

## **BrightLink Privacy Policy**

This website is operated by Bright Link Technology, LLC (“BrightLink”, “we”, “us” and “our”), with its principal place of business located at 502 Bombay Lane, Roswell GA 30076, USA. This privacy policy (“Privacy Policy”) explains to visitors (“you” and “your”) how we collect, use and disclose personal information concerning visitors to this website and users of our products and Services.

CERTAIN BrightLink WEBSITES AND SERVICES, INCLUDING BUT NOT LIMITED TO PASSWORD PROTECTED SITES AND SERVICES, CONTAIN TERMS AND CONDITIONS WHICH CONTAIN PRIVACY STATEMENTS THAT ARE SPECIFIC TO THE PURPOSES OF THOSE WEBSITES, PRODUCTS AND SERVICES. SUCH PRIVACY STATEMENTS ARE IN ADDITION TO THIS PRIVACY POLICY and shall prevail In the event of any inconsistency between such Privacy Statements and this Privacy Policy.

### **Commitment to Privacy**

BrightLink is committed to respecting your privacy. We help people reach their career goals by providing professional certifications, specialized certificate programs, exam preparation and study tools and analytic reporting. We may work with you directly or through your school or employer, or through another organization you use, such as a training center.

This Privacy Policy describes how we collect, use, share and protect information about you. When you interact with or use the products, services or websites of BrightLink (“Services”) or it’s clients, you consent to such collection, use and sharing of your information as described in this Privacy Policy, our Terms of Use for our websites and the Terms and Conditions provided during account registration with BrightLink or any BrightLink product.

Our privacy practices may vary among the states, countries and regions in which we operate in order to comply with applicable legal requirements. We are committed to compliance with the EU-U.S. and SWISS-U.S. Privacy Shield.

## **Consent**

When you interact with or use our Services, and when you enter any personal information into any of our other Services, you are consenting to the collection, use, and transfer of your personal information as outlined in this Privacy Policy, our Terms of Use for our websites and the Terms and Conditions provided during account registration with BrightLink or any BrightLink product. If you are located outside the United States, your use of, and entry of personal information into, any of the Services constitutes your consent to the transfer of your personal information into the United States. Although we do not require that you provide any sensitive personal information (such as ethnicity or race, religious beliefs or medical conditions), your provision of any such sensitive information in using our Services is your express consent to the collection, use and transfer of such information.

If you do not consent to the terms of this Privacy Policy, please do not continue to use our Services.

## **Data Collection**

BrightLink is dedicated to protecting the privacy of all personal information collected through this website and our Services. We may collect information from you (directly or through third party vendors we retain) or from a third party who is authorized by you or otherwise permitted by applicable law to share information with us (for example, your school or employer) in situations such as the following:

- Website visit. When you provide information during a login process, when you access certain portions of our website, when you ask us to provide more information, when you purchase online or in connection with any online employment applications.

- Registration. When you create an account on our Services, make a purchase, register or login to access or use functions or features.
- Communications. When you communicate with us.
- Learning and Certification Activities. When you use our Services, information about your grades and scores, instructor feedback and comment, your personal learning behaviors, and various metrics related to your learning of particular subject matters is recorded.
- Surveys and Research. If you participate in our research studies about our products or the industries and professions we support or our market research surveys or programs.
- Forums. If you participate in our forums, blogs, intranets, chat rooms, "wikis" or other similar features.
- Subscriptions. If you subscribe to one of our newsletters or request text alerts.
- Social Media. If you use or interact with our Services on social media and networking pages and applications, such as Facebook, Instagram, LinkedIn and others.

We also may collect information about you from other sources. We work closely with third parties (for example, business partners, service providers, sub-contractors, educational institutions, analytics providers, search information providers, fraud protection services) and may receive information about you from them. We may also collect and process information about you that your Institution or an organization (such as a professional, governmental, oversight or other organization) with which you are, or previously were, affiliated provides to us. We may also collect and process information about you that we receive from other sources including organizations that are our customers (which might be your Institution, for example), organizations that provide our products or services by way of a co-branded or private-labeled platform, product, service, website or application, and organizations that sponsor surveys or programs in connection with our Services. If you use our Services through a third party, please contact that third party first if

you have any questions about the data they collect from you and share with us. If they do not address your concerns, please contact us.

