MAIN SERVICES AGREEMENT

The Main Services Agreement (this "MSA" or "Agreement") is entered into by and between DoubleVerify, Inc., a company incorporated under the laws of the State of Delaware with a principal place of business at 233 Spring Street, 4th Floor, New York, New York 10013, and its subsidiaries ("DV"), and «CONTRACT_ACCOUNT» ("Client"), and is effective as of the later date of the signatures below (the "Effective Date").

Client and DoubleVerify hereby agree that the following terms and conditions shall apply on all purchases of DoubleVerify Services.

1. **Service(s), Implementation and Fees**.

a. Services. DV provides digital media measurement and analytics services ("Services", and each a "Service") through its software platform (the "Platform"). Each purchase of a Service shall be made by executing a service order or main service order ("SO" or "MSO" respectively), itemizing the Services ordered and duration of the Services. During the Term of this Agreement and as may occur from time to time, the Services, the Platform, and the Platform's user interface ("UI") may be adjusted, improved, or modified as DV may deem necessary. DV may use affiliated entities, subsidiaries and/or other related entities ("DV Affiliates") to fulfil its obligations hereunder. During the Term of this Agreement, DV shall make the Services and UI available to the Client pursuant to the terms of this Agreement and all applicable SOs and MSOs. Access to and use of the Services and UI is granted solely to the Client stated in the SO or MSO and shall not be shared with any third parties other than those designated by Client and approved by DV. As applicable, Client hereby grants to DV a royalty-free right, during the Term of this Agreement, to add tracking technology to advertisements or designated advertisement inventory which may be delivered by or on behalf of the Client or any of its clients or that may be on Client's media properties ("DV Technology"). The Term of this Agreement shall commence on the Effective Date, and shall continue thereafter unless terminated pursuant to this Agreement (the "Term").

b. Implementation. In the event that the Client is responsible for implementing the DV Technology, it is Client's responsibility to ensure that the DV Technology is properly implemented in accordance with any instructions provided to Client by DV, and DV shall assume no responsibility regarding the implementation of the DV Technology. DV may assist Client with implementation, but does not make any guarantees that implementation will ultimately meet Client's expectations. If the Services cannot be provided by DV due to the implementation, DV shall have no liability or obligations hereunder.

c. Fees. Client on behalf of itself, affiliates, and its subsidiaries and/or related entities ("Client Affiliates") who may later become a party to this MSA upon written approval by DV, shall pay the fees ("Fees") as specified in each SO or MSO. All applicable Fees shall be paid within 30 days from the issuance of an invoice. DV reserves its right to increase Fees for any of its Services upon providing Client with thirty (30) days prior written notice. Such price increases shall apply to all SOs and MSOs subsequent to the effective date of such price increase unless otherwise stated by DV in its notification. The termination of any specific Service shall not affect Client's obligations to pay for other Services. DV usage statistics shall be used for billing purposes unless otherwise specified in a SO or MSO. Client authorizes DV to invoice Client for any DV recorded usage of the Services regardless of whether the Services are active under the Agreement. All undisputed, based upon written commercially reasonable objections, past due Fees shall bear interest at the rate of one percent (1%) per month, beginning with the date on which the applicable amount became past due ("Default Interest"). It is expressly agreed that in the event that any undisputed payment is past due, DV may limit or restrict the provision of the Services with or without notice. All Fees are exclusive of all applicable taxes, duties, tariffs and similar fees now in force or enacted in the future imposed on the transaction and/or the delivery of Services, all of which Client shall be responsible for and shall pay in full. In the event DV is obligated to charge any value added, sales, or similar tax to Client, DV shall ensure that Client is invoiced in accordance with applicable laws. Neither party is responsible for taxes on the other party's income or the income of the other party's personnel or subcontractors. If Client is required by government regulation to withhold taxes for which DV is responsible, Client will deduct such withholding tax from payment to DV and provide to DV a valid tax receipt in DV's name. If DV is exempt from such withholding taxes as a result of a tax treaty or other regime, DV shall provide to Client a valid tax treaty residency certificate or other tax exemption certificate. All applicable taxes and Fees must be paid in accordance to the applicable payment terms.

2. **Intellectual Property**.

a. "Intellectual Property Rights" consists of the following: (i) copyrights, including moral rights, registrations and applications for registration thereof; (ii) software, data and documentation; (iii) patents, patent applications and all related

continuations, divisional, reissue, utility model, design patents, applications and registrations thereof, certificates of inventions; (iv) mask works and registration thereof; (v) trade secrets,Confidential Information, know-how, manufacturing and product process and techniques, designs, concepts, methodologies, models, templates, algorithms, prototypes, enhancements, improvements, work-in progress, research and development information; and (vi) other proprietary rights relating to the foregoing.

b. Ownership. DV owns and shall retain all rights, including Intellectual Property Rights, in and to the Platform, UI, the DV Technology, Services, the DV Data (as defined below), and to Confidential Information provided by DV in connection therewith (collectively, "DV Intellectual Property"). Client owns and shall retain all rights, including Intellectual Property Rights, in and to the Client Data (as defined below), and to Confidential Information provided by Client in connection therewith. Without limiting the foregoing, Client may not, and may not cause or permit others to: (i) license, rent, sale, distribute, lease, encumber, pledge, lend, copy, make available, or resell any of the DV Intellectual Property, including but not limited to the DV Data, to any third party, except as expressly permitted in this MSA, SO or MSO, (ii) reverse engineer or decompile, modify, or create derivative works of, or revise the DV Intellectual Property or any part thereof, (iii) access or use the Services, data or any DV Intellectual Property in order to build a similar or competitive product or provide a substitute solution to an existing DV Service, or (iv) make, create or contribute to any public comments, remarks or publications that disparage DV or the Services to the extent DV's Intellectual Property, the DV Data, any Confidential Information, or the Services are used as supporting or source material ("Restricted Uses").

