

ID5 ID Agreement
IMPORTANT – PLEASE READ CAREFULLY

v1.2 December 2025

“Company”:

Full Legal Entity Name:		
Legal Address:		
Country:		
Company Contact Information		
	<u>Name/Title</u>	<u>Email Address</u>
Legal Notices		
Operational Contact		
Privacy Contact		

These terms of service and the accompanying DPA(s) annexed hereto (collectively, the “**ID5 ID Agreement**”) is entered into as of the date of the last signature below (“**Effective Date**”) by and between ID5 Technology Limited (“ID5”) and the Company identified above (“**Company**”). ID5 and Company may be referred to herein together as the “**Parties**” or individually as a “**Party**”. For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, ID5 and Company hereby agree as follows:

- 1) **Introduction.**
 - a) **Definitions.** Defined terms as used in this ID5 ID Agreement are provided below and in **Exhibit A** (Definitions).
 - b) **Interpretation.** For the purposes of this ID5 ID Agreement, (a) the words “include,” “includes,” “including,” and similar terms are deemed to be followed by the words “without limitation”; (b) unless the context otherwise requires, words in the singular include the plural and in the plural include the singular; (c) headings in this ID5 ID Agreement are only for reference and will not affect the interpretation of this ID5 ID Agreement; and (d) references to a statute, regulation, directive, or other legally binding rule (each, a “**Law**”) means such Law as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder.
 - c) **ID5 ID Service Free of Charge.** ID5 provides the ID5 ID Service free of charge subject to the terms and conditions hereof, including its warranties, indemnities, and limitations of liability.
 - d) **Service Limitations.** The no-cost ID5 ID Service hereunder is limited to the delivery of an encrypted ID5 ID. Additional ID5 services, including the ability to decrypt encrypted ID5 IDs, information on the connections between ID5 IDs, or use of the ID5 Data, are available for purchase by emailing contact@id5.io.
- 2) **ID5 ID Service; Rights; Related Parties.**
 - a) **ID5 ID Service.**
 - i) Subject to the terms and conditions of this ID5 ID Agreement, when a Visitor accesses any of the Digital Properties, ID5 will process Personal Data for the Permitted Purpose, including for the purpose of returning a Visitor’s ID5 ID and/or other User IDs to Company or its Related Party (as applicable) in real time through the ID5 ID Service.
 - ii) To activate the ID5 ID Service, Company and its Related Parties must incorporate its/their assigned ID5 Partner Number into each instance of the ID5 Software and ID5 OSS which the applicable party integrates on its Digital Properties in accordance with the ID5 ID Requirements.
 - iii) Company or its Related Parties may enable ID5 Identity Insights, ID5’s proprietary analytics adapter for prebid, at any time.
 - b) **Rights.**
 - i) **Rights granted by ID5.**

- (1) Subject to the terms and conditions of this ID5 ID Agreement, ID5 hereby grants Company a non-exclusive, revocable, worldwide, non-transferable and non-sublicensable right and license during the Term to: (i) integrate and use the ID5 Software on Digital Properties solely to enable the ID5 ID Service; and (ii) to receive and utilize the specific encrypted instance of each ID5 ID in accordance with Applicable Privacy Law. The ID5 OSS is not licensed under this ID5 ID Agreement and is instead provided under the terms of its applicable open-source license, and Company shall comply with such terms of use when utilizing ID5 OSS.
- (2) Company may permit its Related Parties to use the ID5 ID Service, including integrating the ID5 Software, solely for the Permitted Purpose in connection with such Related Parties' activities related to Digital Properties, *provided that* Company is directly liable for any act or omission of any Related Party in violation of this ID5 ID Agreement as if it were committed by Company. Notwithstanding the foregoing, Company shall not be directly liable for any Related Party which has executed a ID5 ID Agreement directly with ID5 for such party's use of the ID5 ID Service.

ii) **Rights granted by Company.** Subject to the terms and conditions of this ID5 ID Agreement, Company hereby grants, and is authorized to grant, a non-exclusive, worldwide, royalty-free license during the Term to ID5 to access, use, process, and store the Company Signals and Collected Signals from each Digital Property for ID5 to provide the ID5 ID Service and fulfill the Permitted Purpose, including the generation of ID5 Data as further described herein. ID5 may sublicense the foregoing rights to its Affiliates and subcontractors as necessary to assist ID5 in the performance of its obligations.

