Privacy Shield Policy

ClearCompany Inc. (hereafter, "ClearCompany") has adopted this Privacy Shield Policy (hereafter, "Policy") to establish and maintain an adequate level of Personal Data privacy protection. This Policy applies to the processing of Personal Data that ClearCompany obtains from Subscribers located in the European Union or Switzerland.

ClearCompany complies with the US-EU and US-Swiss Privacy Shield Framework as set forth by the United States Department of Commerce regarding the collection, use, and retention of personal information from Subscribers in European Union member countries. ClearCompany has certified that it adheres to the Privacy Shield Privacy Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement and liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Privacy Principles, the Privacy Shield Privacy Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov.

The Federal Trade Commission (FTC) has jurisdiction over ClearCompany's compliance with the Privacy Shield.

All ClearCompany employees who handle Personal Data from Europe and Switzerland are required to comply with the Principles stated in this Policy.

Capitalized terms are defined in Section 14 of this Policy.

I. SCOPE

This Policy applies to the processing of Personal Data that ClearCompany receives in the United States concerning Data Subjects who reside in the European Union and Switzerland. ClearCompany provides products and services to businesses (“Subscribers”) for the purpose of hiring and managing employees.

This Policy does not cover data from which individual persons cannot be identified or situations in which pseudonyms are used. (The use of pseudonyms involves the replacement of names or other identifiers with substitutes so that identification of individual persons is not possible.)

II. RESPONSIBILITIES AND MANAGEMENT

ClearCompany has designated the President to oversee its information security program, including its compliance with the EU-US and US-Swiss Privacy Shield programs The President shall review and approve any material changes to this program as necessary. Any questions, concerns, or comments regarding this Policy also may be directed to legal@clearcompany.com.

ClearCompany will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Data that it collects. ClearCompany personnel will receive training, as applicable, to effectively implement this Policy. Please refer to Section 7 for a discussion of the steps that ClearCompany has undertaken to protect Personal Data.

III. RENEWAL / VERIFICATION

ClearCompany will renew its EU-US and US-Swiss Privacy Shield certifications annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, ClearCompany will conduct an in-house verification to ensure that its attestations and assertions with regard to its treatment of Individual Customer Personal Data are accurate and that the company has appropriately implemented these practices. Specifically, as part of the verification process, ClearCompany will undertake the following:

- Review this Privacy Shield policy and its publicly-posted website privacy policy to ensure that these policies accurately describe the practices regarding the collection of Personal Data
- Ensure that the publicly posted privacy policy informs Individual Customers of ClearCompany's participation in the EU-US and US-Swiss Privacy Shield programs and where to obtain a copy of additional information (e.g., a copy of this Policy)
- Ensure that this Policy continues to comply with the Privacy Shield principles
- Confirm that Data Subjects are made aware of the process for addressing complaints and any independent dispute resolution process (ClearCompany may do so through its publicly posted website, Subscriber contract, or both)
- Review its processes and procedures for training Employees about ClearCompany's participation in the Privacy Shield programs and the appropriate handling of Data Subjects' Personal Data
- ClearCompany will prepare an internal verification statement on an annual basis.

IV. COLLECTION AND USE OF PERSONAL DATA

ClearCompany provides an online human resource management software suite (hereafter, "System") to its Subscribers, who use the System to support business processes associated with the hiring and management of employees or contractors.

ClearCompany collects Personal Data from Data Subjects who are employees of a Subscriber or seeking employment with a Subscriber. For example, a Data Subject seeking a job with a Subscriber company may submit an application through the System.

The Personal Data that we collect will vary based on the Data Subject's role as an employee or job-seeker, and which ClearCompany products the Subscriber has purchased and is using. As a general matter, ClearCompany collects the following types of data from Data Subjects applying for employment at a Subscriber: name, address, and contact information; work history and education as would typically be found on a resume or CV; and responses to job-specific qualification questions which the Subscriber asks of applicants to specific jobs. For Data Subjects employed by a Subscriber, additional data may include completed forms associated with their employment, as well as performance reviews and other human resource management business processes which the System is used to conduct online.