3. Data and License.

a. DV Data. DV Data shall mean any data or information collected by the DV Technology or stored in its UI or Platform, excluding Client Data.

b. License. Subject to the terms and conditions of this Agreement and as more specifically defined in any applicable SO or MSO, DV hereby grants to Client a limited, non-exclusive, non-transferrable, non-sublicensable, worldwide right to access and use the Services and UI for Client's own internal business purposes during the Term.

c. Client Data. Client Data shall mean any and all details input into the UI that are not independently available ("Client User Details"), intellectual property, and any other data that directly identifies the Client, other than Excluded Information. Client is solely responsible for collecting, inputting, and updating Client User Details. Client acknowledges and agrees that DV may collect Client Data through the provision of the Services. Client represents and warrants that all Client Data has been and will continue to be collected and delivered to DV in compliance with all applicable laws, rules and regulations, and without infringing any rights of any third party including, without limitation, Intellectual Property Rights. Unless otherwise altered or modified by DV, Client acknowledges that DV shall assume no liability with respect to the Client User Details. Notwithstanding Section 4, Client shall grant to DV a non-sublicensable, non-exclusive, worldwide license to use Client Data during the Term for: (i) reporting, including but not limited to, compilations of aggregated and anonymous statistics about the Services for purposes of fraud and IVT analysis and prevention, to promote brand safety and content contextual analysis, and to further analyze the performance and usage of the Services that may be provided to customers and prospects; (ii) performing its obligations and enforcing its rights hereunder; (iii) improving the DV Intellectual Property which may occur through insights and the creation of derivative data or future services; and (iv) compliance with its certifications and accreditations (e.g., the Media Ratings Council) ("Permissible Uses"). DV may disclose Client Data in accordance with any applicable law or other legal requirements.

4. Confidentiality. "Confidential Information" shall mean all information disclosed to the "Recipient" and designated by the "Discloser" as confidential, whether disclosed orally or in writing, graphic or electronic form. In particular, Confidential Information shall include, but not be limited to, this MSA and any SOs or MSOs, the DV Data, Client Data, Discloser's know-how, research, research results, development, development methodology, Intellectual Property Rights, trade secrets, general business operations, methods of doing business, pricing, prices paid for materials, charges for services and products; financial information, including costs, profits and sales; marketing strategies; names of suppliers, personnel, clients and potential clients; negotiations or other business contacts with suppliers personnel, form and content of bids, proposals and contracts; the Discloser's internal reporting methods; technical and business data documentation and drawings; software programs, however, embodied, manufacturing processes, inventions, and information obtained by or given to the Discloser about or belonging to third parties. The term "Confidential Information" does not include any Excluded Information. Excluded Information shall mean information that was: (a) already in the possession of the Recipient without an obligation of confidentiality; (b) developed independently by the Recipient, as demonstrated by the Recipient, without use of, or reference to, the Discloser's Confidential Information; (c) lawfully obtained from a source other than the Discloser without an obligation of confidentiality; or (d) publicly available when received, or thereafter becomes publicly available (other than through any unauthorized disclosure by the Recipient); or (e) approved in writing to be disclosed by the Discloser. A Recipient shall maintain all Confidential Information in trust and confidence and shall not publish, disseminate or otherwise disclose any Confidential Information to any third party without the written consent of the Discloser or as may be permitted under this Agreement. The Recipient may only disclose Confidential Information to the Recipient's employees, agents or persons within its control ("Permitted Transferees"), provided, at all times, that any such disclosure is limited to a need to know basis and only after the Permitted Transferees have been advised of the confidential nature of such Confidential Information and provided that they are bound by confidentiality obligations, substantially similar to the obligations imposed on the Recipient herein. Notwithstanding anything to the contrary, Recipient shall be liable and responsible towards the Discloser for any disclosure made by any of the Permitted Transferees. Disclosure of Confidential

Information shall not be prohibited if such disclosure: (i) is in response to a valid order of a court ordering such disclosure; provided, however, that the Recipient shall first have given at least fifteen (15) days, advance written notice to the Discloser; or (ii) is otherwise required by law. Recipient shall promptly advise Discloser of any discovered breach by Recipient or its representatives and shall reasonably cooperate, at Recipient's expense, in retrieving the disclosed Confidential Information and restricting any continuing breach.

5. **Representations and Warranties**.

   a. **Mutual Representations and Warranties.** The parties represent and warrant to the other that it: (a) has full power and authority to enter into this MSA, to perform all of its obligations hereunder, and its entry into this MSA does not violate any other agreement to which it is bound. THE WARRANTIES SET FORTH HEREIN ARE LIMITED WARRANTIES AND ARE THE ONLY WARRANTIES MADE BY DV. DV EXPRESSLY DISCLAIMS, AND CLIENT HEREBY EXPRESSLY WAIVES, ALL OTHER EXPRESS WARRANTIES AND ALL DUTIES, OBLIGATIONS AND WARRANTIES IMPLIED IN LAW, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. DV DOES NOT WARRANT AND SPECIFICALLY DISCLAIMS ANY REPRESENTATIONS THAT THE OPERATION OR USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.

   b. **DV Representations and Warranties.** DV represents and warrants that the Services and DV Data: (i) will at all times comply with applicable laws, statutes, statutory instruments, rules, and regulations including but not limited to intellectual property and privacy laws, and (ii) do not currently and shall not infringe upon the Intellectual Property Rights of a third party.

   c. **Client Representations and Warranties.** Client represents and warrants that its use of the Services and DV Data: (i) will at all times comply with applicable laws, statutes, statutory instruments, rules, and regulations including but not limited to intellectual property and applicable privacy laws, and (ii) shall not infringe upon the Intellectual Property Rights of a third party.

6. **Indemnification**: Each party agrees to defend, indemnify (the "Indemnifying Party") and hold the other party and its officers, directors, employees, agents, successors and assignees (the "Indemnified Party"), from and against any third party liability, claims, loss, damage, injury or expense, including reasonable attorney's fees, (collectively, a "Claim") arising out of a breach of any representation or warranty made by the Indemnifying Party set forth herein; provided, however, that the (a) Indemnified Party shall have given the Indemnifying Party a prompt written notice of a Claim; (b) Indemnified Party shall reasonably cooperate with the Indemnifying Party in the defense and settlement thereof; and (c) Indemnifying Party shall have sole control of the defense of such Claim and the settlement or compromise thereof. Notwithstanding anything herein to the contrary, the Indemnifying Party shall not enter into any compromise or settlement that shall have the effect of creating any liability or obligation (whether legal or equitable) on the part of the Indemnified Party without the Indemnified Party's prior written consent, and no such compromise or settlement is hereby authorized unless the Indemnified Party receives a complete release of liability under such compromise or settlement. The Indemnified Party's failure to give notice pursuant to this subsection shall not relieve the Indemnifying Party from its indemnification obligations except to the extent, if any, that the Indemnifying Party is actually prejudiced as a result of such failure. However, and in addition to DV's indemnification obligations herein, if DV believes or in the event that the Services are found to violate the Intellectual Property Rights of a third party, then DV may choose to either (i) procure for Client the right to continue receiving the Services; or (ii) replace or modify the same so that it no longer infringes such Intellectual Property Rights, so long as the utility or performance of the Services is not materially affected by such replacement or modification; or (iii) where (i) or (ii) are not practicable, to terminate this Agreement and stop rendering the Services hereunder without further liability to Client. Notwithstanding the foregoing, DV will not be obligated to indemnify Client if Client alters the Services or uses the Services outside the scope of use identified in this MSA or any applicable MSO or SO.