To the extent permitted by applicable law, we may collect data in an automated manner and make automated decisions, including using machine learning algorithms, about users of our Services in order to provide or optimize the Services offered and/or delivered, for security or analytics purposes, and for any other lawful purpose. Our Services may collect certain information by automated means when you access or use our Services. This information may include, but is not limited to, usage details, Internet Protocol ("IP") address, browser type, browser language, devices you use, access times, the sites linked from, pages visited, applications downloaded or accessed, links and features used, content viewed or requested, information collected through cookies and other such information. We generally collect this information to improve our Services for our users, to learn about our users' interests and enhance the Services we provide, for security and analytics purposes, and for other lawful purposes. To learn more, please see our "Cookies and Similar Technologies" section below.

Educational Records (FERPA) and Medical Records (HIPAA). In providing our Services, we are not directly covered by the U.S. Federal Educational Rights and Privacy Act ("FERPA") or the U.S. Health Insurance Portability and Accountability Act ("HIPAA"). However, to the extent we are required to do so by contract with an organization who provides your personal information to us or with whom we share your information, and to the extent that such personal information provided to us is subject to FERPA or an equivalent law or regulation for your state or country of residence, or HIPAA or an equivalent law or regulation for your state or country of residence, we will comply with such applicable law as required by such contract.

### **How We May Use Your Information.**

We use your information to provide you, either directly or through a third party, with our Services. We also may use your information to support our business functions, such as fraud prevention, marketing, analytics and legal functions.

We may use your information:

- To fulfill your requests for Services and communicate with you about those requests.
- To set up your account and verify your identity when you register for our Services.
- To process your payments - but we do not retain your credit card data after a payment has been processed.
- To monitor, record, analyze and report on your activity, interactions and engagement with our Services.
- To track and analyze and report on your progress, success, results, performance, registrations, incomplete attempts, and results in connection with our certification and specialized certificate program Services. If your use of our Services is in connection with a school, employer, institution or other organization ("your Institution"), we may share your data with your Institution, its instructors and staff, and other parties associated with or required by your Institution.
- To perform research and analysis for our Services and to further develop and improve our Services or to perform research concerning the industries and professions we serve.
- To perform benchmarking analytics and general metrics about your performance or, after anonymizing, de-identifying or aggregating the data, your Institution's performance as compared to other schools and institutions and other BrightLink customers.
- To analyze technical data such as cookies, content viewed, IP address, device use, site volume and load.

- To verify compliance with license terms.
- To support and personalize our Services, websites, mobile services, and advertising.
- To inform you of new products, services or promotions we may offer.
- For research, analysis, benchmarking or surveys.
- To engage you in our social media platforms.
- To protect the security and integrity of our Services, content, and our business.
- To respond to reviews, comments, or other feedback you provide us.
- To comply with applicable legal or regulatory requirements and our policies, protect against criminal activity, claims and other liabilities.
- For any other lawful purpose for which the information is provided.

We also may use, process, transfer, and store any data about you in an anonymous, aggregated manner. We may combine personal information with other information, collected online and offline, including information from third party sources.

We may also use information in other ways with your consent or as permitted by applicable law.

### **Information Sharing**

To the extent permitted by applicable law, we may share information about you, including your personal information, as set forth below or as otherwise described in this Privacy Policy or the terms and conditions for use of the Services:

- Affiliates, Agents and Partners. We may share information with our parent corporations and affiliates (or any business partner or agent acting on our behalf) worldwide as necessary to provide you with the Services, each such parent corporation, affiliate, business partner, and agent will be under the same obligations

as is BrightLink to protect the confidentiality of your information and protect your privacy.

