

The Ken Blanchard Companies EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework

Effective Date: May 25, 2018

Introduction

The Ken Blanchard Companies (the “Company”) is a global leader in workplace learning, productivity, performance, and leadership training solutions. We help companies improve their performance, productivity, and bottom-line results. Protecting the privacy of our clients is important to the Company. The Company adheres to the EU-U.S. Privacy Shield Framework and Swiss-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 European Union (“EU”) and Switzerland to the United States of America. Accordingly, the Company has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles (“Principles”) with respect to all such data. This document outlines the Company’s general policy and practices for implementing the Principles, including the types of information gathered, how it is used, and the notice and choice affected individuals have regarding the use of and their ability to correct that information.

The detailed Company Privacy Policy is published at <http://www.kenblanchard.com/Privacy-Policy>. If there is any conflict between the policies contained within the published privacy policy and the Principles, the Principles shall govern. This privacy policy applies to all personal information received by the Company whether in electronic, paper, or verbal format. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>

Definitions

- “Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.
- “Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
- “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- “Sensitive information” is personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.

Principles

Notice

To the extent permitted by the Privacy Shield Framework Agreement, Company reserves the right to process personal information in the course of providing professional services to the Company’s clients. Where the Company collects and processes, at the direction of clients, personal information directly from individuals in the E.U., Company shall inform the individual of the purposes for which data is collected and

used, how to contact Company with inquiries or complaints, their right to access their data, and the independent dispute resolution mechanism available to the individual. Company does not collect any sensitive information about an individual.

Choice

It is the Company's responsibility to inform those individuals about the choices and means, if any, offered the individuals for limiting the use or disclosure of their information.

Company will not disclose an individual's personal information to third parties unless directed by the client or when one or more of the following conditions are true:

- Company has the individual's permission to make the disclosure;
- The disclosure is required by law or professional standards;
- The disclosure is reasonably related to the sale or disposition of all or part of the Company business;
- The information in question is publicly available;
- The disclosure is reasonably necessary for the establishment or defense of legal claims; or
- The disclosure is to another Company entity or to persons or entities providing services on the Company's or client's behalf (each a "transferee"), consistent with the purpose for which the information was obtained, if the transferee, with respect to the information in question:
 - is subject to law providing an adequate level of privacy protection;
 - has agreed in writing to provide an adequate level of privacy protection; or
 - subscribes to the Principles.

Accountability for Onward Transfer

Permitted transfers of information, either to third parties or within the Company, include the transfer of data from one jurisdiction to another, including transfers to and from the United States of America. Company may transfer data to a third party acting as a controller, which provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual or the organization pursuant to the principle of Choice and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate. Because privacy laws vary from one jurisdiction to another, personal information may be transferred to a jurisdiction where the laws provide less or different protection than the jurisdiction in which the information originated.

The Company has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Company shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

Data Security

Company shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing

and the nature of the personal data. Company has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction. Company cannot guarantee the security of Information on or transmitted via the Internet.

Data Integrity and Purpose Limitation

Company shall only process Personal Information in a way that is compatible with and relevant for the purpose for which it was collected or authorized by clients. To the extent necessary for those purposes, Company shall take reasonable steps to ensure that Personal Information is accurate, complete, current, and reliable for its intended use.

Company retains information in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of the preceding paragraph at the express direction of the client. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Company takes reasonable and appropriate measures in complying with this provision.

Access and Correction

Company processes data under the guidance and direction of the clients. If an individual becomes aware that information the Company maintains about that individual is inaccurate, or if an individual would like to update or review his or her information, the individual must contact the Company and request amendments.

Recourse, Enforcement and Liability

Company uses a self-assessment approach to assure compliance with this privacy policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible and in conformity with the Principles. We encourage interested persons to raise any concerns using the contact information provided and we will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of Personal Information in accordance with the Principles.

In compliance with the Privacy Shield Principles, The Ken Blanchard Companies commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact The Ken Blanchard Companies using the name provided under the heading **Contact Information** provided below.

The Ken Blanchard Companies has further committed to cooperate with EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources and non-human resources data transferred from the EU and Switzerland in the context of the employment relationship.

Company is subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body with jurisdiction to investigate claims against

our organization regarding possible unfair or deceptive practices and violations of laws or regulations covering privacy.

An individual may, under certain conditions, invoke binding arbitration. See Section C of Annex I to the Privacy Shield Principles for more information. That information may be found on the web at <https://www.privacyshield.gov/article?id=ANNEX-I-introduction>

Amendments

The privacy policy published on the company website may be amended from time to time consistent with the requirements of the Privacy Shield Framework. We will post any revised policy on our website accessible at <http://www.kenblanchard.com/Privacy-Policy>

Contact Information

Questions, comments or complaints regarding the Company's Privacy Shield Framework or data collection and processing practices may be emailed to:

Terry Orletsky
Vice President of Information Technology
The Ken Blanchard Companies
125 State Place
Escondido, CA 92029

terry.orletsky@kenblanchard.com
1-800-728-6000