7. **Limitation of Liability**: TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER DV NOR CLIENT SHALL HAVE ANY LIABILITY WITH RESPECT TO THEIR RESPECTIVE OBLIGATIONS UNDER THIS MSA INCLUDING ITS SOs, MSOs OR WITH RESPECT TO THE USAGE OR PERFORMANCE OF THE SERVICES OR OTHERWISE FOR CONSEQUENTIAL, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. WITH THE EXCEPTION OF INDEMNIFICATION OBLIGATIONS, IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY WITH RESPECT TO ANY SPECIFIC SERVICE EXCEED THE AGGREGATE SUM OF THE FEES ACTUALLY RECEIVED FROM THE CLIENT DURING THE PREVIOUS THREE (3) MONTHS BEFORE SUCH CLAIM AROSE.

8. **Termination**: Either party may terminate this MSA or any of the MSOs or SOs at any time upon the giving of written notice in the event the other party should become (i) insolvent; (ii) upon the filing by or against the other party of a petition in bankruptcy or reorganization; (iii) upon the filing of a request for the appointment of a trustee, liquidator or receiver for such party; (iv) upon an assignment for the benefit of creditors by such party; or (v) such similar action, should said event continue for a period of sixty (60) days. Upon termination or expiration of this MSA (a) all Services provided to Client shall cease immediately; (b) all unpaid Fees of Client under this MSA and any MSO or SO provided through the date of termination shall immediately become due; and (c) upon the written request of the Discloser, the Recipient shall return to Discloser all Confidential Information.

9. **Logo and Trade Marks**: During the Term of this MSA, Client agrees that DV may display Client's logo and name, as provided by the Client, on DV's website, and within its marketing materials. DV may publicly refer to Client, verbally and in writing, as

a client of DV. Client agrees to display DV's logo in a manner consistent with DV's written logo and trademark usage policy which is available at the request of Client.

10. **Governing Law**: Any and all disputes concerning this Agreement shall be submitted exclusively to the jurisdiction of the State of New York, pursuant to the laws of the State of New York.

11. **Miscellaneous**:

a. Force Majeure. Neither party will be liable for failure or delay in performing its obligations due to causes beyond its reasonable control, including events outside of human control, terrorism, war, fire, earthquake, or internet failure (each a "Force Majeure Event"); provided that the party relying upon this provision: (i) gives prompt written notice thereof (if reasonably practicable under the circumstances), and (ii) takes all steps reasonably necessary to mitigate the effects of the Force Majeure Event; provided further, that in the event a Force Majeure Event extends for a period in excess of thirty (30) days, the party awaiting performance may immediately terminate this MSA and any MSO or SO upon written notice.

b. Assignment. Each Party may only assign this MSA in whole as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets, provided that, the other party may terminate this MSA without liability if the assignee is a direct competitor of the other party. Further, such assignment shall only be valid to the extent (i) the assignee shall agree in writing to be bound by this Agreement, and (ii) the assignment shall not release any of the assignor's obligations under this Agreement.

c. User Accounts. As applicable, Client is responsible for the acts and omissions of its users, usernames, and passwords. Client is responsible for any and all uses of its accounts, whether or not authorized by Client. Client is further responsible for maintaining the confidentiality of its usernames and passwords. Client agrees to immediately notify DV of any unauthorized use of Client's account of which Client becomes aware.

d. System Access. In order to provide proper configuration of the Services, DV may require access to certain systems the Client uses in the course of managing its business. These systems will include locally controlled ad serving systems as well as third party reporting systems used to aggregate information pertaining to ad deliveries. System accounts given to DV will be treated as read-only and DV will not insert, remove, or in any other way change the contents contained within them with the sole exception of the creation, alteration, and removal of reports, which DV may require during the normal course of business.

e. Reference to Certain Terms. The term "impression" or "ad impression" as used in this Agreement or any SO or MSO is a reference to contractual unit of billing representing a single instance of a billable Service event. An impression or ad impression may be identified in the DV Technology, DV Data, Services, Platform, UI or 3rd-party systems using a variety of metric labels including, but not limited to, ads, allows, auctions. bids, blocks, calls, filters, impressions, or requests as applicable to the specific Service and billing system of record.

f. Suggestions. DV shall have a royalty-free, worldwide, irrevocable, perpetual license to use and incorporate into any of its current or future Services any suggestions, enhancement requests, recommendations, or other feedback provided by Client.

g. Relationship. The relationship of the parties is that of an independent contractor, and this MSA shall not establish any relationship or partnership, joint venture, employment, franchise, or agency between the parties. Neither party shall have the power to bind the other or incur obligations on the other's behalf without the other party's prior written consent, except as otherwise expressly provided herein. Neither the Client, nor its representatives or employees shall be considered employees of the DV.

h. Entire Agreement. This MSA and the SOs, constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes any prior understanding between the parties. This MSA may not be modified, amended, nor waived, except by a written instrument executed by both parties.

i. Survival. The following Sections which by their nature are intended to survive will survive expiration or termination of this MSA, the MSOs and SOs: Section 2, 3, 5, 6, 7, and 11.

j. Notices. All notices and requests required or delivered under this MSA will be deemed to have been given immediately when made by first class U.S. mail, postage prepaid, to each party's physical address set forth herein. Notices delivered by fax or email will be deemed effective the same day.

k. Conflicting Terms. In the event of a conflict between or among the terms of this MSA, the SOs, or any other document(s) between the parties, they shall control in the following order: the SOs with the most recent date, this MSA and other document(s) executed between the parties.

l. Waiver. The failure of either party at any time to require the performance by the other party of any provision of this MSA shall not affect in any way the right to require such performance at any later time, nor shall the waiver by either party of a breach of any provision hereof be taken or held to be an implied waiver of that provision.

m. Severability. In the event any provision of this MSA shall be determined to be unenforceable, because it is invalid or in conflict with any law of any relevant jurisdiction, the validity of the remaining provisions shall not be affected, and the rights

and obligations of the parties shall be construed and enforced as if this MSA did not contain the particular provision(s) held to be unenforceable.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed and delivered as of Effective Date.

DOUBLEVERIFY, INC.

