Privacy Shield Policy

Version 1.2

April 1st, 2018

DOCUMENT REVISION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
04/03/2018	1.0	Creation of Document	David O'Connell
05/02/2018	1.1	Review & Updates	David O'Connell
08/02/2018	1.2	Review & Updates	David O'Connell

DOCUMENT DISTRIBUTION AND REVIEW TABLE

NAME	VERSION	DATE
Michael Concannon	1.0	04/03/2018
Michael Concannon	1.1	05/02/2018
Michael Concannon	1.2	08/02/2018

CONTENTS

INTRODUCTION

D3 Data, LLC. respects individuals' privacy, and strives to collect, use and disclose personal information in a manner consistent with the laws of the countries in which it and its subsidiaries do business. This Privacy Shield Privacy Policy (the "Policy") describes the privacy principles as follows with respect to certain personal information transmitted to D3 Data in the United States of America (the "U.S.") from countries located within the European Economic Area and Switzerland.

1. PRIVACY SHIELD OVERVIEW

The U.S. Department of Commerce and the European Commission as well as the Swiss Federal Council have agreed on a set of data protection principles and associated supplemental principles to enable U.S. companies to satisfy European Union ("EU") and Swiss law requiring that Personal Data transferred from the EU and/ or Switzerland to the U.S. be adequately protected (the "EU-U.S. Privacy Shield" and the "Swiss-U.S. Privacy Shield" respectively, together the "Privacy Shield"). The European Economic Area (the "EEA"), which as of the date of this Policy includes all member states of the EU and Iceland, Liechtenstein and Norway, and Switzerland have recognized the Privacy Shield as providing adequate protection of Personal Data.

Consistent with its commitment to protect personal privacy, D3 Data has made a decision to voluntarily adhere to the principles set forth in the Privacy Shield (the "Privacy Shield Principles"). As such, D3 Data has certified its compliance with the Privacy Shield Principles with the U.S. Department of Commerce.

For more information about the Privacy Shield Principles or to access D3 Data' certification statement, please go to https://privacyshield.gov.

Should there be any conflict between the Privacy Shield Principles and this Policy, this Policy shall be interpreted to be consistent with the Privacy Shield Principles.

2. SCOPE

This Policy applies to all Personal Data received by D3 Data in the United States from the EEA and/ or from Switzerland, either directly from individuals, from its affiliates or from other third-party organizations, and in any format whatsoever, including electronic, paper or oral transmission.

This Policy also applies to D3 Data' Agents (defined below) that process Personal Data received by D3 Data in the United States from the EEA and/ or from Switzerland on behalf of D3 Data.

3. DEFINITIONS

For purpose of this Policy, the following definitions shall apply:

- **"Personal Data"** and **"Personal Information"** means data about an identified or identifiable individual that are within the scope of the Directive 95/46/EC or the Swiss Federal Act on Data Protection, received by an organization in the United States from the European Union and/ or Switzerland, and recorded in any form. Personal Data includes all Sensitive Personal Data (as defined below).
- **"Sensitive Personal Data"** or **"Sensitive Personal Information"** means 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 or, where received from a third party, data that is identified and treated as sensitive by the third party. Where Swiss individuals are concerned, "Sensitive Personal Data" or "Sensitive Personal Information" also includes ideological views or activities, and information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.
- **"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.

- **"Agent"** means any third party that collects or uses Personal Data provided by D3 Data to perform tasks on behalf of D3 Data under the instructions of, and solely for, D3 Data.
- **"D3 Data," "we," "our**" or **"us"** means D3 Data, LLC. and its successors, assigns and wholly-owned affiliates and subsidiaries and their respective divisions and groups, each of which are located within the U.S.

4. PRIVACY PRINCIPLES FOR PROCESSING OF PERSONAL DATA RECEIVED FROM THE EEA AND/ OR SWITZERLAND

The privacy principles set forth in this Policy have been developed based on the Privacy Shield Principles.