- 3) **Proprietary Rights.**
 - a) **Intellectual Property.**
 - i) As between the Parties, Company owns all right, title and interest in and to its intellectual property, including the raw Company Signals provided to ID5 hereunder.
 - ii) As between the Parties, ID5 owns and will retain all right, title and interest in and to its ID5 Intellectual Property. Notwithstanding anything to the contrary in this ID5 ID Agreement, Company acknowledges and agrees that ID5 exclusively owns all right, title, and interest in and to any and all ID5 Data. Company acknowledges that ID5 Data results from the application of ID5's proprietary algorithms to a vast dataset aggregated from thousands of independent sources, and as such, constitutes a new and distinct asset wholly owned by ID5. ID5 Data shall not be considered the property of Company or a derivative work of Company's intellectual property or Company Signals.
 - iii) Each Party reserves any and all rights not expressly granted in this ID5 ID Agreement and disclaims all implied licenses.
 - b) **Feedback.** If Company provides any Feedback to ID5:
 - i) In its sole discretion, ID5 will determine whether to proceed with the development of any enhancements, features and/or functionality, in whole or in part; and
 - ii) Company hereby grants ID5 a royalty-free, fully paid-up, irrevocable, perpetual, worldwide license to use such Feedback for any lawful purpose, including, without limitation, the development and/or improvement of features and/or functionality for the ID5 ID Service and/or any other ID5 products and/or services; provided that ID5 will not publicly disclose any of the Feedback in such a way as to identify or that would reasonably be expected to identify Company as the source of such Feedback.
 - c) **Publicity; Press Releases.** Without the other Party's prior written consent, neither Party shall use the other Party's name or logo to (a) issue public announcements or marketing communications referencing the other Party; or (b) issue case studies, testimonials, or press releases. Notwithstanding the foregoing, each Party grants the other Party a limited, non-exclusive, revocable right to use the other Party's name and logo in client or vendor lists, subject to any brand guidelines and any reasonable written restrictions of such Party.
 - 4) **Representations and Warranties.** Each Party represents and warrants to the other Party that: (a) it has the full right, power, and authority to enter into this ID5 ID Agreement and to convey the rights and perform its obligations hereunder; (b) its execution and performance of this ID5 ID Agreement does not and will not violate any other agreement to which it is a party or by which it is otherwise bound; and (c) it will comply with all Applicable Laws to the extent applicable to its performance of its respective obligations and exercise of its respective rights under this ID5 ID Agreement, *except* to the extent non-compliance arises from the action or inaction of the other Party (including such other Party's Affiliates and Related Parties).
 - 5) **Security**
 - a) **Information Security Standard.** Each Party agrees that it will use commercially reasonable efforts to maintain administrative, technical, and physical safeguards that are no less rigorous than industry standard practices and the requirements of Applicable Privacy Law to ensure the security and confidentiality of Personal Data, protect against any anticipated threats

or hazards to the confidentiality, availability, or integrity of Personal Data, and protect against unauthorized access, use, or alteration of Personal Data.

- b) **Written Information Security Program.** Throughout the Term, each Party shall maintain, in writing, reasonable security procedures and practices necessary to protect Personal Data within its control from unauthorized access, destruction, use, modification, or disclosure.
- c) **Unauthorized Access.**
 - i) Throughout the Term, without limiting any of its obligations under this ID5 ID Agreement, Company will use commercially reasonable efforts to prevent unauthorized access to or use of the ID5 ID Service.
 - ii) Each Party shall promptly notify the other Party in writing upon becoming aware of any security incident or breach that materially impacts or compromises: (i) the security, integrity, or operation of the ID5 ID Service on the Digital Properties; or (ii) the confidentiality, integrity, or security of Collected Signals or Company Signals transmitted, or intended to be transmitted, to ID5 from Digital Properties.

6) Obligations and Restrictions

a) Company Obligations.

- i) For each Digital Property, Company or the applicable Related Party owns, operates, or controls the property, or has otherwise obtained and will maintain all necessary rights, permissions, licenses, and consents required to perform its obligations in compliance with Applicable Law and this ID5 ID Agreement.
- ii) Company is solely responsible for implementing and maintaining reasonable security measures to safeguard its assigned ID5 Partner Number(s). Company shall not, and shall ensure its Related Parties do not, publish, share, or otherwise disclose its ID5 Partner Number(s) in any manner that would facilitate its unauthorized use by a third party. For the purposes of this Agreement, any and all use of the ID5 ID Service associated with Company's assigned ID5 Partner Number(s) shall be deemed to be use by Company, and Company shall be fully liable for all such use in accordance with Section 2(b) and Section 11.
- iii) Throughout the Term, without limiting any of its obligations under this ID5 ID Agreement, Company (on behalf of itself and its Related Parties) is solely and directly responsible for:
 - (1) all implementation and use of the ID5 ID Service hereunder (including all use of the ID5 IDs) on all Digital Properties;
 - (2) compliance with the ID5 ID Requirements;
 - (3) performance of all obligations hereunder in accordance with good industry practice and without gross negligence or willful misconduct; and
 - (4) ensuring that:
 - (a) each Digital Property displays a clear, comprehensive, and accurate privacy notice regarding the collection, Processing, use, and sharing of Collected Signals and Company Signals for the Permitted Purpose(s) as contemplated by this ID5 ID Agreement which is sufficient to meet the requirements of all Applicable Privacy Law;
 - (b) all Visitor Choices required under Applicable Law are offered to Visitors in a prominent and easily accessible manner;
 - (c) Visitor Choice Signals are collected, recorded, and respected as required under Applicable Law;
 - (d) Visitor Choice Signals are accurately, completely, and promptly transmitted to ID5 via the ID5 ID Service in accordance with the ID5 ID Requirements.
- iv) **Industry Frameworks.** To the extent Company or its Related Parties utilize recognized industry-standard privacy compliance frameworks (such as the IAB TCF or GPP) to transmit Visitor Choice Signals to ID5, Company warrants that it will implement and adhere to the applicable policies and technical specifications of such frameworks. Company further warrants that it will accurately configure such frameworks on the Digital Properties to reflect the Permitted Purpose and ID5's status as an independent controller or equivalent under Applicable Privacy Law.

b) ID5 Obligations.