Signature: {{_es_signer2_signature }}
By: {{_es_signer2_fullname }}
Title: {{_es_signer2_title }}
Date: {{_es_signer2_date }}

CLIENT: «CONTRACT_ACCOUNT»

Signature: {{_es_signer1_signature }}
By: {{_es_signer1_fullname }}
Title: {{_es_signer1_title }}
Date: {{_es_signer1_date }}

Exhibit 1

DATA PRIVACY ADDENDUM

This Data Processing Addendum (this "DPA") is supplemental to the Agreement and entered into between the Client and DoubleVerify, Inc., on behalf of itself, its affiliates and subsidiaries (hereinafter the "DV"). For the avoidance of doubt, the scope of this DPA is to memorialize obligations and rights mandated by applicable laws and the obligations herein are intended to apply to the extent required by applicable laws in each relevant instance. This DPA shall become effective upon the start of the processing of Personal Data under the terms of the Agreement by DoubleVerify.

1. Definitions

1.1 For the purposes of this DPA, the following terms shall have their respective meanings set forth below. Any other capitalized terms used but not defined in this DPA have the same meanings as set forth, as applicable, in the Agreement or in relevant and applicable laws and regulations:

(a) "**Affiliate**" means, with respect to any Party to the DPA, any person, partnership, joint venture, corporation or other entity which directly or indirectly controls, is controlled by, or is under common control with such Party where "control" (or variants of it) means the ability to direct the affairs of another by means of ownership, contract or otherwise.

(b) "**Agreement**" means the legal agreement entered into between DV and Client, to which this DPA is attached or incorporated by reference providing for the provision by DV to Client of the Services described therein.

(c) "**Client**" means the Party who entered into the Agreement with DV and any successor of same.

(d) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data pursuant to Data Protection Laws, including, as applicable including the "business" under the CCPA.

(e) "**Data Protection Laws**" means any and all applicable national, international, provincial, federal, state and local laws and regulations relating to data protection, data privacy, data security, or the Processing of Personal Data, including (where applicable) European Union Data Protection Legislation, the California Consumer Privacy Act ("**CCPA**") (California Civil Code §§ 1798.80, et seq.), and any other provincial or state privacy laws that may take effect during the term of the Agreement. References to the GDPR shall be construed to refer equally to the retained UK GDPR under the Data Protection Act 2018.

(f) "**Data Subject**" has the meaning given in the GDPR and shall encompass, as applicable the term "consumer" as defined in the CCPA.

(g) "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein.

(h) **"EU"** means European Union.

(i) "**EU Data Protection Legislation**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") (as amended, replaced or superseded).

(j) "**Personal Data**" means any information relating to an identified or identifiable natural person, or, as applicable, a household. The definition of Personal Data herein shall include "pseudonymous information" as defined by the GDPR.

(k) "**Processing**" has the meaning given in the GDPR and includes any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(l) "**Processor**" means an entity which Processes Personal Data on behalf of the Controller, including, as applicable the "service provider" under the CCPA.

(m) "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data caused by DV's acts or omissions.

(n) "**Sensitive Data**" means (a) racial or ethnic origin; (b) political opinions; (c) religious or philosophical beliefs; (d) trade union membership; (e) genetic data; (f) biometric data for the

purpose of uniquely identifying a natural person; (g) data concerning health; (h) data concerning a natural person's sex life; (i) sexual orientation; and (ii) without limiting the foregoing, any additional information that falls within the definition of "special categories of data" under EU Data Protection Legislation or Data Protection Laws.

(o) "**Standard Contractual Clauses**" or "**SCCs**" or "**Clauses**" means (a) with respect to EU Data Protection Legislation, the Standard Contractual Clauses (Processors) approved by and set out in the Annex to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data (available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) or any subsequent version thereof released by the European Commission (which will automatically apply to the extent applicable), and (b) with respect to the Data Protection Laws of the United Kingdom, any standard international data transfer agreement or addendum issued under section 119A of the Data Protection Act 2018 or any replacement or subsequent document adopted by the Secretary of State in order to comply with Article 46 of the retained UK GDPR.

2. Relationship with Agreement & Roles of the Parties

2.1 Order of Precedence. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control with respect to the subject matter of the DPA. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.2 Effective Date. This DPA shall become binding on the Parties on the later of: (a) the date this DPA is fully executed, or (b) the commencement of Services.

2.3 Parties' Roles. With respect to the Processing of Personal Data, Client, as Controller or Processor, as applicable, appoints DV, as the Processor, to Process the Personal Data described in **Annex B** on Client's behalf. Notwithstanding the foregoing, the Parties acknowledge and agree that a portion of the Services (fraud elimination) are operated by DV as Controller and DV, in its capacity as Controller, shall comply with the applicable obligations set forth in this DPA and by the GDPR, as well as other applicable laws. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA, nor confer any rights or benefits or impose any obligations on either Party not otherwise required by appliable laws in each relevant instance. For the avoidance of doubt, the Parties acknowledge and agree that DV's Processing, in its capacity as a Processor or a Controller, is limited to pseudonymous information.

3. Controller Terms

3.1 Applicability of the DPA. To the extent that DV processes any Personal Data as a Controller in connection with the Agreement or in the performance of the Services, the terms set out in this Section 3 shall apply. Further, Sections 5, 6, 7, 9, 10, 11 and 12 of this DPA shall be deemed applicable, as detailed therein, to DV in its capacity as a Controller.

3.2 Purposes of the Processing, DV shall only process such Personal Data for purpose of providing, maintaining and improving the Services, to fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Services such as billing, account management, technical maintenance and support, product maintenance and improvement.

3.3 Responsibilities of the Parties. Each party shall be responsible for its compliance with all applicable obligations imposed by applicable Data Protection Laws in relation to its processing of Personal Data as it relates to the Agreement. In particular, each Party shall be individually responsible for ensuring that its processing of the Personal Data is lawful, fair and transparent in accordance with Data Protection Law, including the maintenance of applicable notices related to the Party's privacy practices.

4. Processor Terms

4.1 Applicability of the DPA. To the extent that DV processes any Personal Data as a Processor in connection with the Agreement or in the performance of the Services, the terms set out in this Section 4 shall apply.

4.2 Purpose Limitation. Processor shall Process the Personal Data for the purposes described in **Annex B**

and only in accordance with Client's lawful, written instructions, except where otherwise required by applicable law. The Agreement and this DPA sets out Client's complete instructions to Processor in relation to the Processing of the Personal Data and any Processing required outside of the scope of these instructions will require prior written agreement between the parties. Client acknowledges that Processor shall have a right to Process Personal Data in order to provide the Services to Client, fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Services such as billing, account management, technical maintenance and support, product improvement and maintenance.