4.1 NOTICE

Where D3 Data collects Personal Data directly from individuals in the EEA and/ or Switzerland or receives it from its European or Swiss affiliates, it or its European or Swiss affiliates will inform those individuals about the purposes for which they collect and use Personal Data about them; the transfer of Personal Data to D3 Data in the U.S., the types or identity of third parties to which D3 Data discloses that information and the purposes for which it does so; and the choices and means D3 Data offers individuals for limiting the use and disclosure of their Personal Data. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Data to D3 Data, or as soon as practicable thereafter, and in any event before D3 Data uses the information for a purpose other than that for which it was originally collected.

D3 Data may from time to time process certain Personal Data about customers, business partners, suppliers, vendors and service providers, including information recorded and stored on various types of media, including electronic media.

D3 Data will process these types of data in conformity with the Privacy Shield Principles and will continue to apply the Principles to personal data received under the application of the Privacy Shield as long as it holds this data.

Purposes for which we may collect and use Personal Data from our customers, consumers and other non- employees include:

- Communicating to individuals about our products, services and related issues.
- Notifying individuals of, and administering, contests, sweepstakes, promotions and other offers.
- Evaluating the quality of our products and services.
- Allowing individuals to register for our websites, online communities and other social networking services, and administering and processing these registrations.
- Transferring Personal Data in connection with D3 Data' legal, regulatory compliance and auditing purposes.
- Facilitating D3 Data' internal administrative purposes and application functionality, maintaining, administering and complying with D3 Data' legal, regulatory compliance and auditing obligations, policies and procedures.
- Execution of contracts and delivery of products and services to customers; execution and management of development etc.

We may share Personal Data within the U.S. family of D3 Data companies. D3 Data may also share Personal Data with its third-party Agents for the sole purpose of, and only to the extent needed to, support D3 Data' or our customers' business needs. We may also disclose Personal Data to our Agents in the U.S. and other third parties when required to do so under law or by legal process. Third Party Agents are required to keep confidential Personal Data received from D3 Data and may not use it for any purpose other than originally intended.

4.2 CHOICE

D3 Data will offer individuals in the EEA or Switzerland the opportunity to choose (by either opt-out or opt- in) if their Personal Data is (a) to be disclosed to a third party that is not an Agent, or (b) to be used for a purpose materially different from the purpose for which it was originally collected or subsequently authorized by the individual.

For Sensitive Personal Data, D3 Data will give individuals the opportunity to affirmatively and explicitly consent (opt-in) to permit D3 Data to (a) disclose their Sensitive Personal Data to a third party that is not an Agent or (b) use Sensitive Personal Data for a purpose materially different from the purpose for which it was originally collected or subsequently authorized by the individual.

D3 Data will provide individuals with reasonable, clear and conspicuous and readily available mechanisms to exercise these choices.

4.3 ACCOUNTABILTY FOR ONWARD TRANSFER

D3 Data will transfer Personal Data to Agents only for limited and specific purposes. D3 Data will obtain contractual assurances from its Agents that they will safeguard Personal Data in a manner consistent with this Policy and that they will provide at least the same level of protection as is required by the relevant Privacy Shield Principles. D3 Data recognizes its responsibility and potential liability for onward transfers to Agents. Where D3 Data has knowledge that an Agent is using or disclosing Personal Data in a manner contrary to this Policy and/or the level of protection as required by the Privacy Shield Principles, D3 Data will take reasonable steps to prevent, remediate or stop such use or disclosure.

If D3 Data transfers Personal Information to non-agent third parties acting as a Controller, D3 Data will apply the Notice and Choice principles and will obtain contractual assurance from these parties that they will provide the same level of protection as is required under the principles, unless a derogation for specific situations under European data protection law applies.