- **Analytics and Reporting.** We may share your information to (i) analyze and provide certain information about your learning and academic performance to you, your Institution, including other parties associated with and required by your Institution, and your instructor(s) or supervisor(s) from your Institution; (ii) generate reports and analytics for use by you, your Institution, other parties associated with and required by your Institution, and your instructor(s) regarding the learning and academic performance of an entire class or cohort at your Institution and (iii) generate reports and analytics to be used by researchers or third parties in the industries or fields that we support to better understand changes and trends in such industries or fields.
- **Service providers.** We may share information with agents, contractors, service providers, vendors, business partners, and other third parties we use to support our business and Services. We may share information to provide technical support to you and your Institution, its instructor(s) or staff. Some examples of third parties we work with are shippers, payment servicers, information processors, financial institutions, data centers, educational institutions you attend, other organizations you are affiliated with, or their support service providers. Such third-party providers may perform technical operations such as database monitoring, data storage and hosting services and customer support software tools. Such third parties may access, process or store personal data in the course of providing these services.
- **Your Institution and other Organizations.** We may share information about your use of our Services with your Institution and its faculty or staff, and other parties associated with or required by your Institution. We also may share information with governmental agencies, oversight organizations, professional organizations, certification or accreditation organizations, and industry self-regulatory organizations.
- **Fraud Prevention.** We may share your information to confirm your identity to ensure only authorized users are accessing our Services and for general security.

- Mergers, Acquisitions, Divestitures. We may share, disclose or transfer information about you to a buyer, investor, new affiliate, or other successor in the event BrightLink, its parent companies or affiliates, or any portion, group or business unit thereof, undergoes a business transition, such as a merger, acquisition, consolidation, reorganization, divestiture, liquidation or dissolution (including bankruptcy), or a sale or other transfer of all or a portion of any assets or during steps in contemplation of such activities (e.g., negotiations and due diligence).
- Law Enforcement and National Security. We may share information to comply with any law or directive, judicial or administrative order, legal process or investigation, warrant, subpoena, government request, regulatory request, law enforcement or national security investigation, or as otherwise required or authorized by law.
- Protection of Rights, Property or Safety: We may also share information if, in our sole discretion, we believe disclosure is necessary or appropriate to protect the rights, property or safety of any person, or if we suspect fraud, illegal activity, abuse or testing misconduct has taken place.

We also may share information to fulfill any other purpose for which you have provided information to us; for any other purpose disclosed by us or the third party with whom you are interacting when you provide the information; to enforce our rights arising from any contracts; for billing and collection; or as otherwise permitted under applicable law.

## **Data Security**

Security of your personal information is of the utmost importance to us. We use administrative, technical and physical safeguards to protect the security of your personal information from unauthorized disclosure. We take reasonable security measures to secure your personal information against unauthorized access, loss, use, disclosure, or alteration by third parties and unauthorized employees. Despite our efforts, we cannot guarantee the security of your personal information during its transmission or its storage in our systems. No method of transmitting or storing electronic information is ever completely secure. We make no warranty, express, implied, or otherwise, that your information will never be accessed, used or released

in a manner that is inconsistent with this Privacy Policy. We are not responsible for any damages or liabilities relating to any security incidents, and we disclaim all representations and warranties regarding such matters to the fullest extent permitted by law. Where required under law, we will notify you of any loss, misuse or alteration of personal information that may affect you so that you can take the appropriate actions for the due protection of your rights. We review our security procedures periodically to consider appropriate new technology and updated methods.

If information is transmitted to us using a means that is outside our systems, or if you transmit information to a third party, we cannot guarantee the security of information during transmission. Any such unsecured transmission is at your own risk. We recommend that you use appropriate security measures to protect your information.

### **Correction of Your Personal Information**

Accuracy is a top priority for us. You can ensure that any contact data is up-to-date and can correct, update or delete inaccuracies to the information by either logging into your account to review and maintain your information or by contacting customer service. In certain situations, you may need assistance from customer service in making a change. For example, if you received a certification and then realized that your name was misspelled, we may need to take certain steps to verify your identity before making the change, ensure that your name change is linked to all of your certification records and, in some states or countries, that the oversight agency receives the correction. We will respond to your request to make changes to your records as soon as reasonably possible.