- i) **Privacy Policy.** Throughout the Term, the ID5 website will prominently display the ID5 Privacy Policy.
- ii) **Data Retention.** ID5 shall retain Company Signals and Collected Signals for no longer than one hundred days, except to the extent reasonably necessary for internal logs, security, and compliance with Applicable Law.
- iii) **Permitted Purpose.** Throughout the Term, ID5 will Process the Company Signals and Collected Signals hereunder in compliance with the Permitted Purpose, ID5 Privacy Policy, and Visitor Choice Signals.
- c) **Company Restrictions.** Without limiting any of Company's obligations under this ID5 ID Agreement, Company will not, and will not assist or knowingly permit any Related Party or third party to:

- i) Use the ID5 ID Service for any fraudulent purpose or otherwise in violation of any Applicable Law, or outside the Permitted Purpose;
- ii) Copy, reproduce, modify, translate, host, sublicense, lease, transfer, resell, disassemble, decompile, reverse engineer, or create derivative works from the ID5 ID Service, ID5 Platform, ID5 Software, the ID5 IDs, or any aspect thereof;
- iii) Send or provide to ID5, including via the ID5 ID Service, any material that is or is intended to be technically harmful (including viruses, worms, Trojan horses, logic bombs, or other malicious code or features);
- iv) Damage, impair, disable, breach, tamper with, misappropriate, circumvent, or interfere with any security measure, access or use restrictions, or any other aspect of the ID5 ID Service;
- v) Provide to ID5 any Directly Identifiable Data or Sensitive Data;
- vi) Use the ID5 ID Service on any Digital Property, or portion thereof, that is directed to users or Visitors below the Restricted Age or knowingly collect or transmit Personal Data (including Collected Signals or Company Signals) to ID5 from users or Visitors reasonably known by Company to be under the Restricted Age; or
- vii) Use the ID5 ID Service or ID5 IDs:
 - (1) to make, or assist in making, a decision about a Visitor's eligibility for employment, health care, credit or insurance; or
 - (2) to make, or assist in making, a decision by automatic means that produces legal effects concerning, or has a similarly significant effect on, the Visitor; or
 - (3) in combination with any other data where such combination would constitute Sensitive Data or is otherwise prohibited by any Applicable Law, including precise location data.

7) Confidentiality.

- a) The receiving Party shall (i) maintain the confidentiality of the disclosing Party's Confidential Information using at least the same degree of care it uses to protect its own confidential information, but no less than a reasonable degree of care, (ii) not disclose such information to any third party without the disclosing Party's prior written consent, and (iii) use such information solely for the purpose of performing its obligations and exercising its rights under this ID5 ID Agreement.
- b) ID5's obligations with respect to Company Signals (including but not limited to confidentiality obligations therewith) are governed by Section 8 of this ID5 ID Agreement, Applicable Privacy Laws, and all data processing agreements executed between the Parties (including but not limited to Exhibit X and Exhibit Y hereto, as applicable) and, therefore, Company Signals is expressly excluded from Confidential Information.

8) Data Protection; Privacy.

- a) **Data Processing Addenda.**
 - i) The Parties shall comply with the terms of the Data Processing Addenda attached to this ID5 ID Agreement as Exhibit X and Exhibit Y (each a "DPA", collectively the "DPAs"), which are incorporated herein by reference and govern the Processing of Personal Data under this ID5 ID Agreement. In the DPAs, "Prime Agreement" means this ID5 ID Agreement. The specific DPA applicable to a Processing activity depends on the nature of the Applicable Privacy Law governing such activity:
 - (1) **Opt-In Jurisdictions.**
 - (a) Where Opt-In Applicable Privacy Laws apply, the terms of Exhibit X, the Opt-In Jurisdiction Data Processing Agreement, shall apply subject to Section 8(b). As of the Effective Date, Opt-In Applicable Privacy Laws include, without limitation, Applicable European Data Protection Law such as GDPR and UK GDPR.
 - (b) The Parties acknowledge and agree that to the extent Opt-In Applicable Privacy Laws apply, each Party acts as an independent controller or similar term under Applicable Privacy Laws with respect to its respective Processing of Personal Data. As such, Company is solely responsible for ensuring that it has secured any legally required rights, consents, or permissions (including those from its Visitors/data subjects) necessary to enable ID5 to Process Personal Data for the Permitted Purpose in accordance with this ID5 ID Agreement and the ID5 Privacy Policy.
 - (2) **Opt-Out Jurisdictions.** Where Opt-Out Applicable Privacy Laws apply, the terms of Exhibit Y, the Opt-Out Jurisdiction Data Processing Agreement, shall apply subject to Section 8(b). As of the Effective Date, Opt-Out Applicable Privacy Laws include, without limitation, certain Applicable U.S. Privacy Laws.
 - ii) The Parties agree that the applicable DPA governing their Processing activities under the ID5 ID Agreement shall automatically be determined by the nature of the Applicable Privacy Law governing the specific Processing activity in question, without requiring further amendment to this ID5 ID Agreement, as further detailed in the DPAs.

- iii) In the event of any conflict or inconsistency between the terms of this ID5 ID Agreement and the terms of an applicable DPA concerning the Processing of Personal Data, the terms of the applicable DPA shall control.
- iv) **Future Legal Frameworks.** In the event a new Applicable Law governing a specific Processing activity does not align with the criteria for either Opt-In Applicable Privacy Laws or Opt-Out Applicable Privacy Laws, the Parties agree to cooperate in good faith to apply the principles of the applicable DPAs to ensure such Processing complies with said Law.