4.4 ACCESS

Upon request and in accordance with the Privacy Shield Principles, D3 Data will grant individuals reasonable access to their Personal Data that is held by D3 Data. In addition, D3 Data will take reasonable steps to permit individuals to correct, amend, or delete their Personal Data that is demonstrated to be inaccurate, incomplete or processed in violation of the Privacy Shield Principles. In accordance with the Privacy Shield Principles, D3 Data may limit or deny access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, where the legitimate rights of persons other than the individual would be violated or if necessary to safeguard important countervailing public interests (e.g., national security) or in other limited circumstances (e.g., disclosure would breach a legal or other professional privilege).

4.5 SECURITY

D3 Data will take reasonable precautions to protect Personal Data in its possession 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.

4.6 DATA INTEGRITY AND PURPOSE LIMITATION

D3 Data will use Personal Data only in ways that are compatible with the purposes for which it was originally collected or as subsequently authorized by the individual. D3 Data will also take reasonable steps to ensure that Personal Data is relevant to its intended use, accurate, complete, and current. D3 Data will adhere to the Privacy Shield Principles for as long it retains Personal Information received under its Privacy Shield certification.

4.7 RECOURSE, ENFORCEMENT AND LIABILITY

D3 Data utilizes the self-assessment approach to verify its compliance with this Policy. D3 Data periodically verifies that this Policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented, and in conformity with the Privacy Shield Principles. D3 Data will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the Privacy Shield Principles. D3 Data will also investigate suspected infractions of this Policy.

D3 Data Privacy and Information Security programs include adequate training for employees and personnel on their responsibilities with reference to the implementation of the Privacy Shield Principles.

If D3 Data determines that any employee of D3 Data is in violation of this Policy, such person will be subject to disciplinary action up to and possibly including termination of employment.

D3 Data encourages interested persons with questions or concerns relating to this Policy to contact us using the contact information below. Any questions or concerns regarding the use or disclosure of Personal Data should be directed to the Chief Information Officer at the address set forth below.

With respect to any complaints relating to this Policy that cannot be resolved through D3 Data' internal processes, D3 Data has agreed to refer unresolved privacy complaints under US-EU Privacy Shield and Swiss-US Privacy Shield to an independent dispute resolution mechanism operated by the DMA (Data & Marketing Association). D3 Data is also subject to the investigatory and enforcement powers of the Federal Trade Commission, which is the competent supervisory authority under the Privacy Shield.

If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed by D3 Data , EU and Swiss individuals may bring a complaint before the DMA EU and Swiss Privacy Shield program can be found at: https://thedma.org/resources/consumer-resources/privacyshield-consumers/dma-eu-privacyshield-complaint-form/.

Where a complaint cannot be resolved by any of the before mentioned recourse mechanisms, individuals have a right to invoke binding arbitration under the Privacy Shield Panel as a recourse mechanism of 'last resort'.

In the event that D3 Data or such authorities determines that D3 Data failed to comply with this Policy, D3 Data will take appropriate steps to address any adverse effects arising directly from such failure and to promote future compliance.

5. LIMITATIONS

D3 Data ' adherence to the Privacy Shield Principles may be limited (a) to the extent necessary to meet applicable national security, public interest, or law enforcement requirements, e.g. in the course of lawful requests by public authorities (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

6. CONTACT INFORMATION

Questions or comments regarding this Policy or our practices concerning Personal Data should be submitted to D3 Data by mail or e-mail as follows:

Chief Information Officer,

D3 Data, LLC.

530 Jackson Street, Fourth Floor,

San Francisco, CA 94133, United States of America

e-mail: privacyshield@d3data.com

If you are a citizen of an EEA member state, you may also address any unresolved complaints to the panel of the EU Data Protection Authorities at the following address:

- http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

If you are a citizen of Switzerland, you may address any unresolved complaints to the Swiss Federal Data Protection and Information Commissioner at the following address:

- https://www.edoeb.admin.ch/org/00126/index.html?lang=en

7. CHANGES TO THIS POLICY

This Policy may be amended from time to time, consistent with the requirements of the Privacy Shield Principles. Appropriate public notice will be given concerning such amendments.