DATA PRIVACY ADDENDUM

This Data Privacy Addendum (this "**DPA**") is supplemental to the agreed upon terms, whether in the form of a Main Services Agreement, trial agreement, end user license agreement or similar legal instrument which, for purposes of this DPA, shall be referred to as the "**Agreement**", entered into by the Client and DoubleVerify Inc., on behalf of itself, its affiliates and subsidiaries (hereinafter "**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) "**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.

(c) "**Client**" means a party leveraging the DV Solutions in accordance with the Agreement.

(d) "**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.

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

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

(g) "**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). References to the GDPR shall be construed to refer equally to the retained UK GDPR under the Data Protection Act 2018, as may be updated in the future.

(h) "**Personal Data**" means any information relating to an identified or identifiable natural person, or, as applicable, a household.

(i) "**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.

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

(k) "**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.

(l) "**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.

(m) "**Solutions**" shall mean the suite of products and/or services provided or made available by DV to Client.

(n) "**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 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 Solutions (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 Solutions, the terms set out in this Section 3 shall apply. Further, Sections 5, 6, 7, 9, 10, 11, 12 and 13 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 Solutions, to fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Solutions 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 Solutions, the terms set out in this Section 4 shall apply. Further, Sections 5, 6, 7, 9, 10, 11, 12 and 13 of this DPA shall be deemed applicable, as detailed therein, to DV in its capacity as a Processor.

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 Solutions to Client, fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Solutions such as billing, account management, technical maintenance and support, product maintenance and improvement.

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 Solutions 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 Solutions, 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 Personal Data or to any of DV's equipment or facilities storing Customer 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. 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 8.1 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 Solutions in accordance with the termination provisions of the Agreement. In the event that Client suspends or terminates the Solutions 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. To the extent such audits are conducted, the parties further acknowledge that these audits:

(a) are performed at least once each year;

(b) are conducted by auditors selected by DV, but otherwise conducted with all due and necessary independence and professionalism; and

(c) are 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 to the extent available at the time of the request, DV will (on a confidential basis) provide Client with a summary of the 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 the Report and written responses provided under Section 10.2 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 Solutions, 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. Liability

Liability Terms. Any exclusions or limitations of liability that may have been negotiated in the Agreement shall apply to this DPA.

13. Miscellaneous

13.1 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.

13.2 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.

13.3 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 determination is 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 may 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.

In relation to transfers of Personal Data processed in accordance with Section 3 of this DPA, to the extent applicable, the Standard Contractual Clauses are completed as follows:
To the extent both parties act as Controllers, Module One may apply.

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 D**.
- Competent Supervisory Authority: The data exporter's competent supervisory authority will be determined in accordance with EU Data Protection Legislation.

Annex II is completed as follows:
The required information is set out in **ANNEX E**. Please note the applicable list depends on the scope of Solutions provided.

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

ANNEX B
UK International Data Transfer Addendum to the EU Standard Contractual Clauses[1]

In relation to transfers of Personal Data originating in the UK and processed in accordance with Section 4 of this DPA, to the extent applicable, this UK International Data Transfer Addendum is completed as follows:

PART 1: TABLES

Table 1: Parties

Start date	The start of the processing of Personal Data under the terms of the Agreement by DoubleVerify.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Client	DV
Key Contact	Client main contact as defined by the Client	Privacy-policy@doubleverify.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ **The version(s) of the Approved EU SCCs which this UK Addendum is appended to, including the Appendix Information detailed below.**

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties: Please refer to the **DPA**.
Annex 1B: Description of Transfer: Please refer to **Annex D**.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please refer to **Annex F**.
Annex III: List of Sub processors (if applicable): Please refer to **Annex E**.

