Volt Information Sciences, Inc. Privacy Policy

Effective Date: May 10, 2019
Updated 1/1/2020 – California Consumer Privacy Act Supplement

---

This Privacy Policy discloses practices for collection, use and protection of your personal information by Volt Information Sciences, Inc. and its subsidiaries, affiliates, and divisions (hereinafter collectively the "Company"). The Company operates in accordance with the EU Data Protection Directives 95/46/EC and 2002/58/EC as amended and updated (the "Directives") as appropriate to the jurisdiction in which Company is trading.

Personal Information the Company Collects

In the course of its business, the Company collects personal information, which was given to or made available to the Company for an intended business function or purpose. The information may include a name combined with a unique identification number, including a social security and/or national identification number, home address, mailing address, e-mail address, social media identifier, driver's license number, birthdate, country location, personal home, or cell/mobile telephone number(s), historical work or education information, compensation/benefits/pay rates, bank account information, pricing, medical or claims information and/or performance data (hereinafter collectively referred to as "Personal Information").

Use and Disclosure of Your Personal Information

Personal Information is used in connection with the Company's business, including providing recruitment, placement, and employment services to our employment candidates, employees, customers and for other lawful purposes.

The Company does not disclose Personal Information except in the following instances:

- With the subsidiaries and affiliates within the Company, as needed;
- With your express consent;
- Where permitted and/or required by our customer/client agreements, including for billing purposes;
- To facilitate job opportunities for our candidates;
- With third party entities, vendors, consultants, agents and/or other service providers engaged to handle or manage some or all of the Personal Information on our behalf, who shall be required to protect Personal Information from dissemination and/or use;
- When we believe disclosure is appropriate to prevent physical harm or financial loss and/or when reasonably necessary to an investigation of suspected or actual illegal activities;
- When required and/or otherwise permitted by law;
- In response to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- If you are a customer/client, the Company may share information with third parties, such as with a credit bureau or agency; and
- In connection with any merger, sale of Company assets or acquisition of all or a portion of the Company's business or with respect to any Company financing.

Data Processing Outside Your Country

We may transfer your information and process it outside your country of residence to wherever Company or our clients or our third-party data processors operate.

Privacy Shield

With respect to Personal Information associated with individuals located in European Economic Area (EEA) countries ("EEA Data Subjects"), the Company complies with the Data Protection Directive 95/46/EC as amended. For a list of the U.S. subsidiaries that adhere to the Privacy Shield principles, please reference our Privacy Shield registration at https://www.privacyshield.gov/list.

To the extent that Personal Information of EEA Data Subjects is transferred to the United States of America, the Company complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information transferred from the EEA to the United States. The Company remains responsible for personal information that is shared under the Onward Transfer Principle with third parties for external processing on Company's behalf.

The Company has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit www.privacyshield.gov.

Notice of material changes to the use or transfer of your Personal Information incompatible with the purpose for which it was originally collected will be provided through our website or by other means so that you may review the changes before you continue your relationship with the Company. If you object to the changes, you must notify of us of your wish to sever your relationship with the Company; otherwise, your continuance of the relationship after the notice means that you are consenting to the changes.

The Company is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission to ensure compliance with the EU-US Privacy Shield principles outlined in this Privacy Policy.

In compliance with the EU-US Privacy Shield Principles, the Company commits to resolve complaints about your privacy and our collection or use of your personal information. JAMS will be the US-based independent organization responsible for reviewing and resolving complaints about our Privacy Shield compliance. We ask that you first submit any such complaints directly to us via Privacy@volt.com. If you are not satisfied with our response, please contact JAMS at https://jamsadr.com/eu-us-privacy-shield. In the event your concern still is not addressed by JAMS, you may be entitled to a binding arbitration under Privacy Shield and its principles.

The Company commits to cooperate with EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU in the context of the employment relationship.

Solicitations and/or Marketing Contacts

The Company does not sell, convey and/or communicate customer/client, business associate, supplier, vendor, employee and/or candidate Personal Information to third parties for purposes of direct mail, telemarketing, and/or related promotions, solicitations or marketing contacts.

Management of Personal Information

The Company uses a combination of reasonable security technologies, policies and procedures, and non- disclosure, confidentiality and/or other forms of agreement(s) to help protect your Personal Information from unauthorized access, destruction, use, modification or disclosure. In the event that local law in the country of disclosure or use of Personal Information is more stringent than the requirements set out in this policy, local law will prevail over this policy to the extent necessary to meet the requirements of that legislation.

Changes to our Privacy Policy

The Company, in its sole and absolute discretion, reserves the right to supersede, modify, supplement, replace or eliminate this Policy, which shall be effective upon publication on the Company's website.

Requests to access and to make changes in Personal Information

In the event that any individual wishes to access, change, correct or delete Personal Information and its treatment as covered by this Privacy Policy, he or she must submit a written request to privacy@volt.com. You have the right to request that usage or disclosure of your information be limited, however such usage of your information as described above may be necessary for the performance of recruitment, placement, and employment services that we provide to you. As such, a request to withdraw consent, object to processing, limit usage or erase your information may result in Volt being unable to continue providing its services such as recruitment, placement or employment services.

Who to Contact About this Privacy Policy?