b) **DPA Revisions to Comply with Applicable Laws.**

- i) ID5 may update the DPAs from time to time as reasonably necessary to comply with changes in Applicable Laws or binding regulatory guidance where such changes materially alter the Parties' rights or obligations under the DPA ("Required DPA Updates"). For any Required DPA Update, ID5 will provide Company with at least thirty (30) days' prior written notice unless a shorter period is necessitated by Applicable Law. The notice will identify the modifications and the effective date.
- ii) If Company reasonably objects in writing within fifteen (15) days of receiving such notice, specifying that the modifications go beyond what is legally required or materially prejudice Company in a manner not necessitated by Applicable Privacy Law, the Parties will discuss the objection in good faith. If Company does not object within fifteen (15) days, or if the Parties cannot resolve a timely objection within fifteen (15) days of discussion commencing, the Required DPA Update will be deemed incorporated into this ID5 ID Agreement as of the effective date specified in the notice. ID5 will maintain an accessible archive of previous versions of the DPAs at id5.io/legal/agreements/dpa.
- iii) If Company has any proposed changes to the DPAs required by the Applicable Privacy Law, it may notify ID5 by email to legal@id5.io. Upon receipt of such notice, the Parties shall cooperate in good faith to implement the proposed amendments, if required and appropriate, as soon as is reasonably practicable.
- iv) **Notwithstanding the foregoing, ID5 may make non-substantive changes or clarifications to the DPAs that do not materially alter the Parties' rights or obligations (such as correcting typographical errors, clarifying existing provisions without changing their substantive meaning, reformatting, or making other purely stylistic revisions) by posting an updated version at the designated URL(s) without providing formal notice under this section. The archive of previous versions will reflect these updates.**

9) **Term; Termination; Suspension.**

- a) **Term.** This ID5 ID Agreement shall commence on the Effective Date and shall continue in full force and effect until terminated by either Party pursuant to Section 9(b), 9(c), or 9(d) (the "Term").
- b) **Termination for Convenience.** Company may terminate this ID5 ID Agreement at any time upon five (5) business days' prior written notice to ID5. ID5 may terminate this ID5 ID Agreement at any time upon at least sixty (60) days' prior written notice to Company.
- c) **Termination for Breach.** Each Party may terminate this ID5 ID Agreement immediately on notice to the other Party if it reasonably believes that Party is in material breach hereof; provided that, if the breach is capable of cure, the breaching Party will have thirty (30) days from the notice date to cure the breach to the non-breaching Party's reasonable satisfaction.
- d) **Actions Upon Termination.** Notwithstanding any other provision in this ID5 ID Agreement, in the event this ID5 ID Agreement is terminated for any reason, Company and its Related Parties must remove or deactivate the ID5 Software and ID5 OSS on all Digital Properties. Whilst the ID5 ID Service remains active on any Digital Property, including where any ID5 Software or ID5 OSS instance references Company's or any Related Party's ID5 Partner Number, and notwithstanding the termination or expiration of the Term, the terms and conditions of this ID5 ID Agreement shall remain in force as between ID5 and Company in respect of such usage.
- e) **Suspension of Service.** Without limiting any of ID5's rights under this ID5 ID Agreement, ID5 may immediately suspend Company's (and/or any Related Party's) access to or use of the ID5 ID Service, in whole or in part, if ID5 reasonably determines that: (i) Company or any Related Party has breached any material term of this ID5 ID Agreement ; (ii) Company's or any Related Party's use of the ID5 ID Service poses a security risk to the ID5 ID Service or to other users thereof, or may adversely impact the ID5 ID Service or systems operated by ID5; or (iii) suspension is required pursuant to a legal or regulatory requirement. ID5 will use commercially reasonable efforts to provide Company with prior notice of any suspension and an opportunity to remedy the issue, where practicable.
- f) **Survival.** Without limiting the foregoing, the following provisions shall survive any termination or expiration of this ID5 ID Agreement: Section 3(a) (Intellectual Property), Section 7 (Confidentiality), Section 8(a) (Data Processing Addendum), Section 9(d) (Actions on Termination), Section 10 (Disclaimers; Limitation of Liability), Section 11 (Indemnification), and Section 13 (Miscellaneous), together with the Definitions and any other provisions that by their nature are intended to survive.

10) DISCLAIMERS; LIMITATION OF LIABILITY.

