PRIVACY POLICY 2018

DEMAND FRONTIER

1. General Privacy Statement:

Demand Frontier, LLC has adopted consistent, globally valid data protection and data security standards for processing the sensitive data of its clients, partners, prospects, and employees in line with globally accepted principles. Demand Frontier holds responsibilities for protecting the privacy of sensitive data, including any personal information being maintained, against threats posed by unauthorized access or misuse. In addition, Demand Frontier respects individual privacy and shall handle all sensitive information with care.

This statement undergirds Demand Frontier's ability to adapt to a changing global marketplace and forms the basis for long-lasting business relationships built on trust. This statement also sets important basic conditions for the global exchange of data, as it guarantees a reasonable level of data protection for trans-border data flows.

This statement applies to Demand Frontier and covers the following: processing of sensitive data relating to clients, partners, Demand Frontier employees, and prospects.

2. Appropriate Use:

Customer may not use nor allow its Users to use Demand Frontier products or features in connection with any (a) infringement or misappropriation of any copyright, trademark, patent, trade secret or other intellectual property rights; (b) defamation, libel, slander, obscenity or violation of the rights of privacy or publicity; (c) promotion of violence, hatred, or racial or religious intolerance; or (d) any other offensive, harassing or illegal conduct. Demand Frontier will cooperate with law enforcement and other authorities in investigating claims of illegal activity or suspected illegal activity, including, but not limited to, illegal transfer or publication of copyrighted material. If Customer violates any portion of this Acceptable Use Policy, Customer accepts sole responsibility for all remedial actions and costs related to such violation(s), including but not limited to, compliance efforts and costs associated with statutory obligations or government investigations.

3A. Personal Information.

Demand Frontier will not use personal information to collect or store account numbers from credit cards, debit cards, bank accounts or other financial systems; collect or store U.S. Social Security Numbers, drivers' license or other personal identification numbers issued by any government or financial institution; or collect, store or otherwise handle personal information in a manner not disclosed by Customer to the user, or in violation of any applicable state or federal laws; or collect, store or transmit Personal Health Information ("PHI") as defined by HIPAA if Customer is a Covered Entity as defined by HIPAA if Customer is a Covered Entity as defined by HIPAA.

3B. How We Use Personal Information

As a policy, Demand Frontier only uses sensitive information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. Demand Frontier takes reasonable steps to ensure that sensitive information is relevant to its intended use, accurate, complete, and current. Demand Frontier does not provide any of the information we collect to third parties other than to market our products and services.

Website: Demand Frontier uses the information we collect to identify and contact visitors to our website(s) who are seriously interested in our products and services. Cookies allow us to store user preferences and settings; enable sign-in; provide interest-based advertising; combat fraud; and analyze how our websites and online services are performing.

Applications: Using Demand Frontier applications, information can be processed on an organization's own computers or on computers hosted by Demand Frontier. In the latter case, Demand Frontier is an Application Service Provider (ASP), however, each client, as the collector, administrator, and user of sensitive information within applications, has primary responsibility for the privacy of that information. Demand Frontier, as an ASP, may collect application usage data for the purpose of product improvement and support.

Clients, Partners, and Prospects: Demand Frontier may collect information from Clients, Partners, and Prospects for the purposes of marketing, product support, and other appropriate channels. Demand Frontier takes reasonable steps to ensure that sensitive information is relevant to its intended use, accurate, complete, and current. Demand Frontier does not provide any of the information we collect to third parties other than to market our products and services.

4. Notice and Consent

Demand Frontier will inform individuals about the type(s) of sensitive information it collects, the purposes for which it collects and uses sensitive information, and the types of non-agent third parties to which Demand Frontier discloses or may disclose information, and the choices and means, if any, Demand Frontier offers individuals for limiting the use and disclosure of their sensitive information. Notice will be provided in clear and conspicuous language before individuals are first asked to provide sensitive information to Demand Frontier, or as soon as practicable thereafter, and in any event before Demand Frontier uses or discloses the information for a purpose other than that for which it was originally collected.

Demand Frontier will offer individuals the opportunity to choose (opt-out) where their information is to be (a) disclosed to a non-agent third party, or (b) used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Per the EU General Data Protection Regulation, an opt-in opportunity will be provided to applicable individuals prior to data collection.

Sensitive Personal Information may be processed only under certain conditions. Demand Frontier will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of any information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Demand Frontier will provide individuals with reasonable mechanisms to exercise their choices.

5. Access and Correction

Upon request, Demand Frontier will grant data subjects reasonable access to sensitive data that it holds about them, including information about how the data was collected and its purpose(s).

Additionally, Demand Frontier will take reasonable steps to delete information if the processing of such data has no legal basis, or if the legal basis has ceased to apply. Individuals may also request the correction or amendment of information that is determined to be inaccurate or incomplete, or objection to information processing altogether.

6. Information Security and Confidentiality

Demand Frontier has implemented industry standard security methods, technologies, and processes to safeguard sensitive information from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. All sensitive information is treated confidential; any unauthorized collection, processing, or use of such data is prohibited. In the context of increasingly flexible company organization, it must be ensured that employees have access to sensitive data on a need-to-know basis only. The need-to-know principle means that employees may have access to sensitive information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

7. Regulatory Information

This statement embodies the internationally accepted principles of data protection and privacy, without replacing existing national laws. It applies in all cases as far as it is not in conflict with the respective national law; additionally, the national law shall apply if it makes greater demands. National law applies in the case that it entails a mandatory deviation from, or exceeds the scope of, this statement for data protection. This statement also applies in countries in which there is no corresponding national legislation in place.

EU GDPR: Demand Frontier adheres to the EU General Data Protection Regulation as set forth by the European Parliament & Council regarding the processing of personal data and the free movement of such data.

EU-U.S. and Swiss-U.S Privacy Shield: Demand Frontier adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Demand Frontier has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. The Federal Trade Commission has jurisdiction over Demand Frontier's compliance with the Privacy Shield.

If there are any conflicts between the terms in this statement and EU data privacy principles, the principles shall govern.

This statement will be revised periodically in accordance with industry standards and changes in Demand Frontier's operational environment.