Any questions or complaints regarding the Company's Privacy Policy should be directed to:

Volt Information Sciences, Inc.
959 Route 46 East, Suite 201
Parsippany, NJ 07054
Attn: Vice President Risk Management
Privacy@volt.com

PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

(Supplement to Volt's Privacy Policy)

Volt has adopted this notice to comply with the California Consumer Privacy Act of 2018 ("CCPA") and other privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice. This notice should be read in conjunction with our privacy policy above.

Information We Collect

Volt is a human resources service provider and in order to perform our services, we collect and use information about employees, job applicants and interested parties. This policy outlines the type of information we collect, how we use that information and your privacy rights in relation to that information. We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("personal information").

In particular, we have collected the following categories of personal information from consumers within the last twelve (12) months:

A. Identifiers

A legal name (first and last), alias, physical address, postal address, unique personal identifier, mobile or other telephone number, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar personal identifiers.

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. Some personal information included in this category may overlap with other categories.

C. Protected classification characteristics under California or federal law.

Age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or 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).

D. Correspondence

Records of correspondence including mobile text messages and email correspondence relating to job applications, job performance, feedback and other discussions.

E. Internet or Other Similar Network Activity.

We use session tracking to customize your experience on our websites.

F. Geolocation Data.

Physical location.

G. 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, and sleep, health, or exercise data.

H. Professional or Employment-Related Information.

Current or past job history or performance evaluations.

I. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).

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, student identification codes, student financial information, or student disciplinary records.

J. Inferences drawn from other personal information.

Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
    - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Sources of Information we collect

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

- Directly from applicants and/or employees. For example, information entered in connection with a job application.
- Directly or indirectly from our clients or their agents. For example, candidates referred to us by clients or other resource providers.
- Directly and indirectly from activity on our website (www.volt.com). For example, from submissions through our website portal or website usage details collected automatically.
- From third-parties that interact with us in connection with the services we perform. For example, job boards, social media sites, employment verification and background check service providers.
- From government authorities. For example, obtaining security clearance and fulfilling garnishment requests.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following business purposes:

- To provide services for which the information was provided. For example, finding potential jobs/assignments for candidates, communicating your interest in a position to our clients, qualifying potential employees for assignments, fulfilling training requirements, etc.
- To provide you with information or services that you request from us.
- To provide you with email alerts, event registrations and other notices concerning our services, or events or news, or investor information that may be of interest to you.
- To monitor and maintain compliance with internal policies and procedures.
- To investigate and respond to complaints or other incidents.
- To carry out our obligations and enforce our rights arising from any contracts entered into between us.
- To fulfill our obligations to tax authorities, federal, state and other regulators
- To respond to law enforcement requests and as required by applicable law, subpoena, court order, or governmental regulations.
- As disclosed to you when collecting your personal information or as otherwise set forth in the CCPA.

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.

Are you required to provide personal information?

While you are not required to provide us with your personal information, it is often not possible for us to perform our services to you and our clients without personal information.

Sharing Personal Information

We may disclose your personal information to a third party for the purposes of performing our services to you and our clients. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to comply with all applicable laws and maintain the confidentiality of such information.

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

Category A:	Identifiers.
Category B:	Customer Records personal information categories.
Category C:	Protected classification characteristics under California or federal law.
Category D:	Correspondence
Category F:	Geolocation data
Category H:	Professional and Employment-related information

We disclose your personal information for a business purpose to the following categories of third parties:

- To our suppliers: We engage suppliers to carry out administrative and operational work in support of our services and our relationship with you. The supplier(s) are subject to contractual and other legal obligations

to preserve the confidentiality of your data and to respect your privacy, and they will only have access to and use the data they need to perform their functions. Some examples of these suppliers include, for example, background check vendors and drug screening vendors, IT Cloud providers (who host or support our IT systems, which contain you Identifiers), premises management systems (used for physical security at our buildings) and back office finance and accounting management providers (who need to handle details of certain individuals in order to process accounts payable and receivable. We also work with other human resource providers who may have a direct relationship with clients but utilize Volt employees for their assignments;

- To affiliated companies: Our affiliated companies are located in the U.S. and internationally; different Volt companies fulfill different functions and as result, your information will be shared with them for different reasons, however all for the furtherance of the services we provide to you and our clients;
- To our clients: As a job candidate, we will share your data with our clients or prospective clients of ours that are offering jobs/assignments you may be interested in, or that we believe may be interested in your profile;
- To government & law enforcement: We also will share your data with government regulators and/or law enforcement agencies if, at our sole discretion, we are legally obliged ,authorized or we believe it is prudent or reasonably necessary to do so; and/or
- To other third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we may provide to you.

In the preceding twelve (12) months, we have not sold any personal information.

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your request, including verifying your identity, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources of the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).

Deletion Request Rights

Under certain circumstances, you may have the right to request that we delete personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information, provide or continue to provide the service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.

- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and/or deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at 1-833-976-1993;
- Sending an email to privacy@volt.com with specific information about your request; or
- Completing our Personal Information Request Webform available at CCPA Webform.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, 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.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to 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. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

Upon receiving a request, we may contact you via email, text message or telephone to verify your identity by asking additional security questions in order to match your identity with the information we maintain about you.

We endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the reason in writing. If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding receipt of the verifiable consumer request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will notify you through a notice on our website homepage.

Contact Information

If you have any questions about this notice, our Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, please do not hesitate to contact us at: privacy@volt.com.