- a) **Disclaimers.** EXCEPT AS EXPRESSLY SET FORTH HEREIN, THE ID5 ID SERVICE, THE ID5 SOFTWARE, AND ID5 PLATFORM ARE PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS, WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. ID5 AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING, USAGE OR TRADE PRACTICE. ID5 DOES NOT WARRANT THAT THE ID5 ID SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE.
- b) **Limitations of Liability.**
 - i) **Basis of Bargain.** THE PARTIES ACKNOWLEDGE AND AGREE THAT THE DISCLAIMERS AND LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION 10 ARE FUNDAMENTAL AND REFLECT A REASONABLE AND FAIR ALLOCATION OF RISK BETWEEN THE PARTIES, TAKING INTO ACCOUNT THE FACT THAT (i) THE ID5 ID SERVICE IS PROVIDED FREE OF CHARGE; (ii) ID5 OWES A MATERIAL PORTION OF ITS OBLIGATIONS DIRECTLY TO REGULATORS AND DATA SUBJECTS UNDER APPLICABLE PRIVACY LAW; (iii) THE ID5 ID SERVICE IS, BY ITS NATURE, AUTOMATED AND HIGH-VOLUME, AND THEIR PROVISION IS PREDICATED ON THE WARRANTIES AND COMPLIANCE OF THOUSANDS OF INDEPENDENT PARTNERS, INCLUDING COMPANY; (iv) A CORE COMPONENT OF THE SOLUTION, THE ID5 OSS, IS PROVIDED AS FREE AND OPEN-SOURCE SOFTWARE UNDER THE APACHE LICENSE, VERSION 2.0, WHICH ITSELF DISCLAIMS WARRANTIES AND LIMITS LIABILITY; AND (v) ID5 IS PRIMARILY AND EXISTENTIALLY RELIANT ON COMPANY’S, AND ITS RELATED PARTIES’, COMPLIANCE WITH THIS ID5 ID AGREEMENT AND APPLICABLE PRIVACY LAW. THE PARTIES FURTHER ACKNOWLEDGE THAT ID5 WOULD NOT BE ABLE TO PROVIDE THE ID5 ID SERVICE ON AN ECONOMICALLY VIABLE BASIS WITHOUT THESE LIMITATIONS AND THAT THEY FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES.
 - ii) **Exclusion of Certain Damages.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ID5 OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF BUSINESS, LOSS OF DATA, OR COST OF SUBSTITUTE GOODS OR SERVICES, ARISING OUT OF OR IN CONNECTION WITH THIS ID5 ID AGREEMENT OR THE USE OF OR INABILITY TO USE THE ID5 ID SERVICE, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), STATUTE, OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT ID5 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ID5 BE LIABLE FOR ANY CLAIMS OR DAMAGES OF ANY KIND ARISING FROM OR RELATING TO THE USE OF COLLECTED SIGNALS AND COMPANY SIGNALS SO LONG AS SUCH USE IS IN ACCORDANCE WITH THE PERMITTED PURPOSE.
 - iii) **Maximum Aggregate Liability.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, AND SUBJECT TO SECTION 10(b)(iv), ID5’S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS ID5 ID AGREEMENT OR THE ID5 ID SERVICE, FOR ANY AND ALL CLAIMS (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STATUTE, OR OTHERWISE), SHALL NOT EXCEED ONE THOUSAND GREAT BRITAIN POUNDS (£1000). THIS LIMITATION IS CUMULATIVE FOR ALL CLAIMS AND NOT PER INCIDENT.
 - iv) **Exclusions.** NOTHING IN THIS ID5 ID AGREEMENT SHALL LIMIT OR EXCLUDE EITHER PARTY’S LIABILITY FOR: (A) DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR THE NEGLIGENCE OF ITS EMPLOYEES, AGENTS OR SUBCONTRACTORS; (B) FRAUD OR FRAUDULENT MISREPRESENTATION; OR (C) ANY OTHER LIABILITY THAT CANNOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW.

11) Indemnification.

- a) Company will defend, indemnify, and hold harmless ID5, its Affiliates, and its and their respective officers, directors, employees, agents, successors and assigns (each, an “**ID5 Indemnified Party**”), from and against all third-party claims, liabilities, damages, losses, costs, and expenses (including reasonable outside attorneys’ fees and disbursements) (collectively, “**Losses**”), incurred by any ID5 Indemnified Party and arising out of or related to Company’s, or any Related Party’s: (a) **breach** or alleged breach of any representation, warranty, covenant, or obligation set forth in Section 6 (Obligations and Restrictions) and Section 8 (**Data Protection; Privacy**); or (b) Company’s **material breach** of any representation, warranty, covenant, or obligation under this ID5 ID Agreement **other than** those set forth in Section 6 and Section 8.
- b) **Indemnification Procedure.**
 - i) ID5 shall promptly notify Company in writing of any third-party claim subject to indemnification hereunder (“**Claim**”), provided any delay shall not relieve Company of its obligations.

- ii) Company shall assume the defense of the Claim with legal counsel reasonably acceptable to ID5, and Company shall control such defense in reasonable consultation with ID5 regarding material strategic decisions.
- iii) Company requires ID5's prior written consent (not unreasonably withheld, conditioned or delayed) for any settlement that involves an admission of fault or wrongdoing by ID5, imposes non-monetary obligations or liability on ID5, requires ID5 to take or refrain from taking any action, or could reasonably be expected to materially adversely affect ID5's reputation, business operations, or regulatory standing, provided that ID5's consent is not required for settlements solely involving the payment of money fully covered by Company under this indemnity where such settlement includes a full release of ID5 from all liability regarding the Claim. ID5 shall provide reasonable cooperation with Company's defense at Company's reasonable expense for ID5's related out-of-pocket costs.
- iv) ID5 may participate in the defense using its own counsel at its own expense. If Company fails to assume and diligently conduct the defense of a Claim after reasonable notice from ID5, ID5 may assume the defense at Company's reasonable expense.

12) Compliance

- a) **Anti-Bribery and Corruption.** During the Term, each Party shall:
 - i) comply with all Applicable Laws relating to anti-bribery and anti-corruption ("ABC Laws"), including by way of example the UK Bribery Act 2010 and the US Foreign Corrupt Practices Act;
 - ii) establish, maintain and enforce its own policies and procedures to ensure compliance with the ABC Laws;
 - iii) the other party if it becomes aware of any breach of this Section 12 or has reason to believe that it has received a request or demand for any undue financial or other advantage in connection with the performance of this ID5 ID Agreement; and
 - iv) ensure that any of its Related Parties do so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed under this Section 12.
- b) **Trade Sanctions.** Company shall not enable or use the ID5 Software, the ID5 ID Service, or the ID5 IDs where such enablement or use would violate any applicable trade sanctions, export control laws, or embargoes.
- c) **Compliance with U.S. Data Security Regulations.** Company represents and warrants that it is not, and any party who use its ID5 Partner Number (including Related Parties) is not, and is not owned or controlled by, an entity or person located in, or subject to the jurisdiction of, any "Country of Concern" (defined by the U.S. government from time to time, which currently includes China, Russia, Iran, North Korea, Cuba, and Venezuela). Company further agrees that it will not transfer, license, or provide access to any data received from the ID5 ID Services to any such entity or person.
- d) **Global Trade Compliance.** Company represents and warrants that it, and any third party utilizing its ID5 Partner Number, is not a person or entity subject to restrictions under any applicable economic sanctions, trade embargoes, or export control laws and regulations. Company agrees that it will not use ID5's services in a manner that violates such laws, nor will it provide access to the services to any party in a comprehensively sanctioned or embargoed country or territory or for a prohibited end-use.
- e) Breach of this Section 12 shall be deemed an irremediable material breach of this ID5 ID Agreement.

