Leadership Alliance, Inc.
Privacy Shield Policy

Leadership Alliance, Inc. (the “Company”) complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce (“Privacy Shield Principles”) regarding the collection, use, and retention of personal information from European Union (“EU”) member countries, the United Kingdom, and Switzerland (collectively, “Privacy Shield Countries”) transferred to the United States pursuant to Privacy Shield. The Company has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this Privacy Shield Policy (“Policy”) and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Company is subject to the regulatory and enforcement powers of the U.S. Federal Trade Commission.

The Company’s Collection And Use Of Personal Data

For purposes of this Policy, “Personal Data” means any information received by the Company from Privacy Shield Countries, recorded in any form, which relates to a natural person who is identified in, or identifiable based on, the information received.

The Company receives Personal Data about individuals in Privacy Shield Countries, including current, former, and prospective employees of the Company’s clients located in Privacy Shield Countries (“Client Employees”). The Company collects Personal Data about Client Employees from the Company’s clients and from the Client Employees, for example, when they take tests. This Personal Data includes Client Employees’ names, testing results, and native language. The Company uses this information to assist the Company’s clients with their employment-related decisions such as hiring, promoting, and developing individuals.

The Company’s Disclosure Of Personal Data

The Company may disclose the Personal Data of individuals located in Privacy Shield Countries, subject to written agreement, to authorized service providers which provide services related to the purposes for which the Company collects that Personal Data. For example, the Company contracts with third-party service providers that assist in the collection and assessment of the Personal Data. Additionally, the Company will disclose the Personal Data about Client Employees, subject to written agreement, to the Company’s client for whom the Personal Data was collected. The Company may be liable for the onward transfer of Personal Data to third parties.
The Company may be required to disclose, and may disclose, Personal Data in response to lawful requests by public authorities, including for the purpose of meeting national security or law enforcement requirements.

The Company’s accountability for personal data that it receives in the United States under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, the Company remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless the Company proves that it is not responsible for the event giving rise to the damage.

**Choices For Limiting The Use And Disclosure Of Personal Data**

The Company or the Company’s client for whom Company processes the Personal Data will provide the opportunity for individuals to opt out from: (a) the disclosure of their Personal Data to a non-agent third party; and (b) the use of their Personal Data for purpose(s) that are materially different from the purpose(s) for which the Personal Data was originally collected or subsequently authorized by the individual. In addition, the Company or the Company’s client will provide individuals with clear, conspicuous and readily available mechanisms to exercise their choices regarding Personal Data should such circumstances arise. Individuals who wish to limit the use or disclosure of their Personal Data as described in this Policy should submit their requests to testing@leadershipall.com.

The Company does not review notices provided by clients to individuals in Privacy Shield Countries, or authorizations to the client from individuals in Privacy Shield Countries, regarding Company’s processing of Personal Data to determine whether the notices or authorizations are in compliance with, or conflict with, applicable law or any policy or notice published by the client. The Company’s clients are responsible for providing instructions and authorizations that comply with their policies, notices, and applicable laws.

**Individuals’ Right To Access Their Personal Data**

Upon request and except where the rights of persons other than the individual would be violated, the Company will grant individuals access to their Personal Data and permit individuals to correct, amend, or delete Personal Data that is inaccurate or incomplete or that is being processed in violation of the Privacy Shield Principles. Individuals who wish to exercise these rights can do so by contacting testing@leadershipall.com. For security purposes, the Company may require verification of the requester’s identity before providing access to Personal Data.

**More Information And What To Do If You Have a Complaint**

Individuals can contact the Company with any inquiries about the Privacy Shield or the processing of their Personal Data at testing@leadershipall.com.
In compliance with the Privacy Shield Principles, the Company commits to resolve complaints about your privacy and our collection or use of your Personal Data transferred to the United States pursuant to Privacy Shield. Individuals in Privacy Shield Countries with Privacy Shield inquiries or complaints should first contact the Company by email at testing@leadershipall.com. The Company will promptly investigate, and attempt to resolve, such complaints in accordance with this Policy and the Privacy Shield Principles.

The Company has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your complaint involves human resources data transferred to the United States from Privacy Shield Countries in the context of the employment relationship, and the Company does not address it satisfactorily, the Company commits to cooperate with the panel established by the EU data protection authorities (DPA Panel) and/or the Swiss Federal Data Protection and Information Commissioner, as applicable and to comply with the advice given by the DPA panel and/or Commissioner, as applicable with regard to such human resources data. To pursue an unresolved human resources complaint, you should contact the state or national data protection or labor authority in the appropriate jurisdiction. Complaints related to human resources data should not be addressed to the BBB EU PRIVACY SHIELD.

Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction

Effective Date: January 31, 2020