4.3 Description of Processing. A description of the nature and purposes of the Processing, the types of Personal Data, categories of Data Subjects, and the duration of the Processing are set out further in **Annex B**.

4.4 Compliance. Client shall be responsible for ensuring that:

(a) Client has complied, and will continue to comply, with Data Protection Laws, in Client's use of the Services and Client's own Processing of Personal Data, including, where applicable, by providing notice and obtaining all consents and rights necessary under Data Protection Laws for Processor to process Personal Data. To the extent consent is required, Client shall, at all times, make available, maintain and make operational a mechanism for obtaining such consent from data subjects in accordance with the requirements of the Data Protection Laws; and a mechanism for data subjects to withdraw such consent (opt-out) in accordance with the Data Protection Laws; Client shall maintain a record of all consents obtained from data subjects as required by the Data Protection Laws, including the time and date 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; maintain a record of the same information in relation to all withdrawals of consent by data subjects; and make these records available to Processor promptly upon request; and

(b) Client has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Processor for Processing in accordance with the terms of the Agreement and this DPA.

5. Prohibited Practices

5.1 Sale and Enrichment of Data Sets. Under no circumstances will DV lease, rent or sell, Personal Data. This prohibition shall extend, as applicable, to prohibit any "sale" as defined by the CCPA. The Parties further agree that, under no circumstance will DV be required to enrich any Personal Information it may Process in any capacity under the terms of this DPA to identify the individuals to whom such Personal Data is linked.

5.2 Prohibited Data. Client will not provide (or cause to be provided or collected) any Sensitive Data to DV for Processing under the Agreement, and DV will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, the obligations of DV under this DPA will not apply to Sensitive Data unless the Processing of Sensitive Data is otherwise permitted by Data Protection Laws or Client has obtained DV's prior written consent.

5.3 Disclosures. Neither Party shall make any statement (or provide any documents) about matters concerning the processing of Personal Data under the Agreement (or that otherwise refers to or identifies (directly or indirectly) the other Party), without the prior written approval of the other Party, except where the Party is legally required to do so without the approval of the other Party, in which case the disclosing Party shall promptly provide a copy of any such statements or documents to the other Party unless prohibited by applicable law.

6. Data Security and Confidentiality

6.1 Security. DV shall implement and maintain appropriate technical and organizational measures designed to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including as appropriate, the measures referred to in Article 32(1) of the GDPR. Notwithstanding the above, Client agrees that Client is responsible for Client's secure use of the Services, including securing Client's account authentication credentials.

6.2 Security Exhibit. The technical and organizational security measures which DV shall have in place

under the Agreement are set out at **Annex D** to this DPA.

6.3 Confidentiality of Processing. DV shall ensure that any person that it authorizes to Process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

6.4 Security Incidents. Upon becoming aware of a Security Incident DV shall: (a) take appropriate steps to investigate and mitigate the effects of such a Security Incident on the Personal Data under this Agreement; (b) notify Client (by contacting the Client's business, technical or administrative contact, including via email) without undue delay, and, (c) provide such timely and known information as Client may reasonably require, including to enable Client to fulfil any data breach reporting obligations under Data Protection Laws. This Section 4.4 does not apply to Security Incidents that are caused by Client, including Client's employees, partners, subcontractors, or agents. Client further agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer Personal Data or to any of DV's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7. International Transfers

7.1 Restricted Transfers. With respect to Personal Data originating in the EEA, the Parties agree that an adequate transfer mechanism much be used to legally support such transfers ("Restricted Transfers").To the extent that the Processing by DV involves any such Restricted Transfers, such export shall be governed by either: (i) a compliance scheme recognized as offering adequate protection for the rights and freedoms of Data Subjects as determined by the European Commission, (ii) Binding Corporate Rules, or (iii) the latest approved version of the Standard Contractual Clauses.

7.2 Execution of the Standard Contractual Clauses. To the extent applicable to the relationship between the Parties, the Parties hereby agree that by signing this DPA, the most relevant (whether Controller to Controller, Controller to Processor or Processor to Processor, as applicable from time to time) and up to date version of the Standard Contractual Clauses ("**SCCs**" or the "**Clauses**") are deemed to have been executed, with Client in the capacity of Exporter and DV in the capacity of Importer. To the extent the Commission has not released a set of SCCs applicable to Controllers and Processors located both outside the EEA, if Client is not a Controller or a Processor in the EU, notwithstanding the absence of a specific set of clauses for Restricted Transfers between non-EU Controllers or Processors to non-EU Processors, the parties hereby agree that, to the extent applicable, Client enters into the SCCs as exporter. Client agrees that this DPA constitutes Client's written authorization for DV and its sub-processors to Process Personal Data, in accordance with the terms of this Section, anywhere in the world where DV or its Sub-processors maintain data Processing operations.

7.3 Governing Law and Choice of Forum and Jurisdiction. To the extent they are deemed applicable, these Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Spain, or with respect to the UK, the laws of England. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State. The Parties agree that those shall be the courts of Spain or with respect to the UK, the courts of England. A data subject may also bring legal proceedings against the data exporter and/or data importer before the court of the Member state in which he/she has his/her habitual resident. The Parties agree to submit themselves to the jurisdiction of such courts.

7.4 Additional Controls. The Parties understand that by virtue of the judgment in the EU Court of Justice Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("Schrems II Decision"), Restricted Transfers to the United States of America require, in addition to the SCCs, additional safeguards in order to ensure an adequate level of protection for Personal Information originating in the EEA ("Additional Safeguards"). The Parties agree to supplement the Standard Contractual Clauses with the following Additional Safeguards: (i) Personal Information shall be protected by DV in accordance with the security safeguards agreed upon by the Parties and memorialized in Annex D (ii) DV represents that, as of the date of this DPA, it has not received any national security orders of the type described in Paragraphs 150-202 of Schrems II Decision; (iii) DV represents that, as of the date of this DPA, it has no knowledge of any court having found DV to be deemed an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4)

or a member of any of the categories of entities described within that definition that could be compelled to provide assistance under the process contemplated in section 702 of the United States Foreign Intelligence Surveillance Court ("FISA"); and (iv) DV will resist, in accordance to applicable laws, any request under FISA for bulk surveillance (i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).

