

CALIFORNIA PRIVACY NOTICE

Where we provide our services in California, the California Consumer Privacy Act (CCPA) requires us to provide a privacy policy that contains a comprehensive description of our online and offline practices regarding our collection, use, sale, sharing, and retention personal information, along with a description of the rights individuals have regarding their personal information, in connection with the provision of our recruitment services. This privacy notice provides the information the CCPA requires, together with other useful information regarding our collection and use of personal information. Any terms defined in the CCPA have the same meaning when used in this policy.

This privacy notice applies only to individuals who are residents of California, whose personal information is processed by Momentum Technology Global Ltd in connection with our recruitment services.

Personal Information collected

We collect and use information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual ("**personal information**"). Personal information does **not** include:

- Publicly available information, including from government records, through widely distributed media, or that the individual made publicly available without restricting it to a specific audience.
- Lawfully obtained, truthful information that is a matter of public concern.
- Deidentified or aggregated individual information

Personal Information Categories Chart

The chart below identifies which categories of personal information we collected from individuals within the last 12 months.

Category	Examples	Collected
A. Identifiers.	A real name, unique personal identifier, online identifier, Internet Protocol address, email address, account name.	YES
B. Customer Records Information (Cal. Civ. Code § 1798.80(e)) (" California Customer Records ").	A name, signature, address, telephone number, employment.	YES
C. Protected classification characteristics under California or federal law (" Protected Classes ").	Gender, age, and citizenship.	YES
D. Commercial information.	Records of services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES
E. Biometric information.	Fingerprints, faceprints or voiceprints.	YES
F. Internet or other similar network activity.	Browsing history, information on a customer's interaction with a website or application.	YES
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, visual information.	YES
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 and Privacy Act ("FERPA Information")).	Education records directly related to a student such as grades, transcripts, 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.	YES
L. Sensitive personal information.	Further identified in the chart below.	YES

Sensitive Personal Information Categories Chart

Sensitive personal information is a subtype of personal information consisting of the specific information categories listed in the chart below. Importantly, the CCPA only treats this information as sensitive personal information when we collect or use it to infer characteristics about an individual.

The chart below identifies which sensitive personal information categories, if any, we have collected information from an individual to infer characteristics about them in the last 12 months.

Sensitive Personal Information Category	Collected to Infer Characteristics?
L.1. Government identifiers, such as your SSN, driver's license, state identification card, or passport number.	YES
L.2. Complete account access credentials, such as usernames, account logins with required access/security code or password.	NO
L.3. Precise geolocation, such as physical access to a Company office location, the location of a delivery, sales, or other individual in the field, or GPS data from the Company's mobile phone, device, or vehicle used by an individual that can provide its location in a geographic area, with an approximate radius of 1,850 feet.	NO
L.4. Racial or ethnic origin.	YES
L.5. Citizenship or immigration status.	YES
L.6. Religious or philosophical beliefs.	NO
L.7. Union membership.	NO
L.8. Mail, email, or text messages not directed to the Company.	NO
L.9. Genetic data.	NO
L.10. Neural Data, such as information generated by measuring a consumer's central or peripheral nervous system's activity that is not inferred from nonneural information.	NO
L.11. Unique identifying biometric information.	NO
L.12. Health information	YES
L.13. Sexual orientation information.	NO
L.14. Children's personal information (under age 16).	NO

Sources of Personal Information

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from you, such as from the forms or information you provide to the Company.
- Indirectly from you, such as from your interactions with the Company's computer or other communications systems.
- From our service providers, such as staffing partners, HR management providers, background check providers, drug testing providers, payroll providers, insurance companies, internet service providers, data analytics providers, operating systems and platforms, data brokers.
- Government entities, such as for background check purposes.
- From other individuals, such as from performance reviews or other observations and interactions.

How We Use Personal Information

Personal Information Collection, Use, and Disclosure Purposes

We may use and disclose the personal information, including sensitive personal information, we collect to advance the Company's business purposes, specifically to:

- Comply with all applicable laws and regulations.
- Recruit and evaluate a job applicant and a candidate for employment.
- Conduct background checks and verify employment eligibility.
- Manage employment relationships with us, including for:
 - onboarding processes;
 - timekeeping, payroll, and expense report administration;
 - the design and administration of benefits plans and programs, including for leaves of absence;
 - training and development requirements;
 - the creation, maintenance, and security of your online accounts;
 - the provision of human resources management services and data maintenance and support services;
 - reaching you, your emergency contacts, and plan beneficiaries when needed, such as when you are not reachable or are injured or ill;
 - workers' compensation claims management;
 - improving productivity and the Company's efficiency, logistics, and supply chain management;
 - ensuring compliance with Company information systems policies and procedures; and
 - maintaining personnel records and comply with record retention requirements.
- Manage and monitor individual access to and prevent unauthorized access to or use of Company property, including its facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of Company policies and procedures.
- Engage in corporate transactions requiring review of individual records, such as for evaluating potential Company mergers and acquisitions.
- Maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.
- For client marketing purposes.
- Exercise or defend the legal rights of the Company, its employees, affiliates, customers, contractors, and agents.
- Respond to law enforcement requests and as required by applicable law or court order.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

