DDB

EU/Swiss-U.S. Privacy Shield: Consumer Privacy Policy

Last Updated: March 20, 2019

DDB Worldwide Communications Group Inc. and its affiliates TLP, Inc. (d/b/a Tracy Locke), Interbrand Corporation and Adam&Eve Inc. (collectively, "DDB") respect your concerns about privacy. DDB participates in the EU-U.S. and Swiss-U.S. Privacy Shield frameworks (collectively, the "Privacy Shield") issued by the U.S. Department of Commerce. DDB commits to comply with the Privacy Shield Principles with respect to Consumer Personal Data the company receives from the EU, UK and Switzerland in reliance on the Privacy Shield. This Policy describes how DDB implements the Privacy Shield Principles for Consumer Personal Data.

For purposes of this Policy:

"Client" means any entity that obtains marketing, corporate communications or other services from DDB.

"Consumer" means any natural person who is located in the EU, UK or Switzerland, but excludes any individual acting in his or her capacity as an Employee.

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Employee" means any current, former or prospective employee, intern, temporary worker or contractor of DDB or any of its EU, UK or Swiss subsidiaries or affiliates, or any related individual whose Personal Data DDB processes in connection with an employment relationship, who is located in the EU, UK or Switzerland.

"EU" means the European Union and Iceland, Liechtenstein and Norway.

"Personal Data" means any information, including Sensitive Data, that is (i) about an identified or identifiable individual, (ii) received by DDB in the U.S. from the EU, UK or Switzerland, and (iii) recorded in any form.

"Privacy Shield Principles" means the Principles and Supplemental Principles of the Privacy Shield of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.

"Processor" means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller.

"Sensitive Data" means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (including

trade union-related views or activities), sex life (including personal sexuality), information on social security measures, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposition of such proceedings, or the sentence of any court in such proceedings (including administrative proceedings and criminal sanctions).

"UK" means the United Kingdom.

"Vendor" means any contractor, supplier, vendor or other third party located in the EU, UK or Switzerland that provides services or products to DDB.

DDB's Privacy Shield certification, along with additional information about the Privacy Shield, can be found at https://www.privacyshield.gov/.

Types of Personal Data DDB Collects

DDB serves as both a Controller and a Processor with respect to the Consumer Personal Data it obtains and maintains.

Controller Activities

As a Controller, DDB obtains Personal Data about Consumers in various ways. For example, DDB collects Personal Data directly from Consumers when they visit DDB's websites.

The types of Personal Data may DDB collect directly from Consumers include:

- Contact information, such as name, postal address, email address and telephone number;
- Personal Data contained in content Consumers submit through DDB's websites; and
- Other data collected automatically through DDB's websites (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on DDB's websites, and dates and times of website visits).

DDB may use the Personal Data described above for various purposes, including to:

- Provide its services;
- market its services;
- respond to Consumers' inquiries;
- operate, evaluate and improve its business (including developing new services; enhancing and improving its services; analyzing its services; managing its

communications; performing data analytics; and performing accounting, auditing and other internal functions);
- protect against, identify and prevent fraud and other unlawful activity, claims and other liabilities; and
- comply with and enforce applicable legal requirements, relevant industry standards, contractual obligations and DDB's policies.

In addition, DDB may obtain Personal Data, such as contact information, of its Clients' and Vendors' representatives, who are located in the EU, UK or Switzerland. DDB uses this information to manage its relationships with its Clients and Vendors, and carry out DDB's obligations under its contracts with its Clients and Vendors.

DDB also may obtain and use Consumer Personal Data in other ways for which DDB provides specific notice at the time of collection.

Processor Activities

As a Processor, DDB receives Personal Data about its Clients' Consumers located in the EU, UK and Switzerland, when Clients provide such Personal Data to DDB. For example, in connection with providing marketing, corporate communications or other services to its Clients, DDB may process Personal Data about a Client's Consumers located in the EU, UK and Switzerland.

DDB's privacy practices regarding the processing of Consumer Personal Data comply with the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

Notice

DDB provides information in this Policy about its Consumer Personal Data practices, including the types of Personal Data DDB collects, the types of third parties to which DDB discloses the Personal Data and the purposes for doing so, the rights and choices Consumers have for limiting the use and disclosure of their Personal Data, and how to contact DDB about its practices concerning Personal Data.

When DDB acts as a Processor and Consumer Personal Data is transferred to DDB in the U.S. on behalf of a Client, the Client is responsible for providing appropriate notice to its Consumers and obtaining the requisite consent.

Relevant information also may be found in notices pertaining to specific data processing activities.

Choice

When DDB collects Personal Data directly from Consumers, the company generally offers those Consumers the opportunity to choose whether their Personal Data may be (i) disclosed to third-party Controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Consumer. To the extent required by the Privacy Shield Principles, DDB obtains opt-in consent for certain uses and disclosures of Sensitive Data. Consumers may contact DDB as indicated below regarding the company's use or disclosure of their Personal Data. Unless DDB offers Consumers an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

When DDB maintains Personal Data about Consumers with whom DDB does not have a direct relationship because DDB obtained or maintains the Consumers' data as a Processor, DDB's Clients are responsible for providing the relevant Consumers with certain choices with respect to the Clients' use or disclosure of the Consumers' Personal Data.

DDB shares Consumer Personal Data with its affiliates and subsidiaries. DDB may disclose Consumer Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. DDB also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

Accountability for Onward Transfer of Personal Data

This Policy describes DDB's sharing of Consumer Personal Data.