8. Sub-Processing

8.1 Sub-Processors. Client agrees that this DPA constitutes Client's written authorization for DV, in its capacity as a Processor, to engage Affiliates and third-party sub-processors (collectively, "**Sub-processors**") to Process the Personal Data on DV's behalf, including Sub-processors currently engaged by DV. As applicable law requires, DV will notify Client of any new Sub-processor being appointed by posting an updated list of Sub-processors in the applicable reporting portal. A list of the then applicable Sub-processors is included in this DPA as Annex C. For the avoidance of doubt, future updates to the list shall not require an amendment to this DPA.

8.2 Objection to Sub-processors. Client may object in writing, stating Client's reasonable grounds for the objection, to the appointment of an additional Sub-processor within five (5) calendar days after receipt of DV's notice in accordance with the mechanism set out at Section 7.1 above. In the event that Client objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, DV will, at its sole discretion, either not appoint such Sub-processor, or permit Client to suspend or terminate the Services in accordance with the termination provisions of the Agreement. In the event that Client suspends or terminates the Services in accordance with the preceding sentence, Client shall immediately pay all fees and costs then owing and all fees and costs incurred by DV as a result of the termination.

8.3 Sub-processor obligations. Where a Sub-processor is engaged by DV as described in this Section 6, DV shall:

(a) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data at least as restrictive as the ones agreed upon herein and in the Agreement;

(b) for all Restricted Transfers involving a Sub-processor other than in-house contractors, DV shall ensure that the Standard Contractual Clauses or any other lawful transfer mechanism is in place before the Sub-processor Processes any Personal Data; and,

(c) remain responsible for any breach of the DPA caused by a Sub-Processor.

9. Cooperation

9.1 Cooperation and Data Subjects' rights. In the event that a Data Subject request is made directly to DV, DV shall, unless prohibited by law, address such request directly. To the extent DV operates as a Processor, where any such Data Subject request identifies Client, DV shall promptly notify Client of the request and defer to Client's instruction for its resolution. In the event that a Data Subject request is made directly to the Client, DV shall, taking into account the nature of the Processing, provide commercially reasonable assistance to Client insofar as this is possible, to enable Client to respond to requests from a Data Subject seeking to exercise their rights under Data Protection Laws in the event Client does not have the ability to implement such requests without DV's assistance. To the extent legally permitted, Client shall be responsible for any costs arising from DV's provision of such assistance.

9.2 Data Protection Impact Assessments. DV shall, to the extent required by EU Data Protection Legislation and at Client's sole expense, taking into account the nature of the Processing and the information available to DV, provide Client with commercially reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Client are required to carry out under Data Protection Laws.

10. Security Reports and Audits

10.1 Annual Security Reviews. The parties acknowledge that DV may use external auditors to comprehensively assess the security of the systems and premises used by DV to provide data Processing

services. The parties further acknowledge that best practice is for these audits:

(a) To be performed at least once each year;
(b) To be conducted by auditors selected by DV, but otherwise conducted with all due and necessary independence and professionalism; and
(c) Must be fully documented in an audit report that affirms that DV's controls meet industry standards against which they are assessed ("**Report**").

10.2 Summary Reports. At Client's written request and at Client's sole expense, DV will (on a confidential basis) provide Client with a summary of any available Report so that Client can verify DV's compliance with the audit standards against which it has been assessed. DV will further provide written responses (on a confidential basis) to reasonable requests for information made by Client, no more than once per year, including responses to information security and audit questionnaires that are necessary to confirm DV's compliance with this DPA.

10.3 Audits. While it is the parties' intention to rely on the provision of a Report and written responses provided under Section 8.2 above to verify DV's compliance with this DPA, DV shall permit Client (or Client's appointed third party auditors, which must be reasonably acceptable to DV), at Client's sole expense, to carry out an audit of DV's Processing of Personal Data under the Agreement following a Security Incident suffered by DV, or upon the instruction of a data protection authority, to determine DV's compliance with this DPA. Any such audits must be limited to once per calendar year. Client must give DV at least twenty (20) days' prior notice of such intention to an audit. Audit requests must be delivered in accordance with the notification requirements outlined in the Agreement. Audits shall be carried out on agreed upon dates, remotely or at DV's primary place of business, during normal business hours, in a manner that shall prevent unnecessary disruption or unduly burden DV's operations. Any such audit shall be subject to DV's health, safety, security and confidentiality terms and guidelines. Following completion of the audit, upon request, Client will promptly provide DV with a complete copy of the results of that audit. Notwithstanding the foregoing, DV will not be required to disclose any proprietary or privileged information, including to Client or any of Client's auditors, agents, or vendors. In the event that such audits reveal DV's material non-compliance with this DPA, the cost of the audit shall be reimbursed by DV.

11. Deletion and Return of Data

11.1 Deletion or return of data. Upon the termination or expiration of the Agreement, upon Client's request, to the legally permitted and in accordance with DV's retention policies, DV will make return of Personal Data entered into the Services, that is in DV's possession or control and at the end of that period. DV will, upon Client's request, delete or destroy all copies of Personal Data in its possession or control, save to the extent that: (i) DV is required by any applicable law to retain some or all of the Personal Data, (ii) DV is reasonably required to retain some or all of the Personal Data for limited operational and compliance purposes, or (iii) Personal Data has been archived on back-up systems. In all such cases, DV shall maintain the Personal Data securely and limit processing to the purposes that prevent deletion or return of the Personal Data.

12. Miscellaneous

12.1 Legal Effect. This DPA shall become legally binding between Client and DV: (i) when the Agreement this DPA is a part of is fully executed by the Parties, or (ii) upon commencement of Processing of Personal Data; whichever comes later. If the Agreement has been electronically signed by either Party such signature will have the same legal affect as a hand written signature.

12.2 Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.3 Governing Law and Venue. This DPA shall be governed by the laws of the jurisdiction specified in the Agreement. Any dispute arising under this DPA shall be resolved in the venue specified in the

Agreement. If either or neither determinations are made in the Agreement, the applicable law and venue shall default to the location of DV's headquarters.

ANNEX A
CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES ADDITIONAL INFORMATION

In relation to transfers of Personal Data processed in accordance with Section 4 of this DPA, to the extent applicable, the Standard Contractual Clauses are completed as follows:

- When Client is acting as a Controller, Module Two will apply.
- In Clause 7 (Docking clause), the optional docking clause will apply.
- In Clause 9 (Use of sub-processors), Option 2 will apply and the time period for prior notice of Sub-processor change shall be set out in Section 1.6 of this DPA.
- In Clause 11 (Redress), the optional language shall not apply.
- In Clause 17 (Governing Law), Option 1 will apply, and the member state will be Spain.
- In Clause 18 (Choice of Forum and Jurisdiction), the member state will be Spain.