We will attempt to answer all requests that we correct the data if it is inaccurate or delete it as long as we are not required to retain it by law or for legitimate business purposes.

In addition, to protect your privacy, we may require you to prove your identity before granting access to, or agreeing to update, correct or delete your personal information.

Not all information about you can be changed. For example, we may have records about how much time you spent working in a training module. Although this information is linked to you, it may not be changed and, in certain instances, it may be subject to government or regulatory oversight. Similarly, learning data, assessment scores and certification status kept in BrightLink systems may not be changed by you, although you should contact us if you believe such data is not accurate.

### **Cookies and other Tracking Devices**

When you visit our websites, you are offered an opportunity to accept our placement of cookie. This section provides more information about our use of cookies and our policies.

We may use cookies and similar technologies to operate and improve our Services, as well as to simplify our interaction with you. A "cookie" is a unique numeric code that we transfer to your computer so that we can keep track of your interests and/or preferences and recognize you as a return visitor to the websites. We may use cookies, log files, pixel tags, web bugs, web beacons, clear GIFs, Local Storage Objects (LSOs) such as HTML5 and Flash or other similar technologies to collect information about the ways you interact with and use our Services, to support and enhance features and functionality, to monitor performance, to personalize content and experiences, for marketing and analytics, and for other lawful purposes. We may also engage third party service providers to provide advertisements and promotions on our behalf, or authorize third parties to advertise and market products and services via our Services.

We may use the following types of cookies and similar technologies:

- Strictly necessary cookies required for the operation of our Services. They include, for example, cookies that enable you to log into secure areas.

- Analytical/performance cookies that collect information about how you use our Services. They allow us to recognize and count the number of visitors and to see how visitors move around our website. This helps us to improve the way our website works. These cookies are sometimes placed by third party providers of web traffic analysis services.
- Functionality cookies that remember choices you make and recognize you when you return. This enables us to personalize our content, greet you by name and remember your preferences (for example, your choice of language or region).
- Targeting cookies that collect information about your browsing habits such as the pages you have visited and the links you have followed. We use this information to make our website more relevant to your interests, and, if we enable advertising, to make advertising more relevant to you, as well as to limit the number of times you see an ad. These cookies are usually placed by third-party advertising networks. They remember the other websites that you visit and this information is shared with third-party organizations, for example advertisers.

Most internet browsers accept cookies by default. You can block cookies by activating the setting on your browser that allows you to reject all or some cookies. The help and support area on your internet browser should have instructions on how to block or delete cookies. Some web browsers (including some mobile web browsers) provide settings that allow you to control or reject cookies or to alert you to when a cookie is placed on your computer, tablet or mobile device. Although you are not required to accept cookies, if you block or reject them, you may not have access to all of the features available through our Services, such as tests, trainings or other activities.

For more information, visit the help page for your web browser or see <http://www.allaboutcookies.org> or visit [www.youronlinechoices.com](http://www.youronlinechoices.com) which has further information about behavioral advertising and online privacy.

We may use third party analytics such as Google Analytics or similar analytics services. For information on how Google processes and collects your information

regarding Google Analytics and how you can opt-out, please see <https://tools.google.com/dlpage/gaoptout>.

We may use third-party advertisers to serve or track advertisements on or relating to the Services. These third parties may use cookies and other tracking and analytical technologies to, among other things, record which ads your browser has loaded and which pages you were viewing when ads were delivered or accessed. Information so collected is subject to the privacy policies of those third parties which you should carefully review. We have limited or no control over third party use of cookies.

**Cross Device Tracking.** When you use your mobile device to interact with us or our Services, we may receive information about your mobile device, including a unique identifier for your device. We and our service providers and third parties we collaborate with, including ad networks, may use cross-device/cross-context tracking. For example, you might use multiple browsers on a single device, or use various devices (such as desktops, smartphones, and tablets), which can result in your having multiple accounts or profiles across these various contexts and devices. Cross-device/cross-context technology may be used to connect these various accounts or profiles and the corresponding data from the different contexts and devices.

