

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 and its current direct and indirect 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.

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.
 - (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 by way of example and as applicable from time to time, the General Data Protection Regulation EU 2016/679 ("**GDPR**") or the California Consumer Privacy Act (California Civil Code §§ 1798.80, et seq.), as amended by the California Privacy Rights Act of 2020 ("**CCPA**"), and any other provincial or state privacy laws that may take effect during the term of the Agreement.
 - (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 ("**EU**") together with Iceland, Norway, and Liechtenstein.
 - (h) "**Personal Data**" means any information relating to an identified or identifiable natural person, or, as applicable, a household. The definition of Personal Data herein includes "pseudonymous information" as defined by the GDPR.
 - (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. As used herein, Processor will include, as applicable, the term "contractor" under the CCPA.
 - (k) "**Prohibited Data**" means Personal Data that the Client is prohibited to submit to DV under this Agreement, including (a) Sensitive Data; (b) Personal Data of children under the age of 13, or the applicable age of consent under relevant Data Protection Laws; (c) Personal Data from geographies that have been deemed as embargoed by the U.S. Department of the Treasury or that DV has expressly designated in writing to Client as geographies where it cannot lawfully operate; and (d) any other data that the Client may not share with DV in a lawful manner.
 - (l) "**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.
 - (m) "**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 Data Protection Laws.
 - (n) "**Solutions**" shall mean the suite of products and/or services provided or made available by DV to Client.
 - (o) "**Standard Contractual Clauses**" or "**SCCs**" means (a) 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 handling of Personal Data. Notwithstanding the foregoing, any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations of liability, 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 use of the Solutions.
- 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 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. Notwithstanding the foregoing, with respect to the CCPA, DV operates all Solutions as a "contractor". 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 applicable 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.
- 2.4 **Business Relationship.** The Parties acknowledge that each Party acts as an independent Controller for any Personal Data Processed or exchanged under this Agreement and during the business relationship between the Parties. Each Party is solely responsible for compliance with applicable Data Protection Laws for the Personal Data it Processes.
- 2.5 **Ongoing Compliance.** DV shall promptly notify Client in the event it becomes unable to meet the requirements imposed by this DPA or applicable Data Protection Laws. If DV is unable to remediate such non-compliance, Client shall have the right to terminate the portion of the Agreement affected.

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 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 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 (or, in limited circumstances, as a Subprocessor) 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, 8, 9, 10, 11 and 12 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. Without prejudice to DV's rights or obligations under this Section 4.2 or any other rights or obligations of either party under the Agreement or this DPA, DV will promptly notify Client if, in DV's reasonable opinion an instruction from Client does not comply or would prevent DV from complying with applicable Data Protection Laws, provided that such notification is not prohibited by applicable laws and that it shall not be deemed to constitute a legal opinion. 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's ongoing compliance with applicable 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, and maintaining any such records in accordance with Applicable Laws, and;
- (b) Client has, and will continue to have for the duration of the relationship, the right to engage DV to carry out the Processing activities outlined 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" or "share" as defined by the CCPA. The Parties further agree that, under no circumstance will DV be required to enrich any Personal Data 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 Prohibited Data to DV for Processing under the Agreement, and DV will have no liability whatsoever for such 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 Prohibited Data unless the Processing of such data is otherwise permitted by Data Protection Laws or Client has obtained DV's prior written consent.

5.3 DV Tags. To the extent DV tags are in scope, Client acknowledges that DV does control how or when the DV tags are applied to a campaign by Client (or its agents and representatives). Client therefore agrees it shall make good faith efforts to follow the Solutions guidelines provided by DV with respect to its usage of the Solutions. DV shall not be liable to Client for violations of this DPA or applicable Data Protection Laws caused by the Client's disregard of DV's Solutions guidelines (e.g., the placement of DV tags on inventory running in jurisdictions where DV is not legally able to operate, Client's disclosure to DV of Personal Data that was improperly collected or disclosed).