Annex I of the SCCs is completed as follows:

- List of Parties: Client is the data exporter and DV is the data importer. The address, contact details and activities relevant to the transfer for the data exporter and data importer are set out in the Agreement. By signing this DPA, the data exporter and data importer will be deemed to have signed Annex I.
- Description of Transfer: The required information is set out in **ANNEX B**.
- Competent Supervisory Authority: The data exporter's competent supervisory authority will be determined in accordance with EU Data Protection Law.

Annex II is completed as follows:
The required information is set out in **ANNEX C**.

Annex III is completed as follows:
The required information is set out in **ANNEX D**.

ANNEX B
PROCESSING REQUIREMENTS

Subject Matter:
The subject matter of the processing is Personal Data as further described below.

Duration:
The duration of the processing is until the earlier of (i) request by Client to stop further processing; (ii) expiration/termination of the Agreement; or (iii) when processing is no longer necessary for purposes of DV performing its obligations pursuant to the Agreement.

Categories of Data Subjects:
The categories of Data Subjects whose Personal Data is processed include: end users who view ads analyzed by DV

Categories of Personal Data:
The categories of Personal Data processed include: IP address.

Sensitive Data:
The Agreement does not involve the processing of sensitive Personal Data.

Frequency of Transfers:
No transfers of Personal Data from Client to DV are contemplated as part of the Agreement. DV collects information directly through its technology. The processing is ongoing for the duration of the Agreement.

Nature of Processing:
The nature of the processing is the Services as described in the Agreement.

Purpose:
The purpose of the processing is for DV to provide geo measurement Services to Client as set out in the Agreement.

Retention:
Personal Data will be retained for the duration of the processing (as described above) and securely purged on a 45-day rolling basis.

Sub-processors:
Any transfer of Personal Data from DV to Sub-processors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Sub-processors are as described above.

ANNEX C
SUB-PROCESSORS

Due to the nature of the services, not all the below listed sub-processors would be involved in the processing of every impression. The specific combination of sub-processors depends upon the specific interaction being analyzed (i.e. the location of the end user). For the avoidance of doubt, updates to this list will be carried out in accordance with the terms of the DPA but shall not require an amendment of this Annex C.

Company Name	Location of Processing	Scope of Processing	Registered Address
Amazon Web Services, Inc.*	USA (primary) Global† (Location varies based on the location of the End User**)	Cloud infrastructure	410 Terry Avenue North, Seattle, WA 98109, USA
Akamai Technologies, Inc.*	Global†† (Location varies based on the location of the End User**)	Cloud infrastructure	145 Broadway, Cambridge, MA 02142, USA
Cloudflare	Global††† (Location varies based on the location of the End User**)	Cloud infrastructure	101 Townsend Street San Francisco, CA 94107, USA
Databricks, Inc.*	USA	Cloud Infrastructure and analytics	160 Spear Street, 13th Fl. San Francisco, CA 94105, USA
DreamHost*	USA	Cloud infrastructure	417 Associated Road PMB, Suite 257 Brea, CA 92821, USA
Equinix	Germany, Singapore	Co-Location Data center	One Lagoon Drive Fourth Floor Foster City, CA 94065, USA
Google LLC (Google Cloud)*	USA (primary) Global†††† (Location varies based on the location of the End User**)	Cloud infrastructure	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
GoodData Corporation	USA	Analytics provider, services embedded in DV products.	111 Sutter Street, San Francisco, CA 94104, USA
Internap	USA	Co-Location Data center	12120 Sunset Hills Road, Suite 330 Reston, VA 20190, USA
Looker Data Sciences, Inc.*	USA	Cloud Infrastructure	101 Church Street Santa Cruz, US-California 95060 United States
Snowflake Inc.*	USA	Cloud Infrastructure	450 Concar Drive San Mateo, CA 94402 United States
Telehouse America	USA	Co-Location Data center	7 Teleport Drive Staten Island, NY 10311, USA

**These sub-processors transmit and/store PII in its encrypted form and have no basis or independent right to access the PII as part of the services provided to DV.*

***These sub-processors maintain distributed network of processing locations based on the end user interaction tracked by the DV products, and focused on ensuring efficiency, resiliency and redundancy.*

†Amazon Web Services Network: https://aws.amazon.com/about-aws/global-infrastructure/

††Counties in which Akamai maintains Server Points of Presence: https://www.akamai.com/us/en/multimedia/documents/akamai/points-of-presence-countries.pdf

†††Cloudflare Global Anycast Network: https://www.cloudflare.com/network/

††††Google Cloud Network: https://cloud.google.com/about/locations

ANNEX D
DOUBLEVERIFY SECURITY EXHIBIT

1. Scope; Definitions. To the extent DV, in the operation of its Products, collects, processes or otherwise handles Personally Identifiable Information, DV shall comply with the requirements set forth in this Data Security Exhibit (the "Exhibit"). For the avoidance of doubt, it is the intent of the Parties that this Exhibit and its obligations apply to DV in its capacity as Processor and as Controller. In the event of a conflict or inconsistency between any provision of this Exhibit and the Agreement, this Exhibit shall control with respect to the subject matter of this Exhibit. Capitalized terms used in this Exhibit shall have the meaning

outlined herein. Terms that are capitalized but not defined herein shall have the meaning assigned to them in the Agreement.

a. "Agreement" shall mean the agreement between Client and DV to which this Exhibit is attached.
b. "DV Personnel" shall mean each directly, officer, manager, employee, representative and each natural person employed by DV.
c. "Documentation" shall mean any DV information security policies and procedures, certifications, reports, audits, white paper and similar instruments leveraged for the memorialization of DV's information security program.
d. "Personally Identifiable Information" or "PII" shall mean information that either (i) directly identifies an individual, (ii) can be used to identify an individual, or (iii) is considered Personally Identifiable Information by applicable laws, rules or regulations, including industry self-regulation, and by way of example, the General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act ("CCPA"), and is associated with the Products provided to Client.
e. "Products" shall mean the tools and offering made available by DV to Client.
f. "Security Incident" shall mean any confirmed unauthorized access, disclosure, misappropriation, theft, loss, acquisition or misuse of PII.
g. "Systems" shall mean hardware, software, networks, network components, applications and other equipment that comprise a technical environment.

2. General. DV shall maintain a comprehensive information security program, inclusive of all reasonable security measures appropriate to the nature of the PII processed by DV, including, without limitation, electronic, physical, administrative and organizational controls as applicable from time to time and further described in the applicable Documentation.

