

EU Data Processing Addendum

Addendum Background

This EU Data Processing Addendum (“Addendum”) supplements our online Terms of Service and Privacy Policy (together and individually, the “Agreement”) with clients (“Client” or “you”) insofar as they relate to processing of data subject to the European Union’s General Data Protection Regulation (“GDPR”). To the extent it conflicts with our Terms of Service or our Privacy Policy, this Addendum will control. Capitalized terms used in this Addendum shall have the same meaning set forth for those terms in the GDPR, unless a different meaning is specified herein.

Elevated Resources, Inc. and its affiliates (“ER,” “we,” or “us”) is a software as a service provider. As such, we act as a “Processor” under the GDPR. As one of our clients, you control the means and purposes for the processing of the data you gather using our services (the “Services”), and thus, you are a Controller under the GDPR. Unless otherwise agreed between us in writing, those items the GDPR requires of Processors will be our responsibility, and those items required of Controllers will be your responsibility. Specifically, the parties agree as follows:

ER’s GDPR Obligations

When you use the Services, you may obtain Personal Data about your job applicants, employees, prospects, marketplace partners, customers, vendors, suppliers, or other individuals with whom you interact, or about whom you gather personal data (“Your Personal Data”), using the Services (collectively and individually, “Your Data Subjects”). That Personal Data may be subject to the protections of the GDPR. For purposes of clarity, the parties agree that Your Personal Data does not include data that is anonymized in a manner that eliminates the possibility that the data can be tracked or identified to any specific individual.

Acknowledging that certain of your obligations as a Controller must be passed along to any company or individual that Processes the Personal Data of Your Data Subjects, we agree to perform the following functions and to facilitate your compliance with the GDPR in the following ways:

1.1 Right of Access by Data Subject and Communication with Authorities and Your Data Subjects

We agree that, in order to assist you in your obligations as a Controller, we will implement the necessary technical and organizational measures to allow you to (1) respond to any request by any individual to exercise his or her rights under the GDPR, and (2) respond to correspondence, inquiries, or complaints from entitled third parties such as individuals, regulators, courts, and other authorities in connection with the processing of Personal Data. If any such requests or correspondence is received directly by us, we will forward you the request or correspondence and will wait for further direction from you before taking action. We will not communicate with authorities or Your Data Subjects without receiving your advance permission, except as

required by applicable law. Upon documented request from you, we will correct, supplement, modify or delete any of Your Personal Data, except as required by applicable law.

1.2 Use Limitation

We agree that we will not use or process any of Your Personal Data for any purpose other than the purpose set forth in the Agreement, except to respond to specifically document requests from you regarding Your Personal Data. In no event will we process, use, or transfer any of Your Personal Data for our own purposes or for the purposes of any third party. In addition, we will delete all Your Personal Data from our systems thirty (30) days after termination of the Agreement, except as may be required by applicable law.

1.3 Standard Contractual Clauses, Privacy Shield, and International Transfers of Data

To the extent your transfer of Your Personal Data to us involves a transfer out of the EU, we agree to comply with the Standard Contractual Clauses attached hereto as Exhibit A. We will execute hard copies of the Standard Contractual Clauses at your request, but we consider ourselves bound by this provision to abide by the Standard Contractual Clauses, whether or not we execute them individually on your behalf, as applicable to this Addendum and to the Agreement.

We are currently pursuing certification under the Privacy Shield Framework (“Privacy Shield”) and agree that once we do obtain certification under Privacy Shield, we will continue to abide by Privacy Shield requirements and maintain certification under Privacy Shield for the duration of the time we process Your Personal Data. If we decide that we will no longer abide by Privacy Shield, we will immediately notify you. In any event, we will continue to abide by the provisions of the Standard Contractual Clauses, which shall form an integral part of this Addendum. In the event of any conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses shall control and supersede. If the European Union or courts thereof decide that the Standard Contractual Clauses or Privacy Shield certification are insufficient protection for citizens of the EU, then the parties agree to work in good faith together to determine how a new valid method can be implemented to meet any new requirements.

We agree that we will not process or transfer any of Your Personal Data originating from the European Economic Area in any country or territory that has been determined to offer an inadequate level of data protection unless it has first obtained your consent or ensured that a valid transfer mechanism similar to the Privacy Shield is in place with respect to such country or territory.