5.4 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 A** 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 6.4 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 UK or Switzerland, the Parties agree that an adequate transfer mechanism must 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 SCCs.
- 7.2 Transfer Mechanism. DV is a registered participant of the EU-US, UK-US and Swiss-US Data Privacy Framework ("DPF") and shall maintain such registration, supported via an external independent verification method (e.g., the *TRUSTe Data Privacy Framework Verification*), as long as the DPF remains a valid adequacy framework per Section 7.1 of this DPA. In the event that the DPF as an adequacy framework becomes invalid or is deemed inapplicable to a portion of DV's Solutions, and to the extent transfers of Personal Data occur between DV and the Client with respect to such portion of DV's Solutions, the Parties hereby agree that by signing this DPA, the most relevant and up to date version of the SCCs are deemed to have been executed in accordance with the terms of [DV's International Transfers Addendum](#), with Client in the capacity of Exporter and DV in the capacity of Importer.
- 7.3 DOJ Final Rule. The Parties understand that by virtue of the recently enacted Protecting Americans' Data from Foreign Adversaries Act of 2024 ("PADFA") and 28 C.F.R. Part 202 (the "DOJ Final Rule"), certain entities may be required to implement additional safeguard to ensure ongoing compliance with these regulations and ensure the protection of specific sensitive and other data related to "U.S. persons".
- 8. Subprocessing**
- 8.1 Subprocessors. Client agrees that this DPA constitutes Client's written authorization for DV, in its capacity as a Processor, to engage Affiliates and third-party Subprocessors (collectively, "Subprocessors") to Process the Personal Data on DV's behalf, including Subprocessors currently engaged by DV. Client agrees that this DPA constitutes Client's written authorization for DV and its Subprocessors to Process Personal Data, in accordance with the terms of this Section, anywhere in the world where DV or its Subprocessors maintain data Processing operations. DV will notify Client of any new Subprocessor being appointed by posting an updated list of Subprocessors in the applicable reporting portal. The lists of the then applicable Subprocessors, as may be relevant to each of DV's Solutions, are included in this DPA in Schedules in **Annex B**.
- 8.2 Objection to Subprocessors. Client may object in writing, stating Client's reasonable grounds for the objection, to the appointment of an additional Subprocessor 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 Subprocessor, 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 Subprocessor obligations. Where a Subprocessor is engaged by DV as described in this Section 6, DV shall:
- (a) enter into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor 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 Subprocessor other than in-house contractors, DV shall ensure that the Standard Contractual Clauses or any other lawful transfer mechanism is in place before the Subprocessor Processes any Personal Data; and,
 - (c) remain responsible for any breach of the DPA caused by a Subprocessor.
- 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, where Client instructs DV to fulfill a request that DV reasonably considered manifestly unfounded or excessive, Client shall be responsible for reasonable administrative costs arising from DV's provision of such assistance.
- 9.2 Data Protection Impact Assessments. DV shall, to the extent required by applicable Data Protection Law 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 is 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. 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.

Entire Agreement. This DPA embodies the entire agreement and understanding between the parties as it relates to the processing of Personal Data, and supersedes all prior agreements and understandings related to its subject matter. This DPA cannot be changed, modified or extended except by written amendment executed by an authorized representative of each Party.

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 determination is made in the Agreement, the applicable law and venue shall default to the location of DV's headquarters.

ANNEX A
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.

ANNEX B
SCHEDULE 1
ADVERTISER SOLUTIONS PROCESSING REQUIREMENTS

Subject Matter:

The subject matter of the processing is Personal Data as further described below and in the relevant Agreements and MSOs.

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:

End users who view ads analyzed through the DV Advertiser Solutions

Categories of Personal Data:

Online identifiers (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 DV Advertiser Solutions

Duration of the Processing:

Ongoing for the duration of the Agreement.

Nature of the Processing:

The nature of the processing is the provision, maintenance, security and ongoing support of the DV Advertiser Solutions

Purpose of the Processing:

The purpose of the processing is for DV to provide the relevant Solutions as set out in the applicable Agreement and in accordance with the Client's instructions.