3. Training. DV shall maintain a comprehensive data security and privacy training program for DV Personnel. The training program is designed to meet the objectives and requirements of this Exhibit. The training program shall be updated from time to time to ensure alignment with best practices and applicable laws.

4. Background Checks. DV shall, to the extent permitted by applicable laws, conduct standard background checks, proportional to the nature of the business DV operates, prior to onboarding new DV Personnel.

5. Access to PII. DV access, by any means and methods, to PII ("Access") is solely for the purpose and will be limited only to the extent necessary for the provision of the Products. DV shall implement controls to ensure Access by DV Personnel is limited to a need-to-know basis. DV shall comply with and ensure DV Personnel comply with such protocols. Without limiting the foregoing, DV shall implement the following Access controls:
    a. Account credentials (such as IDs and passwords) must not be shared among Provider Personnel and must not use generic or default IDs or passwords.
    b. DV shall conduct user Access reviews at least semi-annually.
    c. DV shall, at all times, maintain the logical separation of electronic records of PII from (i) PII associated with other Clients, (ii) DV's PII, and (iii) DV Systems processing, storing, hosting, transporting and/or transmitting such other PII.
    d. DV Systems supporting its Products are protected by a network perimeter that restricts and controls access to permitted network traffic.
    e. If any DV Personnel resigns from employment with DV, is terminated by DV, or ceases to perform work requiring Access, DV shall promptly (i) terminate such individual's Access (including by removing system access, shutting down badge and key cards and retrieving secure fobs and the like), (ii) retrieve any corporate assets assigned to the individual, and (iii) ensure that such individual does not retain any PII in any format.

6. Restrictions on Access. DV and DV Personnel shall not Access PII in applications, reports, data transmissions or other outputs unless required by the operation of the Product and to fulfill DV's obligations under the Agreement, except as may be required by applicable laws or to meet a regulatory requirement. DV and DV Personnel shall not include PII in unencrypted emails or files attached to emails that are transmitted unprotected over the Internet.

7. Separation of Duties. DV shall enforce applicable separation of duties policies to ensure that credentials to grant access to PII on DV Systems do not overlap with DV Personnel requesting access.

8. Authentication. DV shall protect authentication credentials, including by: (i) ensuring that passwords and PINs do not appear in readable form while is typing the password or PIN; and (ii) ensuring passwords and PINs are stored in one-way hashed format, protected with salt. DV shall prevent DV Personnel from elevating their own privileges within a System without first re-authenticating as a more privileged user. Where technologically and commercially feasible, DV shall ensure passwords contains at least either (8)

alpha-numeric characters and at least three (3) of the following criteria: (w) upper case letters, (x) lower case letter, (y) numbers, and (z) special characters.

9. Asset Management. DV shall identify and classify corporate assets. Corporate assets shall be tracked through their lifecycle for vulnerabilities and risks.

10. Retired or Reassigned Equipment. Any corporate assets, including DV portable devices and removable media, that DV has retired shall be wiped or magnetically wiped pursuant to applicable US Department of Defense standards within two (2) weeks of the retirement. Reassigned corporate assets shall be wiped immediately prior to reassignment.

11. Logical Access Security Log. DV shall create, maintain and monitor electronic access security logs for the Provider Systems used to make available the Products or from which DV Personnel gains Access to PII.

12. Changes Log. To the extent such changes relate to the Products, DV shall create and maintain an electronic log of all changes to the technical and logical architecture of DV Systems used to process PII, the physical and electronic access control systems and the logical and physical security standards. DV's change control procedures shall protect the confidentiality, integrity and availability of PII.

13. Encryption. Any encryption applied to PII shall be in accordance with the Advanced Encryption Standards (AES), or any successor standard, and shall be no less than 128-bit. Encryption keys shall be made available to DV Personnel on a need-to-know basis. Compromised keys shall be immediately revoked or disabled.

14. Vulnerability Management. DV shall scan and monitor its network and perimeter on a fortnightly basis to identify potential vulnerabilities. Penetration testing shall be conducted on an annual basis. Any identified vulnerabilities or gaps identified by the scan shall be classified by level of significance and addressed in accordance to the level of criticality.

15. Configuration and Patch Management. DV shall establish standardized security configurations for each computing platform and applied to DV Systems. DV shall ensure timely implementation of essential and necessary security patches and configuration changes. To the extent anti-virus or anti-malware software is used, it shall be configured to the latest virus definition update and shall include technical controls that provide for automatic updates of the virus definition.

16. Back-Ups and Redundancies. DV shall ensure the provision of redundancies and procedures to maintain the continuity of service for its Products. DV shall utilize a defined back-up procedure for any data necessary to ensure continuation of service. service continuation. The back-up procedure shall include the provision of back-ups on a periodic basis (no less frequent than monthly). Back-ups shall be promptly stored at offsite facilities and in accordance with the requirements of this Exhibit.

17. Data Retention and Destruction. DV shall maintain effective data retention and destruction policies and procedures to ensure records containing PII are disposed of in a timely manner that does not compromise the security, confidentiality or integrity of the information.

18. Business Continuity and Disaster Recovery. DV shall create, maintain and review detailed business continuity and disaster recovery plans. The plans shall identify the teams tasked with the management of the applicable contingency plan to ensure continuation of business operations.

19. Security Incidents. DV will be responsible for detecting, investigating and responding to potential compromises on DV Systems, or potentially impacting Access or performance of the Products. Upon confirmation that a Security Incident has occurred, DV shall report such Security Incident without undue delay, by providing a written notification to the Client's day to day contacts. In the event of a Security Incident: (a) DV shall investigate, mitigate and implement any additional controls necessary to prevent re-occurrences, (b) DV shall cooperate with Client to comply with any legal requirements, including, as applicable, with respect to the notification of individuals and regulatory agencies, provided that, unless required by law, in no event shall DV serve any notice or otherwise publicize a Security Incident without the prior consent of the Client to be provided in writing, and (c) upon Client's request and at Client's expense, DV shall engage a regionally recognized independent third party to perform or assist with a forensic review of DV's initial analysis of the Security Incident. Upon request, DV shall deliver the result of the DV's review of the Security Incident, as well as the results of any third-party review conducted on the analysis, which shall be deemed Confidential Information of DV.

20. Miscellaneous. DV shall have no obligation to proactively notify Client of any changes made to its Systems architecture, information security program or its Documentation, provided that such changes shall not reduce the protections agreed upon in this Exhibit.