Sensitive Personal Information Use and Disclosure Purposes

We may use or disclose sensitive personal information for the following statutorily approved reasons (**Permitted SPI Purposes**):

- Performing actions that are necessary for our relationship with an individual for employment or partnership and that an average individual in an employment relationship with us would reasonably expect.
- Preventing, detecting, and investigating security incidents that compromise the availability, authenticity, integrity, and or confidentiality of stored or transmitted personal information.
- Defending against and prosecuting those responsible for malicious, deceptive, fraudulent, or illegal actions directed at the Company.
- Ensuring physical safety.
- Short-term, transient use, such as non-personalized advertising shown as part of an employee's current employment with us, if we do not:
 - disclose the sensitive personal information to another third party; or
 - use it to build a profile about the individual or otherwise alter the individual's experience outside their current employment with the Company.
- Services performed for the Company, including maintaining or servicing accounts, providing human resources and employee benefits administration, processing or fulfilling transactions, verifying employee information, processing payments, or providing financing, analytic services, storage, or similar services for the Company.
- Activities required to:
 - verify or maintain the quality or safety of a product, service, or device that we own, manufacture, had manufactured, or control; and
 - improve, upgrade, or enhance the service or device that we own, manufacture, had manufactured, or controlled.

Collecting or processing sensitive personal information not for the purpose of inferring characteristics about an individual.

Additional Categories or Other Purposes

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice. If required by law, we will also seek your consent before using your personal information for a new or unrelated purpose.

We may collect, process, and disclose aggregated or deidentified information about our employees for any purpose, without restriction. When we collect, process, or disclose this aggregated or deidentified information, we will maintain and use it in deidentified form and will not attempt to reidentify the information, except to determine whether our deidentification processes satisfies any applicable legal requirements.

Disclosing, Selling, or Sharing Personal Information

Business Purpose Disclosures

We may disclose the personal information we collect, including sensitive personal information, to others for the business purposes such as to engage service providers to help us administer human resources functions, payroll, benefits, or plans. For example, we may disclose information from the Company's equipment or your use of our network, systems, or equipment to a service provider that provides us with data and cybersecurity services.

We only make these business purpose disclosures under written contracts that describe the purposes, require the recipient to keep the personal information confidential, and prohibit using the disclosed information for any purpose except performing the contract.

In the preceding 12 months, we have disclosed some or all of the categories of personal information listed above for a business purpose. Service providers include companies that do things to help us provide our website and our services as well as professional service providers, such as auditors, lawyers, consultants, accountants and insurers.

Selling or Sharing Personal Information

In the employment context, we do not sell your personal information to third parties and have not sold it in the past 12 months. We do not share your personal information with third parties for cross-context behavioural advertising purposes and have not shared your personal information in the preceding 12 months.

Your Rights and Choices

If you are a California individual, you have the following rights under the CCPA regarding your personal information:

Right to Know and Data Portability

You have the right to request that we disclose certain information to you about our collection and use of your personal information (the "**right to know**"), including the specific pieces of personal information we have collected about you (a "**data portability request**"). Our response will cover the 12-month period preceding the request, although we will honour requests to cover a longer period that do not extend past January 1, 2022, unless doing so would be impossible or involves disproportionate effort. You may exercise your right to know **twice** in any 12-month period. Once we receive your request and confirm your identity we will disclose to you:

- The categories of:
 - personal information we collected about you; and
 - sources from which we collected your personal information.
- The business or commercial purpose for collecting your personal information and, if applicable, selling or sharing your personal information.
- If applicable, the categories of persons, including third parties, to whom we disclosed your personal information, including separate disclosures identifying the categories of your personal information that we:
 - disclosed for a business purpose to each category of persons; and
 - sold or shared to each category of third parties.
- When your right to know submission includes a data portability request, a copy of your personal information subject to any permitted redactions.

Right to Delete and Right to Correct

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions and limitations (the "**right to delete**"). Once we receive your request and confirm your identity, we will delete your personal information from our systems unless an exception allows us to retain it. We will also notify our service providers, contractors, and other recipients to take appropriate action.

You also have the right to request correction of personal information we maintain about you that you believe is inaccurate (the "**right to correct**"). We may require you to provide documentation, if needed, to confirm your identity and support your claim that the information is inaccurate. Unless an exception applies, we will correct personal information that our review determines is inaccurate and notify our service providers, contractors, and other recipients to take appropriate action.

How to Exercise Your Rights

Exercising the Rights to Know, Delete or Correct

To exercise the right to know (including data portability), delete, or correct described above, please submit a verifiable request to us by either:

- Calling us at +1 512 643 6503
- Emailing us at info@MomentumTechnologyGlobal.com

Please describe your request with sufficient detail so we can properly understand, evaluate, and respond to it. You or your authorised agent may only submit a request to know or for data portability twice in a 12-month period.