Retention:

Personal Data will be processed and retained for the duration of the Agreement and securely purged on a 45-day rolling basis

Subprocessors:

Any transfer of Personal Data from DV to Subprocessors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Subprocessors are as described above. An up-to-date list of the Advertiser Suite Subprocessors is available at: <https://doubleverify.com/advertiser-subprocessors/>

SCHEDULE 2 PUBLISHER SOLUTIONS PROCESSING REQUIREMENTS

Subject Matter:

The subject matter of the processing is Personal Data as further described below and in the relevant Agreements and MSOs.

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:

End users who view ads analyzed through the DV Publisher Solutions

Categories of Personal Data:

Online identifiers (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 DV Publisher Solutions.

Duration of the Processing:

Ongoing for the duration of the Agreement.

Nature of the Processing:

The nature of the processing is the provision, maintenance, security and ongoing support of the DV Publisher Solutions.

Purpose of the Processing:

The purpose of the processing is for DV to provide the Publisher Solutions as set out in the applicable Agreement and in accordance with the Client's instructions.

Retention:

Personal Data will be processed and retained for the duration of the Agreement and securely purged on a 45-day rolling basis.

Subprocessors:

Any transfer of Personal Data from DV to Subprocessors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Subprocessors are as described above. An up-to-date list of the Publisher Suite Subprocessors is available at: <https://doubleverify.com/publisher-subprocessors/>

SCHEDULE 3 ROCKERBOX SOLUTIONS PROCESSING REQUIREMENTS

Subject Matter:

The subject matter of the processing is Personal Data as further described below and in the relevant Agreements and MSOs.

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:

Client's existing and potential consumers.

Categories of Personal Data:

Basic identifiers (e.g., name, email address, physical address)
Online identifiers (e.g., IP address, mobile IDs, customer IDs)
Ad interaction and event data (e.g., order IDs, individual coupon codes)
User generated information (e.g., survey responses)
Advertiser generated information (e.g., segments)

Sensitive Data:

Depending on the nature of the engagement and the instructions of the Client, Sensitive Data (e.g., health related information) may be in scope.

Frequency of Transfers:

Ongoing.

Duration of the Processing:

Ongoing for the duration of the Agreement.

Nature of Processing:

The nature of the processing is the provision, maintenance, security and ongoing support of the Rockerbox Solutions.

Purpose of the Processing:

The purpose of the processing is for DV to provide the Rockerbox Solutions as set out in the applicable Agreement and in accordance with the Client's instructions.

Retention:

Personal Data will be processed and retained for the duration of the Agreement and securely purged thereafter in accordance with the Client's instructions.

Subprocessors:

Any transfer of Personal Data from DV to Subprocessors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Subprocessors are as described above. An up-to-date list of the Rockerbox Subprocessors is available to current Client upon request.

SCHEEDULE 4 SCIBIDS AI™ PROCESSING REQUIREMENTS

Subject Matter:

The subject matter of the processing is Personal Data as further described below and in the relevant Agreements and MSOs.

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:

End users from Client's website

Categories of Personal Data:

Online identifiers (e.g., IP address, Device IDs)
Ad interaction and event data (e.g., conversion information)

Sensitive Data:

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

Frequency of Transfers:

Ongoing.

Duration of the Processing:

Ongoing for the duration of the Agreement.

Nature of Processing:

The nature of the processing is the provision, maintenance, security and ongoing support of the Scibids AI™ Solutions.

Purpose of the Processing:

The purpose of the processing is for DV to provide the Scibids AI™ Solutions as set out in the applicable Agreement and in accordance with the Client's instructions.

Retention:

Personal Data will be processed and retained for the duration of the Agreement and, as applicable, securely purged on a 45-day rolling basis.

Subprocessors:

Any transfer of Personal Data from DV to Subprocessors will be in accordance with the obligations set out in the DPA. The subject matter, nature, and duration of the processing by Subprocessors are as described above. An up-to-date list of the Scibids AI™ Subprocessors is available at: <https://doubleverify.com/scibids-subprocessors/>