13) Miscellaneous.

- a) **Notices.** All notices under this ID5 ID Agreement must be made in writing (including, without limitation, email) and sent to the attention of: (a) if to Company, to the email address of the primary contact provided at the beginning of this ID5 ID Agreement; and (b) if to ID5, ID5's CEO (at 8 Devonshire Square, 6th Floor, London, EC2M 4YJ, UK) and by email to legal@id5.io and contact@id5.io. Each Party may change its contact for notices by providing not less than five (5) business days' prior written notice to the other Party. Notice will be deemed given when delivered.
- b) **Governing Law and Jurisdiction.** This ID5 ID Agreement (and all non-contractual disputes and/or claims arising under or in connection with it) is governed by the laws of England and Wales, excluding principles of conflicts of law and is subject to the exclusive jurisdiction of the Courts of England, AND THE PARTIES HEREBY CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS. This ID5 ID Agreement will not be governed by the United Nations Convention of Contracts for the International Sale of Goods, the application of which is hereby expressly excluded. Nothing in this ID5 ID Agreement will limit a Party's ability to seek equitable relief in any court of competent jurisdiction.
- c) **Assignment.** Neither Party may assign or transfer any part of this ID5 ID Agreement without the written consent of the other Party; provided, however, that this ID5 ID Agreement may be assigned, without the other Party's written consent, (a) by either Party to a person or entity that acquires, by sale, merger or otherwise, all or substantially all of such assigning Party's assets, stock, or business, and (b) by ID5 to an Affiliate of ID5. Subject to the foregoing, this ID5 ID Agreement will bind and inure to

the benefit of the Parties, their respective successors and permitted assigns. Any attempted assignment in violation of this Section will be void and of no effect.

- d) **Entire Agreement, Waiver.** This ID5 ID Agreement is the Parties' entire agreement relating to its subject matter and supersedes any prior or contemporaneous agreements. Without limiting any of ID5's rights or any of Company's obligations with respect to the ID5 ID Requirements, all amendments hereto must be executed by both Parties and expressly state that they are amending this ID5 ID Agreement. Failure to enforce any provision of this ID5 ID Agreement will not constitute a waiver.
- e) **Severability.** If any provision of this ID5 ID Agreement is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.
- f) **Authorship.** No presumption or burden of proof will arise favoring or disfavoring either Party by virtue of the authorship of any of the provisions of this ID5 ID Agreement.
- g) **Relationship, Third-Party Beneficiaries.** There are no third-party beneficiaries to this ID5 ID Agreement. The Parties are independent contractors, and this ID5 ID Agreement does not create an agency, partnership or joint venture.
- h) **Force Majeure.** Neither Party will be liable for any acts or omissions resulting from circumstances or causes beyond its reasonable control.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

For ID5 Technology Ltd.	For Company
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

Exhibit A
Definitions

“ABC Laws” means all Applicable Laws relating to anti-bribery and anti-corruption.

“Affiliate” means, with respect to a Party, an entity that directly or indirectly controls, is controlled by, or is under common control with such Party. “Control” means direct or indirect ownership or control of more than 50% of the voting interests of such Party.

“Applicable Law” means any statute, law, ordinance, regulation, directive, rule, code, order, constitution, treaty, common law, judgment, decree, or other requirement of any federal, state, local, or foreign government or political subdivision thereof, or any arbitrator, court, or tribunal of competent jurisdiction applicable to a Party’s performance of its rights and obligations hereunder, and references to Applicable Law shall include such Applicable Law as amended from time to time, any successor legislation thereto, and any regulations promulgated thereunder. ABC Laws and Applicable Privacy Laws are included in the definition of Applicable Laws.

“Applicable Privacy Law” means, collectively, all Applicable Laws which relate to privacy, processing, or protection of Personal Data, cookies, Targeted Advertising, Profiling, or other laws applicable to the provision or use of the ID5 ID Service (including Opt-In Applicable Privacy Laws and Opt-Out Applicable Privacy Laws) in each case to the extent applicable to a Party’s Processing, or a portion of such Processing, hereunder, and any other laws governing the interception, recording, or monitoring of communications or data transmission. By way of example, Applicable Privacy Laws include (a) the UK Data Protection Act 2018 and the UK GDPR; (b) the EU General Data Protection Regulation (Regulation 2016/679) (“EU GDPR”); (c) the ePrivacy Directive (Directive 2002/58/EC) and implementing national legislation; (d) Applicable U.S. Privacy Laws; and (e) any other laws governing the interception, recording, or monitoring of communications or data transmission.

“Applicable U.S. Privacy Laws” means all U.S. state and federal privacy laws, such as the California Consumer Privacy Act (CCPA) as amended, and all other state and federal privacy laws, regulations, and directives, and any other laws governing the interception, recording, or monitoring of communications or data transmission.

“Business/Third Party” shall have the meaning given under Applicable Privacy Laws including the CCPA as amended.