The Personal Data that we collect from Data Subjects is used exclusively for the business purposes of the Subscriber, to whom we act as a data processor. ClearCompany does not make any independent commercial use of Data Subjects' Personal Data.

ClearCompany uses Personal Data that it collects directly from Data Subjects and for its partners indirectly in its role as a service provider for the following business purposes, without limitation:

- maintaining and supporting its products, delivering and providing the requested products/services, and complying with its contractual obligations related thereto (including managing transactions, reporting, invoices, renewals, and other operations related to providing services to a Individual Customer);
- satisfying governmental reporting, tax, and other requirements (e.g., import/export);
- storing and processing data, including Personal Data, in computer databases and servers located in the United States;
- verifying identity (e.g., for online access to accounts);
- as requested by the Subscriber;
- for other business-related purposes permitted or required under applicable local law and regulation;
- and as otherwise required by law.

V. DISCLOSURES / ONWARD TRANSFERS OF PERSONAL DATA

Except as otherwise provided herein, ClearCompany discloses Personal Data only to Third Parties who reasonably need to know such data only for the scope of the initial transaction and not for other purposes. Such recipients must agree to abide by confidentiality obligations.

ClearCompany does not share data on individuals with non-agent third parties. If this practice should change in the future, we will notify our Subscribers who provide the subject data and instruct our Subscribers as to how they can offer opt-out choice to affected individuals.

ClearCompany also may disclose Personal Data for other purposes or to other Third Parties when a Data Subject has consented to or requested such disclosure. Please be aware that ClearCompany may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. ClearCompany is liable for appropriate onward transfers of personal data to third parties.

VI. SENSITIVE DATA

ClearCompany may collect Sensitive Data from Data Subjects where such data is an intrinsic part of the business process which the System is being used to support. For example, many Subscribers collect data on each job applicant’s race and gender in order to comply with laws forbidding racial or gender-based discrimination in hiring decisions. ClearCompany only shares Sensitive Data with Third Parties who act as a data processor (for example, Amazon Web Services may be used for storage of certain types of data in the System), or who act as an agent providing a specific task in service of the Subscriber’s business processes. ClearCompany does not share Sensitive Data on individuals with non-agent third parties. If this practice should change in the future, we will notify our Subscribers who provide the Data Subjects’ Sensitive Data and instruct our Subscribers as to how they can offer opt-out choice to the Data Subjects.

VII. DATA INTEGRITY AND SECURITY

ClearCompany uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. ClearCompany has implemented physical and technical safeguards to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alternation, or destruction. For example, electronically stored Personal Data is stored on a secure network with firewall protection, and access to ClearCompany's electronic information systems requires user authentication via password or similar means. ClearCompany also employs access restrictions, limiting the scope of Employees who have access to Data Subjects’ Personal Data.

Further, ClearCompany uses secure encryption technology to protect certain categories of data. All data is encrypted (for example using HTTPS) when it is transmitted outside ClearCompany’s

firewall, and certain types of data are encrypted at all times in the System. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

VIII. NOTIFICATION

ClearCompany notifies Data Subjects and Subscribers about its adherence to the US-EU Privacy Shield principles through its publicly posted website privacy policy, available at: http://info.clearcompany.com/hubfs/ClearCompany-PrivacyShield-2017.pdf

IX. ACCESSING PERSONAL DATA

ClearCompany personnel may access and use Personal Data only if they are authorized to do so and only for the purpose for which they are authorized.

X. RIGHT TO ACCESS, CHANGE OR DELETE PERSONAL DATA

Right to Access.

Data Subjects have the right to know what Personal Data about them is included in the System and to ensure that such Personal Data is accurate and relevant for the purposes for which the Subscriber collected it. Data Subjects may review their own Personal Data stored in the databases and correct, erase, or block any data that is incorrect, as permitted by applicable law and Subscriber policies.