1.4 Processing Confidentiality and Agreements by Agents

We agree that we will keep Your Personal Data strictly confidential and that we will ensure that any of our employees, vendors, or other agents “Our Agents” who have access to Your Personal Data (1) are informed of and subject to this strict duty of confidentiality; (2) access and process only such of Your Personal Data as is strictly to perform our obligations under the Agreement; and (3) agree not to permit any person to process Your Personal Data who is not subject to the

foregoing duties. We accept responsibility for the conduct of Our Agents in this regard, including their acts, errors and omissions.

1.5 Disposition of Your Personal Data Upon Request or Termination

At your request or at termination of the Agreement, whichever is sooner, we agree to delete or return to you all Your Personal Data, including any of Your Personal Data subcontracted to a third party for processing, except as required by applicable law. At that time, with respect to Your Personal Data that we are required by applicable law to retain, we will isolate and protect Your Personal Data from further processing, except as required by applicable law. We will ensure that any of our subprocessors who are in possession of Your Personal Data shall also comply with this provision.

1.6 Security Incidents and Security

We will at all times ensure that Your Personal Data is adequately protected in accordance with the requirements of the GDPR. To this end, we agree that we will implement appropriate technical and organizational measures to protect Your Personal Data from security incidents. These measures are described in Exhibit B to this Addendum.

When we become aware of any security incident, which consists of the unpermitted, accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any of Your Personal Data, we will inform you without any undue delay, and in no event longer than 24 hours after we discover the security incident. We will cooperate reasonably with you and provide you the information you need in order to fulfill your data breach obligations under the GDPR. We will also take other further measures and actions that are necessary to remedy or mitigate the effects of the security incident, and we will keep you informed of every material development connected with the security incident. Except as required by law, we will not take action to notify Your Data Subjects of any security incident.

1.7 Subprocessors

In the course of providing our Services, we may be required to contract with a third-party processor (“Subprocessor”) to perform a portion of the Services. We have included as Exhibit C a list of the Subprocessors we currently use. We will not add any additional Subprocessors without informing you of such Subprocessors and giving you an opportunity to object to the use of such Subprocessors. We agree to impose the same data protection obligations upon each of our Subprocessors that we agree to in this Addendum, and we agree to be fully responsible for any liability arising out of the acts and omissions of our Subprocessors.

For the avoidance of doubt, the approval requirements as set out in this subsection will not apply in cases where we subcontract ancillary services to third parties without having access to Your Personal Data. Such ancillary services are not considered data processing.

1.8 Audits, Requests from Law Enforcement, and Impact Assessment

In certain instances, you as a Controller are required to submit to an audit to show that you are complying with the provisions of the GDPR. In any such instance, we agree to cooperate fully with such audit and to maintain a record of all processing activities that we carry out on your behalf. After reasonable notice, we will allow you or your auditors to audit our compliance with

this Addendum, to include communication with our staff and access to our systems and information; provided you conduct your audit during normal business hours and make reasonable efforts to minimize the disruption to our business.

If we are requested by law enforcement to disclose any of Your Personal Data, we will, unless prohibited by law, inform you of the request, attempt to re-direct the law enforcement agency to contact you directly, and only provide such information as required by law.

In the event that you believe that our processing of Your Personal Data is likely to result in a high risk to the data protection rights and freedoms of citizens of the EU, we agree to assist you in a reasonable and timely manner to conduct a data protection impact assessment, which may include consulting with the relevant data protection authority.

Your Obligations

As a Controller under the GDPR, you are required to carry out certain responsibilities and to comply with certain requirements. For example, and without intending to limit your obligations, you are required to comply with the privacy and confidentiality provisions of the GDPR, just as we are. You are also required to ensure that the consent of Data Subjects is obtained and that collection of Your Personal Data is otherwise justified under the GDPR. We acknowledge that in doing so, you are required to ensure that your Processors also comply with certain requirements, and we agree to reasonably cooperate with your requests in this regard. However, if you make requests of us that go beyond our obligations set forth in the “ER’s GDPR Obligations” section of this Addendum, we will comply with your requests at your expense.