To the extent DDB acts as a Controller, except as permitted or required by applicable law, DDB provides Consumers with an opportunity to opt out of sharing their Personal Data with third-party Controllers. DDB requires third-party Controllers to whom it discloses such Consumer Personal Data to contractually agree to (i) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant Consumer, (ii) provide the same level of protection for Personal Data as is required by the Privacy Shield Principles, and (iii) notify DDB and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party Controller determines that it cannot meet its obligation to provide the same level of protection for Personal Data as is required by the Privacy Shield Principles.

With respect to transfers of Consumer Personal Data to third-party Processors, DDB (i) enters into a contract with each relevant Processor, (ii) transfers Personal Data to each such Processor only for limited and specified purposes, (iii) ascertains that the Processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Privacy

Shield Principles, (iv) takes reasonable and appropriate steps to ensure that the Processor effectively processes the Personal Data in a manner consistent with DDB's obligations under the Privacy Shield Principles, (v) requires the Processor to notify DDB if the Processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles, (vi) upon notice, including under (v) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (vii) provides a summary or representative copy of the relevant privacy provisions of the Processor contract to the Department of Commerce, upon request. DDB remains liable under the Privacy Shield Principles if the company's third-party Processor onward transfer recipients process relevant Personal Data in a manner inconsistent with the Privacy Shield Principles, unless DDB proves that it is not responsible for the event giving rise to the damage.

Security

DDB takes reasonable and appropriate measures to protect Consumer Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the Personal Data.

Data Integrity and Purpose Limitation

DDB limits the Consumer Personal Data it processes to that which is relevant for the purposes of the particular processing. DDB does not process Consumer Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Consumer. In addition, to the extent necessary for these purposes and consistent with its role as a Controller or Processor, DDB takes reasonable steps to ensure that the Personal Data the company processes is (i) reliable for its intended use, and (ii) accurate, complete and current. In this regard, DDB relies on its Consumers and Clients (with respect to Personal Data of Consumers with whom DDB does not have a direct relationship) to update and correct the relevant Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized. Consumers (and Clients, as appropriate) may contact DDB as indicated below to request that DDB update or correct relevant Personal Data.

Subject to applicable law, DDB retains Consumer Personal Data in a form that identifies or renders identifiable the relevant Consumer only for as long as it serves a purpose that is compatible with the purposes for which the Personal Data was collected or subsequently authorized by the Consumer.

Access

Consumers generally have the right to access their Personal Data. Accordingly, to the extent DDB acts as a Controller, where appropriate, DDB provides Consumers with reasonable access to the Personal Data DDB maintains about them. DDB also provides a reasonable opportunity for those Consumers to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Privacy Shield Principles, as appropriate. DDB may limit or deny access to Personal Data where the burden or expense of providing access would be

disproportionate to the risks to the Consumer's privacy in the case in question, or where the rights of persons other than the Consumer would be violated. Consumers may request access to their Personal Data by contacting DDB as indicated below.

When DDB maintains Personal Data about Consumers with whom DDB does not have a direct relationship because DDB maintains the Consumers' data as a Processor for its Clients, DDB's Clients are responsible for providing Consumers with access to the Personal Data and the right to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Privacy Shield Principles, as appropriate. In such circumstances, Consumers should direct their questions to the appropriate DDB Client. When a Consumer is unable to contact the appropriate Client, or does not obtain a response from the Client, DDB will provide reasonable assistance in forwarding the Consumer's request to the Client.

Recourse, Enforcement and Liability

DDB has mechanisms in place designed to help assure compliance with the Privacy Shield Principles. DDB conducts an annual self-assessment of its Consumer Personal Data practices to verify that the attestations and assertions DDB makes about its Privacy Shield privacy practices are true and that DDB's privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

Consumers may file a complaint concerning DDB's processing of their Personal Data. DDB will take steps to remedy issues arising out of its alleged failure to comply with the Privacy Shield Principles. Consumers may contact DDB as specified below about complaints regarding DDB's Consumer Personal Data practices.

If a Consumer's complaint cannot be resolved through DDB's internal processes, DDB will cooperate with JAMS pursuant to the JAMS Privacy Shield Program, which is described on the JAMS website at https://www.jamsadr.com/eu-us-privacy-shield. JAMS mediation may be commenced as provided for in the JAMS rules. Following the dispute resolution process, the mediator or the Consumer may refer the matter to the U.S. Federal Trade Commission, which has Privacy Shield investigatory and enforcement powers over DDB. Under certain circumstances, Consumers also may be able to invoke binding arbitration to address complaints about DDB's compliance with the Privacy Shield Principles.

When DDB maintains Personal Data about Consumers with whom DDB does not have a direct relationship because DDB maintains the Consumers' data as a Processor for its Clients, Consumers may submit complaints concerning the processing of their Personal Data to the relevant Client, in accordance with the Client's dispute resolution process. DDB will participate in this process at the request of the Client or the Consumer.

How to Contact DDB

To contact DDB with questions or concerns about this Policy or DDB's Consumer Personal Data practices:

Write to:

DDB Worldwide Communications Group Inc.
Attention: General Counsel
437 Madison Avenue
New York, New York 10022

or

DDB Worldwide Communications Group Inc.
Attention: General Counsel
12 Bishops Bridge Road
W2 6AA London

E-mail: privacyshield@DDB.com