increasing employee engagement
- Training and career development
- Assessing performance
- Determining promotions, transfers, salary, awards, and bonuses
- Managing disciplinary matters
- Managing payroll and business expenses
- Administering leave requests
- Employee communications
- Administration of benefits
- Promoting employee health and safety

[**] Everyday Business Purpose includes the following purposes for which PI may be collected and used:

- To provide the information, product, or service requested by the individual or as reasonably expected given the context in which the PI was collected (such as credentialing, providing service, personalization and preference management, providing updates, and bug fixes)
- For identity and credential management, including identity verification and authentication, system and technology administration
- To protect the security and integrity of systems, networks, applications, and data, including debugging activities to identify and repair errors; detecting, analyzing, and resolving security threats and incidents; and collaborating with cybersecurity centers, consortia, and law enforcement regarding the same
- For fraud detection and prevention, including protecting against malicious, deceptive, fraudulent, or illegal activity, and collaborating with law enforcement and anti-fraud industry groups regarding the same
- For auditing related to interactions with an individual and auditing compliance with specifications and standards
- To perform services on behalf of us or a service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling requests, processing payments, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of us or a service provider
- For short-term, transient use, subject to restrictions as may apply under applicable law
- For legal and regulatory compliance, including all uses and disclosures of personal information that are required or permitted by law or reasonably needed for compliance with company policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines
- For internal business purposes, such as service provider management, finance, security, information technology, managing infrastructure and assets, record retention, budgeting, corporate audit, analysis, training, quality assurance, record keeping and reporting, strategic planning, emergency response and business continuity, and pursuing or defending legal or administrative claims
- To enforce our contracts and to protect against injury, theft, legal liability, fraud, or abuse or to protect people or property, including physical security programs
- To undertake internal research and activities to verify and maintain products or services and to develop changes to, or new, products and services
- To de-identify personal information or create aggregated datasets, such as for consolidating reporting, research, or analytics
- To make back-up copies for business continuity and disaster recovery purposes
- For corporate governance, including mergers, corporate reorganization, acquisitions, and divestitures