## **Links**

Our Sites or Services may contain links or other connections to other third-party websites, platforms, products, services or applications that are independent of our Services. The information collection practices and privacy policies of these third parties may differ from ours. BrightLink provides links to you only as a convenience, and the inclusion of any link does not imply affiliation, endorsement or adoption by BrightLink of any site or any information contained therein.

When you leave our Sites, these Terms will no longer govern your Internet browser session. Your use of any site to which you navigate from our Sites will be subject to

that site's terms of use, if any, and its privacy and data gathering policies. It shall be your sole responsibility to review the applicable terms and policies, including privacy and data gathering practices, of any site to which you navigate from the Sites. We recommend that you carefully read their policies.

### **Data Retention**

To the extent permitted by applicable law, we may retain your information for as long as your account is active or as long as is reasonably necessary to provide you with our Services or as needed for other lawful purposes. We may retain cached or archived copies of your information. We may be required to retain some of your data for a longer period of time because of various laws and regulations or because of contractual obligations. We also will retain your information as long as reasonably necessary to comply with our legal obligations, resolve disputes and enforce our agreements

### **Telephone Consumer Protection Act Notice**

We may use your information to make business, informational and collections calls relating to our Services to all telephone numbers, including cellular numbers or mobile devices, you choose to provide on your account or in registering for any of our Services. You agree such calls may be pre-recorded messages or placed with an automatic telephone dialing system. In addition, you agree that we may send service or account related text messages to cellular phone numbers you provide to us, and you agree to accept and pay all carrier message and data rates that apply to such text messages. If you choose to provide an email or other electronic address on your account, you acknowledge and consent to receive business and informational messages relating to our Services at such address, including collections messages, and you represent and warrant that such address is your private address and is not accessible or viewable by any other person.

### **Additional Notices to California Residents**

Under California's "Shine the Light" law, California residents who provide personal information in obtaining products or services for personal, family or household use may be entitled to request and obtain from us, once per calendar year, information about customer information we have shared, if any, with other businesses for such other businesses' own direct marketing uses. If applicable, this information would include the categories of resident information and the names and addresses of those businesses with which we shared such resident information for the immediately prior calendar year. To obtain this information, please email us at [info@BrightLinknow.com](mailto:info@BrightLinknow.com) with "Request for California Privacy Information" in the subject line of your message, or mail your request to us at the address set forth below:

ATTN: Legal Department - California Privacy Request

BrightLink Technology, LLC

502 Bombay Lane, Roswell, GA 30076

Please include sufficient personal identification information so that we can process your request, including name, mailing address, and email address if you want to receive a response by email.

If you are a California resident under age 18 and are a registered user of any of our Services, then you may request that we remove any content or information that you posted on our websites, online services, online applications, or mobile applications ("User Content"). To request removal of your User Content, please send a detailed description of the specific User Content you want us to remove to the email or regular mail address set forth above. We reserve the right to request that you provide information that will enable us to confirm that the User Content that you want removed was posted by you.

We will make a good faith effort to delete or remove your User Content from public view as soon as reasonably practicable. Please note, however, that your request that we delete your User Content does not ensure complete or comprehensive removal of your User Content. Your User Content may remain on backup media, cached or

otherwise retained by us for administrative or legal purposes or your User Content may remain publicly available if you or someone else has forwarded or re-posted your User Content on another website, online service, online application or mobile application prior to its deletion. We may also be required by law to not remove (or allow removal) of your User Content.

### **Class Action Waiver**

YOU AND WE AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR OUR INDIVIDUAL CAPACITY AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING.

### **Employees and Contractors; Job Applicants**

Employees and Contractors: If you are an employee or contractor of BrightLink, its parent companies or affiliates please contact the Human Resources Department for our privacy policy for employees and contractors. This Privacy Policy is separate from our internal privacy policy for employees and contractors.

Job Applicants: In connection with a job application or inquiry, you may provide us with data about yourself, including your educational background or résumé and other information, including your ethnicity where required or permitted by law. We may share this information with our parent corporations and their affiliates for the purpose of employment consideration. We may keep the information for future consideration unless you direct us not to do so.