“Collected Signals” means any and all data collected by the ID5 Software or ID5 OSS on a Digital Property directly from the Visitor’s browser, including, without limitation, IP address, user-agent string, page URL, and timestamp. Collected Signals exclude Company Signals.

“Company Signals” means Personal Data collected by Company from a data subject outside the ID5 ID Service and provided to ID5 by or at the direction of Company to ID5 hereunder. A list of data types which ID5 accepts as Company Signals is available at <https://wiki.id5.io/docs/passing-partner-data-to-id5> and Company shall not integrate any other types of data.

“Confidential Information” means any information that is disclosed, provided, or made accessible by, or on behalf of, one Party to the other Party in connection with this ID5 ID Agreement, and that is identified as “confidential” or “proprietary” or that, given the nature of the information or material, or the circumstances surrounding the disclosure or provision, reasonably should be understood to be confidential or proprietary (e.g., product or business plans). Confidential Information does not include information that the receiving Party already knew, becomes public through no fault of the receiving Party, or was independently developed by the receiving Party without reference to the disclosing Party’s confidential information. Confidential Information excludes Company Signals, Collected Signals, and encrypted ID5 IDs.

“Digital Property” means any website, application, or other digital property (a) on which the ID5 Software or ID5 OSS is placed; (b) from which Collected Signals and/or Company Signals are collected or provided; or (c) on which Company is authorized to deploy the ID5 Software or ID5 OSS; in each case by or with the authorization of, Company or any of its Related Parties (as applicable).

“Directly Identifiable Data” means any information that can be used to distinguish specific individual, including an un-hashed name, address, telephone number, and email address.

“Effective Date” means the date this ID5 ID Agreement is accepted and agreed by Company.

“Feedback” means any and all suggestions and comments provided by or on behalf of Company related to the ID5 ID Service or other ID5 services.

"ID5 Data" means all data, insights, connections, ID5 IDs, identity graphs, derivative works, and other information generated or derived by ID5 in connection with the ID5 ID Service, including through the processing of Collected Signals and Company Signals. ID5 Data is part of ID5 Intellectual Property and excludes the raw Company Signals.

"ID5 Documentation" means the documentation available at <https://github.com/id5io/id5-api.js>, the ID5 wiki currently available at wiki.id5.io.

"ID5 ID" means a unique User ID created by ID5. For the avoidance of doubt, all ID5 IDs hereunder will be delivered to Digital Properties in encrypted format only.

"ID5 ID Requirements" means, collectively, the ID5 Documentation and all applicable written requirements, specifications, and technical standards of ID5 and third parties, in each case as may be modified from time to time *provided that* ID5 will provide notice to Company of material changes to the ID5 ID Requirements which necessitate changes by Company to continue use of the ID5 ID Service.

"ID5 ID Service" means the free-of-charge, end-to-end identity resolution service provided by ID5 that processes Personal Data via the ID5 Platform to return an encrypted ID5 ID and deliver it to the ID5 Software or ID5 OSS instance.

"ID5 Software" means ID5 proprietary software provided for use with the ID5 ID Service, except the ID5 OSS.

"ID5 Intellectual Property" means all intellectual property and proprietary rights in and to: (A) the ID5 ID Service, the ID5 Software, the ID5 Platform, and the ID5 OSS; (B) the Collected Signals, the ID5 Data, ID5 IDs, and all modifications, updates, processes, and derivative works thereof; and (C) the name "ID5," its derivatives, and all trademarks and logos owned or controlled by ID5.

"ID5 Opt-Out" means ID5's opt-out website that provides end users and visitors the ability to exercise their data subject rights, including but not limited to opting-out of the ID5 ID Service (available at <https://id5-sync.com/privacy>).

"ID5 OSS" means the open-source software components, such as the ID5 javascript API, that ID5 makes available to Company for installation on its Digital Properties to enable the ID5 ID Service. The use of any ID5 OSS is governed by its applicable open-source software license, and not this ID5 ID Agreement. Use of the ID5 javascript API is governed by the terms of the Apache License, Version 2.0.

"ID5 Partner Number" means the number assigned by ID5 to Company or any of its Related Parties following execution of this ID5 ID Agreement.

"ID5 Platform" means ID5's proprietary server-side applications, code, analytics, software, trade secrets, tools, methods, systems, algorithms, and related technologies operated by ID5 to power and deliver the ID5 ID Services and other ID5 services, including all modifications, updates, enhancements, and derivative works. The ID5 Platform is and remains the sole and exclusive property of ID5 and is not licensed to Company.

"ID5 Privacy Policy" means ID5's Platform Privacy Policy (currently available at <https://id5.io/platform-privacy-policy/>), which may be updated from time to time and which discloses ID5's practices with respect to the collection, use, and disclosure of Collected Signals.

"Opt-In Applicable Privacy Laws" means Applicable Privacy Laws which require obtaining the data subject's explicit consent prior to the relevant Processing (e.g., UK, EEA).

"Opt-In Jurisdiction" means a jurisdiction where Opt-In Applicable Privacy Laws apply.

"Opt-Out Applicable Privacy Laws" means Applicable Privacy Laws which permit the relevant Processing to occur based on providing data subjects with notice and an opportunity to opt-out of Processing (e.g., certain U.S. states).

"Opt-Out Jurisdiction" means a jurisdiction where Opt-Out Applicable Privacy Laws apply.