Upon reasonable request and as required by the Privacy Shield principles, ClearCompany allows Data Subjects access to their Personal Data, in order to correct or amend such data where inaccurate. Individual Customers may edit their Personal Data by logging into their online profile or by contacting ClearCompany by phone or email to legal@clearcompany.com. In making modifications to their Personal Data, Data Subjects must provide only truthful, complete, and accurate information. To request erasure of Personal Data, Data Subjects should submit a written request to ClearCompany, 11 Beacon St., 14th Flr., Boston, MA 02108, United States of America. For convenience, Data Subjects may also send a copy of such request to legal@clearcompany.com, however, such request shall not be considered binding under this Policy. In its role as a data processor, ClearCompany may notify our Subscriber of any requests it has received to change or erase data concerning a Data Subject who is a current, former, or prospective employee of the Subscriber, prior to changing or erasing any data.

Requests for Personal Data.

ClearCompany will track each of the following and will provide notice to the appropriate parties under law and contract when either of the following circumstances arise: (a) legally-binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law or regulation; or (b) requests received from the Data Subject. If ClearCompany receives a request for access to his/her Personal Data from a Data Subject, then, unless otherwise required under law or by contract with such Subscriber, ClearCompany will refer such Data Subject to the Subscriber.

Satisfying Requests for Access, Modifications, and Corrections.
ClearCompany will endeavor to respond in a timely manner to all reasonable written requests to view, modify, or inactivate Personal Data.

XI. CHANGES TO THIS POLICY

This Policy may be amended from time to time, consistent with the Privacy Shield Principles and applicable data protection and privacy laws and principles. We will make employees aware of changes to this policy either by posting to our intranet, through email, or other means. We will notify Subscribers and Data Subjects if we make changes that materially affect the way we handle Personal Data previously collected, and we will allow them to choose whether their Personal Data may be used in any materially different manner.

XII. QUESTIONS OR COMPLAINTS

Subscribers and Data Subjects under EU jurisdiction may contact ClearCompany with questions or complaints concerning this Policy at the following address:

ClearCompany
11 Beacon St., 13th Floor
Boston, MA 02108 USA
Attn: Privacy Shield Inquiry

For convenience, notices and inquiries may be copied by email at legal@clearcompany.com, however such notices and inquiries shall be considered binding under this Policy only if received by postal mail at the address above.

XIII. ENFORCEMENT AND DISPUTE RESOLUTION

In compliance with the US-EU and US-Swiss Privacy Shield Principles, ClearCompany commits to resolve complaints about your privacy and our collection or use of your personal information. EU or Swiss individuals with questions or concerns about the use of their Personal Data should contact us at: legal@clearcompany.com.

If a Data Subject's question or concern cannot be satisfied through this process, ClearCompany has further committed to refer unresolved privacy complaints under the Privacy Shield Frameworks to an independent dispute resolution mechanism operated by the Council of Better Business Bureaus.

If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed by ClearCompany, EU and Swiss individuals may bring a complaint before the BBB EU Privacy Shield. Information about how to file a complaint before the BBB EU Privacy Shield program can be found at: www.bbb.org/EU-privacy-shield/for-eu-consumers/.

Finally, as a last resort and in limited situations, EU or Swiss individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

XIV. DEFINED TERMS

Capitalized terms in this Privacy Policy have the following meanings:

"Subscriber" means a client company of ClearCompany that collects Personal Data on Data Subjects residing in the EU or Switzerland. The term also shall include any authorized individual agent or representative of an individual customer of ClearCompany, and all employees of the Subscriber.

"Data Subject" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics. For Customers residing in Switzerland, a Data Subject also may include a legal entity.

"Europe" or "European" refers to a country in the European Union.

“Employee” refers to an employee or contractor of ClearCompany.

"Personal Data" as defined under the European Union Directive 95/46/EC means data that personally identifies or may be used to personally identify a person, including an individual's name in combination with country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone number, e-mail address, user ID, password, and identification numbers. Personal Data does not include data that is de-identified, anonymous, or publicly available. For Switzerland, the term "person" includes both a natural person and a legal entity, regardless of the form of the legal entity.

"Sensitive Data" means Personal Data that discloses a Data Subject's medical or health condition, race or ethnicity, political, religious or philosophical affiliations or opinions, sexual orientation, or trade union membership.

“System” refers to the suite of human resource management software products which Subscriber companies purchase from ClearCompany.

"Third Party" means any individual or entity that is neither ClearCompany nor the Subscriber, nor an employee, agent, contractor, or representative of same.