### **Revisions to this Privacy Policy**

We may update this Privacy Policy at any time in our sole discretion by posting a revised version on this page or on our Services, or with any notice to you if required under applicable law. You can see when the Privacy Policy has changed from the date of the latest revision below. Your continued use of our Services after any such modification constitutes acceptance to any such modified Privacy Policy. Please review this Privacy Policy frequently for updates.

### **Feedback**

You may contact us with any questions, concerns or inquiries about this Privacy Policy or data about you that we maintain. Please contact us by email at [info@BrightLinknow.com](mailto:info@BrightLinknow.com). All feedback will be evaluated and a reply will be sent as soon as appropriate. In some instances, we may cease providing Services to you if, in our sole discretion, we deem it necessary to satisfy your request or if required under applicable law.

## **FOR EUROPEAN VISITORS AND CUSTOMERS:**

### EU-U.S. and SWISS-U.S. Privacy Shield Additional Notice

We are in the process of submitting our certification of compliance with the EU-U.S. and Swiss-U.S. Privacy Shield with respect to the personal data of users of our Services who are residents of the European Union ("EU"), European Economic Area ("EEA") and Switzerland that we receive and process through the Services. We certify that we adhere to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement (hereinafter, "Privacy Shield Principles") for personal data of users of our Services in participating European countries. Once complete, our Privacy Shield certification will be available here. We may also process personal data submitted relating to individuals in Europe via other compliance mechanisms, including use of the European Union Standard Contractual Clauses.

### **Processing of Personal Data, Purposes and Legal Basis**

In this European privacy policy:

"Personal Data" means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of such natural person.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Sensitive Data" means data indicating racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life, or sexual orientation, or for any genetic data or biometric data.

Please note that, in certain circumstances, you may be required to provide the requested Personal Data by contract or law, and your failure to provide such Personal Data may mean we are unable to provide you with our Services.

Our legal bases for the Processing of Personal Data are: 1) consent and/or 2) any other applicable legal bases, such as our legitimate interest in engaging in commerce, offering products and services of value to users of our Services, preventing fraud, ensuring information and network security, direct marketing, processing Personal Data for internal administrative purposes, and complying with industry practices.

To the extent permitted by applicable law, your entry of any Sensitive Data on our Services is your consent to the Processing of such data as set forth in this European Privacy Policy or as otherwise specified in the context of your submission of such sensitive information.

### **Your Additional Rights as an European Resident**

As a resident of the European Union or a country that follows similar regulations for the protection of Personal Data, you may have the following additional rights:

**Consent:** We may be required to obtain your consent for certain Processing of your Personal Data, such as Processing of Sensitive Data.

**Access:** You may request a copy of the Personal Data we have collected from and about you by contacting us. Please be advised that our personnel may have a limited ability to identify and access an individual user's Personal Data if such information was submitted to us by their school, employer or another organization

with whom they are affiliated. Thus, if you wish to request access, to limit use, or to limit disclosure of your Personal Data, we may first refer your request to the school, employer or other organization that submitted your Personal Data to us, and we will support them as appropriate in responding to your request.

**Rectification & Erasure:** You may request that we rectify or delete any of your Personal Data that is incomplete, incorrect, unnecessary or outdated.

**Objection:** You may object, at any time, to your Personal Data being Processed for direct marketing purposes.

**Restriction of Processing:** You may request restriction of Processing of your Personal Data for certain reasons, such as, for example, if you consider your Personal Data collected by us to be inaccurate or you have objected to the Processing and the existence of legitimate grounds for Processing is still under consideration.

**Data Portability:** You may request and receive the Personal Data we have collected on you in a commonly used and machine-readable form.

**Right to Withdraw Consent:** Where your Personal Data is Processed solely based on your consent and not for any other legitimate interest, you have the right to withdraw your consent at any time, without affecting the lawfulness of our Processing based on such consent before it was withdrawn, including Processing related to existing contracts for our products and services.

Swiss users whose Personal Data is within the scope of the Privacy Shield certification may also have rights to access certain Personal Data we hold about them and to obtain its correction, amendment or deletion.

