Data Protection Agreement

This Data Protection Agreement ("Agreement") is entered into by and between TechTarget, Inc., a Delaware corporation with a principle place of business at 275 Grove Street, Newton, Massachusetts, United States 02466 ("TechTarget") and _____, a _____ registered in _____ with a principle place of business at_____ ("Client"), and forms part of all agreements between the parties relating to the subject matter of this Agreement (each a "Contract(s)").

The terms in this Agreement shall only apply to the extent that either party collects or otherwise processes Data (including Personal Data) protected or otherwise regulated by EU Data Protection Law.

IT IS AGREED:

1. Definitions.

1.1 Capitalized terms not otherwise defined in Schedule 1 shall have the meanings attributed to them in TechTarget's Terms and Conditions.

2. Scope of Processing.

2.1 The parties acknowledge that: (i) in connection with the Services, TechTarget may collect or otherwise receive data (including Personal Data) about or related to end users or registered users of the TechTarget Properties (other than such data of Client) as such data is more particularly described in the TechTarget Privacy Policy (collectively "**Data**"). For clarity, the types of Data subject to this Agreement include leads, active prospects, or other such data and deliverables provided by TechTarget to Client pursuant to the Agreement. **Data** does not include data that Client provides to TechTarget to facilitate the administration and delivery of the Services contemplated in the Contract and that type of Client data transfer is governed by a separate data processing agreement signed by the Parties. The parties acknowledge and agree that Client may process the Data for the purposes contemplated by the Contract ("**Permitted Purposes**").

3. Relationship of the Parties.

3.1 The parties acknowledge that, to the extent the Data contains Personal Data, each party shall process such data as a separate and independent Controller and in Client's case, only for the Permitted Purposes. In no event will the parties process Personal Data under this Agreement as joint Controllers and as such, each party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under the Privacy Requirements. Nothing in this Agreement shall limit TechTarget from collecting or using data that TechTarget would otherwise collect and process independently of Client's purchase of the TechTarget Services.

4. Client's Responsibilities.

4.1 Obtaining Consent. TechTarget represents and warrants that it: (a) has obtained all necessary permissions and valid consents from the relevant data subjects in accordance with Privacy Requirements to lawfully permit TechTarget and Client to collect, process and share Data for the purposes contemplated by the Contract(s) and (b) shall, at all times, make available, maintain and make operational on the TechTarget Properties (i) a mechanism for obtaining such consent from data subjects in accordance with the requirements of the Privacy Requirements; and (ii) a mechanism for data subjects to withdraw such consent (opt-out) in accordance with the Privacy Requirements.

4.2 Consent Records. TechTarget shall maintain a record of all consents obtained from data subjects as required by the Privacy Requirements, including the time and data on which consent was obtained, the information presented to data subjects in connection with their giving consent, and details of the mechanism used to obtain consent. Client shall maintain a record of the same information in relation to the use of Data and all withdrawals of consent by data subjects. TechTarget and Client shall make the aforementioned records available to one another promptly upon written request.

4.3 Notice Requirements. TechTarget represents and warrants that it shall conspicuously post, maintain and abide by a publicly accessible privacy notice within the TechTarget Properties from which the Data is collected that satisfies the requirements of the Privacy Requirements. Without prejudice to the generality of the foregoing, such notice shall at a minimum include the following information, as required by applicable law: the type of Personal Data collected by TechTarget and the purposes of processing thereof; the categories of individuals or processors who will have access to the Personal Data; where applicable, the legitimate interests pursued by TechTarget and; the identity of the Controller(s) ; and/or and any other information required to comply with the information and transparency requirements of the EU Data Protection Law.

4.4 Prohibited Data Sharing. Client may only share Data as set forth in the Contract(s) and in accordance with applicable EU Data Protection Law. Upon written request, Client shall provide the names and contact information of the third parties which have access to or process the Data.

4.5 Noncompliance. If Client is unable to comply with its consent and notice obligations under this Agreement in respect of the Data, Client shall promptly notify TechTarget.

5. Cooperation and Data Subject Rights.

5.1 The parties shall, on request, provide each other with all reasonable and timely assistance (at their own expense) to enable the other party to comply with its obligations under the Privacy Requirements, specifically in order to enable the other party to respond to: (i) any request from a data subject to exercise any of its rights under EU Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) in relation to the Data ("**Data Subject Rights**"); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the

processing of the Data. Each party shall promptly inform the other if it receives any request directly from a data subject to exercise a Data Subject Right in relation to the Data.

6. International Transfers.

6.1 To the extent that either party processes (or causes to be processed) any Personal Data protected by EU Data Protection Law and/or originating from the EEA (including the United Kingdom) and/or Switzerland ("EEA Personal Data") in a country outside of the EEA and/or Switzerland (as applicable), it shall first take all such measures as are necessary to ensure an adequate level of protection for such EEA Personal Data in accordance with the requirements of EU Data Protection Law and, to the extent that such Personal Data is transferred outside of the EEA, the parties shall ensure the proper protection of the Personal Data by self-certifying to the Privacy Shield and complying with the Privacy Shield Principles or by using such other legally valid means deemed adequate by the EU for the purposes of transferring Personal Data outside of the region.

7. Security.

7.1 Both parties shall implement appropriate technical and organizational measures to protect the copy of the Data in their possession or control (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data. At minimum, such measures shall include the security measures identified in Schedule 2.

8. General.

8.1 If there is any conflict between any provision in this Agreement and any provision in the Contracts regarding the transfer or use of Data, this Agreement controls and takes precedence.