Table 4: Ending this UK Addendum when the Approved Addendum Changes

Ending this UK Addendum when the Approved Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

[1] Version B1.0, in force 21 March 2022. This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 2: MANDATORY CLAUSES

Entering into this UK Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
2. Although Annex 1.A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this UK Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words:
    "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
    c. Clause 6 (Description of the transfer(s)) is replaced with:
    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
    d. Clause 8.7(i) of Module 1 is replaced with:
    "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
    "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the UK Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the UK Addendum; and/or

    b. its risk under the UK Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

ANNEX C

Swiss Addendum to the EU Standard Contractual Clauses

For transfers of Personal Data originating in Switzerland, the EU Standard Contractual Clauses shall be amended in accordance with statement of the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") of 27 August 2021.[2] In particular:

A. The FDPIC shall be the competent supervisory authority insofar as the transfer is governed by the Swiss Federal Act on Data Protection ("**FADP**") (Clause 13);
B. The law of the country specified in the EU Standard Contractual Clauses shall be the governing law (Clause 17);
C. The courts of the country specified in the EU Standard Contractual Clauses shall be the choice of forum (Clause 18), but this shall not exclude data subjects in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c); and
D. The EU Standard Contractual Clauses shall protect the data of legal entities in Switzerland until the entry into force of the revised FADP.

[2] Available for direct download at: https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf.

ANNEX D
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: Pseudonymous information insufficient on its own to identify an individual (e.g., 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 Solutions as described in the Agreement.

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

Retention:
Personal Data will be processed and retained for the duration of the Agreement (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 E
DOUBLEVERIFY SUB-PROCESSORS

Due to the nature of the Solutions, 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). Please note the applicable Sub-processors vary depending on the nature and scope of the Solutions provided (e.g. advertiser or publisher Solutions).

ADVERTISER SOLUTIONS

Company Name	Location of Processing	Scope of Processing	Registered Address
Amazon Web Services, Inc.*	USA Australia Brazil Canada Germany India Ireland Japan Singapore South Korea UK (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
Digital Ocean, LLC*	USA Canada Germany India Singapore UK (Location varies based on the location of the End User**)	Cloud Infrastructure	101 6th Ave, New York, NY 10013, 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

Metamarkets Group, Inc.	USA	Analytics provider, services embedded in DV products.	300 Brannan Street Suite 510 San Francisco, CA 94107, USA
StackPath* (Formerly MaxCDN)	USA Australia Belgium Brazil Canada China France Germany Italy Japan Philippines Poland Singapore South Korea Sweden The Netherlands UK (Location varies based on the location of the End User**)	Cloud Infrastructure	2021 McKinney Avenue Suite 1100 Dallas, TX 75201, USA
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 Personal Data in its encrypted form and have no basis or independent right to access the Personal Data 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.*

[†]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/

PUBLISHER SOLUTIONS

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 Personal Data in its encrypted form and have no basis or independent right to access the Personal Data 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 F
DOUBLEVERIFY SECURITY EXHIBIT

DV will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risks. Such measures will include reasonable administrative, physical, and technical security controls (including those required by applicable Data Protection Laws) that prevent the collection, use, disclosure, or access to Personal Data, including maintaining a comprehensive information security program that safeguards Personal Data.

Such Security Measures will include: (a) strict logical or physical separation between (i) Personal Data (ii) DV data and data of other clients; (b) implementation and maintenance of administrative, physical or technical controls proportional to the nature and sensitivity of the Personal Data processed by DV, including, by way of example, encryption; (c) maintaining industry standard perimeter protection for DV's network and devices connected thereto; (d) applying, as soon as practicable, patches or other controls to relevant systems that effectively address actual or potential security vulnerabilities; (e) employing commercially reasonable efforts to ensure that relevant systems remains free of security vulnerabilities, viruses, malware, and other harmful code; (f) employing commercially reasonable efforts to practice safe coding standard and practices which address application security vulnerabilities; (g) providing appropriate education and training to DV personnel regarding these Security Measures and ensuring that those individuals are bound by confidentiality obligations; (h) accessing or transferring Personal Data only in a secure and confidential manner; and (i) limiting Supplier employee/agent/subcontractor access to DV's network, Systems, devices and facilities to those with a need for such access, and whose access privileges is revoked promptly upon their termination.