To exercise any of the rights listed above, please contact us as set forth below. We will process any requests in accordance with applicable law and within a reasonable period of time. We may require that you establish your identity and provide a clear and precise description of your request. Please note that in some cases, especially if

you wish us to delete or cease the Processing of your Personal Data, we may no longer be able to continue to provide our Services to you.

### **Third Parties with Whom We May Share Data**

We may use third-party providers to assist us in providing the Services to our users. Such third-party providers may perform technical operations such as database monitoring, data storage and hosting services and customer support software tools. Such third parties may access, process or store Personal Data in the course of providing these services.

To the extent permitted under applicable law, we may share information about your enrollment and participation in our Services, including your Personal Data, with your employer, governmental agencies, oversight organizations, professional organizations, certification or accreditation organizations, educational institutions, and industry self-regulatory organizations.

We may also share information, including your Personal Data, with third parties for marketing, advertising, promotions, contests, or other similar purposes, with your consent or to the extent permitted under applicable law.

If we receive Personal Data that is subject to our certification under the Privacy Shield and then transfer it to a third-party, we may have certain liability under the Privacy Shield if (i) the third-party Processes the Personal Data in a manner inconsistent with the Privacy Shield and (ii) we are responsible for the event giving rise to the damage, or to the extent we are otherwise liable under applicable law or the Privacy Shield Principles.

### **International Data Transfers**

Our Services may be provided using resources and servers located in various countries around the world, including the United States and other countries. Therefore, your Personal Data may be transferred and Processed outside the country where you use our Services, including to countries outside the EU, EEA or

Switzerland, where the level of data protection may not be deemed adequate by the European Commission.

To the extent permitted by applicable law, your use of our Services is your consent to the transfer of your information outside of your country or geographic region, including transfer to the United States, and to processing of your information in the United States by us or by a third party acting on our behalf.

If you wish to know more about international transfers of your Personal Data, please contact us.

### **Questions or Complaints – Europe**

If you are a resident of a European country participating in the Privacy Shield, you may direct any questions or complaints concerning our Privacy Shield compliance to our Privacy Shield and Data Protection Contact. We will work with you to resolve your issue.

If you consider our Processing of your Personal Data to be inconsistent with the applicable data protection laws, you may lodge a complaint with your local supervisory Data Protection Authority responsible for data protection matters.

### **Dispute Resolution and Arbitration**

If you are a resident of a European country participating in the Privacy Shield and you have not received timely response to your concern, or we have not addressed your concern to your satisfaction, you may seek further assistance, at no cost to you, from JAMS, which is an independent dispute resolution body in the United States. For information about JAMS, please see <https://www.jamsadr.com/eu-us-privacy-shield>.

We also will cooperate with competent EU data protection authorities (DPAs) with regard to human resources data transferred from a European country participating in the Privacy Shield in the context of the employment relationship.

You may also be able to invoke binding arbitration for unresolved complaints but prior to initiating such arbitration, a resident of a European country participating in

the Privacy Shield must first: (1) contact us and afford us the opportunity to resolve the issue; (2) seek assistance from JAMS; and (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue. If such a resident invokes binding arbitration, each party shall be responsible for its own attorney's fees. Pursuant to the Privacy Shield, the arbitrator(s) may only impose individual-specific, non-monetary, equitable relief necessary to remedy any violation of the Privacy Shield Principles with respect to the resident.

### **US Federal Trade Commission Enforcement**

Our Privacy Shield compliance is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). For information about Privacy Shield, please see <https://www.privacyshield.gov/welcome>.

### **Privacy Shield and Data Protection Contact**

Your Privacy Shield and Data Protection Contact for the personal information you provide in connection with our Services is:

ATTN: Legal Department – BrightLink European Privacy Contact

BrightLink Technology, LLC

502 Bombay Lane, Roswell GA 30076

Please provide your identification information, a detailed description of the nature of your request, the name of or Services you use, and your country of residence.

BrightLink Privacy Policy (Rev Nov 30, 2018)