8.2 This Agreement shall survive termination or expiry of any Contracts. Upon termination or expiry of the Contracts Client may continue to process the Data provided that such processing complies with the requirements of this Agreement and the Privacy Requirements.

8.3 Each party reserves the right to suspend, or terminate this Agreement should the other party breach this Agreement and such breach cannot be remedied (if remediable) within a reasonable period.

8.4 This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. This Agreement may be executed via a recognized electronic signature service or delivered by facsimile transmission, or may be signed, scanned and emailed, and any such signatures shall be treated as original signatures for all applicable purposes.

IN WITNESS WHEREOF, intending to be legally bound, and further intending that this Agreement constitute an agreement executed under seal, each of the parties have caused this Agreement to be executed as of the day and year of the latter date set forth below.

CLIENT		**TECHTARGET, INC.**	
By:	_____	**By:**	_____
Name:	_____	**Name:**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

Schedule 1

For the purposes of this Agreement, the following terms shall have the meanings set forth below.

1. "**Controller**" means the entity that determines the purposes and means of the processing of Personal Data.

2. "**Data**" has the meaning given to it in Section 2 of this Agreement.

3. "**EU Data Protection Law**" means (i) prior to May 25, 2018, the EU Data Protection Directive (Directive 95/46/EC), and on and after May 25, 2018, the EU General Data Protection Regulation (Regulation 2016/679); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any national laws made under or pursuant to (i) or (ii) (in each case, as superseded, amended or replaced).

4. "**Personal Data**" means any information relating to an identified or identifiable natural person to the extent that such information is protected as personal data under applicable EU Data Protection Law.

5. "**Privacy Requirements**" means all applicable international, federal, national and state data protection and privacy laws, regulations, and industry self-regulatory rules, codes and guidelines that apply to the processing of Data (including Personal Data) that is the subject of this Agreement (including where applicable (i) the rules, codes and guidelines of the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI); and (iii) EU Data Protection Law (in each case, as amended, superseded or replaced.

6. "**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017, respectively.

7. "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded or replaced).

8. "**TechTarget Property**" means the websites, mobile applications and/or other digital media properties owned or operated by TechTarget or which are made accessible through the TechTarget Services.

9. "**Services**" shall mean the services provided by TechTarget to Client in accordance with and as described in the Agreement.

10. "**Tracking Technologies**" means cookies, mobile SDKs, browser cache, unique identifiers, web beacons, pixels and/or similar tracking technologies.

11. "**TechTarget Privacy Policy**" means the TechTarget privacy policy available on TechTarget's public facing website, the most current version of which is available at www.techtarget.com/privacy-policy (as updated or amended from time to time).

12. "**data subject**", "**processing**" (and "**process**") shall have the meanings given to them in EU Data Protection Law.

Schedule 2

Organizational Security

1. The establishment of an ability to evidence the implementation of an information security management program that is actively maintained, continually improving, and reviewed at least annually and provide evidence of such program and review
2. The establishment of an ability to evidence the implementation of Information Security and an Acceptable Use Policies. Such policies must be continually improving, reviewed at least annually, and require all employees, contractors and interns to review and acknowledge annually.
3. The establishment of an ability to evidence the implementation of an Access Control Policy, a Change Management Policy, a Mobile Device Management Policy, and a Remote/Teleworker Policy. The policies must be continually improving and reviewed at least annually.
4. The establishment of an ability to evidence the implementation of Security Awareness and Training Program that all employees are required to complete at hire and at least annually thereafter.
5. The establishment of an ability to evidence the implementation of a Business Continuity Disaster Recovery Plan. The plan must be tested, reviewed, updated, and approved by management at least annually.
6. The establishment of an ability to evidence the implementation of physical security controls and protocols, including Processor shall limit access to areas where Controller data is processed and maintain audit logs of access.
7. The establishment of an ability to evidence the implementation of an Asset Management Program to manage and track all Controller owned or managed assets.

Technical Security

1. The establishment of a method to communicate and/or push security patch updates for operating systems, software, and applications deployed in its environments. Critical patches and or updates must be deployed within thirty (30) days of release.

2. An auditable program by which the Controller will monitor, grant, and terminate access credentials to individuals. Such program shall require all employees who have access to or maintain Controller data to (i) have a unique user id/account, (ii) not share user id/account with other users, and (iii) shall require two (2) factor authentication. Such program shall require all user accounts are required to: (i) have passwords expire at least every one hundred (180) days, (ii) set to remember and not allow the use of at least the last five (5) passwords, (iii) where passwords are used, require the use of complex (upper/ lowercase alpha, special character, and a number) passwords, (iv) lock a user account after five (5) or less unsuccessful attempts, and (v) remain locked out for at least fifteen (15) minutes.
3. Controller shall have in place a method for managing and rotating access keys / SSH keys at a minimum of every one hundred eighty (180) days.
4. Controller must use full disk encryption on all corporate managed devices and encrypt all Controller data in transit and at rest.
5. If Controller performs backup of Controller data the: (i) backups are required to be performed and stored in a secure location and (ii) backups shall be encrypted.
6. Controller must have in place an intrusion detection and prevention system in all corporate and production locations.
7. Controller must have in place anti-virus and anti-malware software on all Processor owned devices. The software must be configured to: update at least daily, not allow local device level deactivation of the product, and perform full scans at least weekly. Controller must require employees to report anomalies to security personnel who shall take appropriate action.