"Permitted Purpose" means (a) Company's exercise of the rights granted to it under Section 2(b)(i); and (b) ID5's performance of the following activities, conducted in a manner consistent with the ID5 Privacy Policy: (i) providing and operating the ID5 ID Service and related identity resolution; (ii) processing Collected Signals and Company Signals in connection with such services, including for the creation of ID5 Data; and (iii) developing, maintaining, operating, securing, analyzing, and improving the ID5 ID Service and providing related ID5 products, services, and technologies such as identity resolution and cross-device linking.

"Personal Data" shall mean any information defined as "personally-identifiable information," "personal information," "personal data" or similar terms as such terms are defined under Applicable Privacy Laws.

"Process" or **"Processing"** means 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.

"Profiling" means any form of automated Processing of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Related Party" means, with respect to Company, (a) its Affiliates; and (b) any third party (such as a digital advertising partner, Subcontractor, managed publisher, vendor, or client); that utilizes the ID5 ID Service, ID5 Software, ID5 OSS, or ID5 IDs via Company's integration, under Company's ID5 Partner Number, or otherwise, where such third party has not entered into a direct agreement with ID5 for the ID5 ID Service. Without limiting the foregoing, all ID5 Software and ID5 OSS which utilizes one or more ID5 Partner Numbers assigned by ID5 to Company related to this ID5 ID Agreement shall be considered Related Parties.

"Restricted Age" means the age below which Applicable Privacy Law imposes specific restrictions or requirements on the Processing of Personal Data relating to individuals under such age, such as requiring verifiable parental or guardian consent prior to Processing (examples include the age thresholds defined under the Children's Online Privacy Protection Act (COPPA) in the United States or Article 8 of the General Data Protection Regulation (GDPR) in the European Union), including as modified by time to time under an Applicable Privacy Law.

"Sensitive Data" means data that constitutes "sensitive data", a "special category of data", or a corresponding term denoting a substantially similar meaning under Applicable Law, which depending on jurisdiction may include: financial account numbers, insurance plan numbers, precise information about health or medical conditions, medical records or pharmaceutical prescriptions, government-issued identifiers (such as a Social Security number), race, ethnicity, religion, trade union membership, sexual orientation, genetic or biometric information and precise location information such as GPS coordinates.

"Subcontractor" means, with respect to a party, a contractor, subcontractor, consultant, third-party service provider, or agent engaged by such party in connection with its use or provision of the ID5 ID Service under this ID5 ID Agreement.

"Targeted Advertising" means the processing of previously Collected Signals about an individual, browser, or device to tailor advertising across unaffiliated web domains, applications, or properties, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about that individual, browser, or device and/or as defined under Applicable Privacy Laws.

"TrueLink" means an optional feature or integration that, when enabled by Company, generates a signal from a secondary domain to assist ID5 in generating a more accurate ID5 ID for a Visitor across different Digital Properties.

"User ID" means a unique identifier that may be associated with an end user or Visitor, such as a cookie ID, a mobile advertising identifier, a hashed email address, or any other identifier.

"Visitor" means an end user or visitor of a Digital Property.

"Visitor Choice" means any expression by a Visitor of their preferences or exercise of their rights regarding the Processing of their Personal Data under Applicable Privacy Law, including expressions of consent, objection, opt-out, withdrawal of consent, or data subject rights requests made pursuant to Applicable Privacy Law. Visitors may exercise their rights directly with ID5 via the ID5 Opt-Out.

"Visitor Choice Signals" means digital or other signals or communications reflecting Visitor Choices that are recognized under this ID5 ID Agreement and supported in the ID5 ID Requirements, including: (i) signals collected via Company's or its Related Parties' consent management platforms or other user interfaces reflecting Visitor Choice; (ii) Visitor Choices communicated via the ID5 Opt-Out or via email to ID5; and (iii) any other signals recognized under Applicable Privacy Law or applicable industry standards (such as the IAB Transparency and Consent Framework and Global Privacy Control signals).

Exhibit X
OPT-IN JURISDICTION DATA PROCESSING ADDENDUM
(Controller-to-Controller)

1. Definitions

- a. Capitalized terms used but not defined in this Opt-In DPA shall have the meanings given to them in the Prime Agreement.
- b. In this Opt-In DPA, the following terms shall have the meanings set out below and, where applicable, shall be interpreted consistently with the definitions provided under the relevant Opt-In Applicable Privacy Law:
 - i. **“Controller”, “Data Subject”, “Personal Data”, “Processing” and “Personal Data Breach”** shall have the meanings given under the relevant Opt-In Applicable Privacy Law. For Processing governed by Applicable European Data Protection Law, these terms shall have the meanings given in the EU GDPR or UK GDPR, as applicable.
 - ii. **“Opt-In Personal Data”** means Personal Data Processed by either Party pursuant to the Prime Agreement where such Processing is subject to Opt-In Applicable Privacy Laws. This includes Collected Signals and Company Signals to the extent they constitute Personal Data under the relevant Opt-In Applicable Privacy Law.

2. Scope and Applicability

- a. To the extent Applicable Privacy Laws require obtaining the data subject's explicit consent prior to the relevant Processing ("Opt-In Applicable Privacy Laws"), the terms of this Opt-In DPA shall apply.
- b. The applicability of this Opt-In DPA may change in the event of a change in Applicable Privacy Laws, and, instead, the Opt-Out DPA (available at id5.io/legal/agreements/dpa/opt-out) may instead apply from the effective date of the revised Applicable Privacy Law(s) with respect to some or all Processing. As of June 2025, Opt-In Applicable Privacy Laws include (i) Applicable European Data Protection Law such as GDPR and UK GDPR (ii) Brazil Data Protection Law; and (iii) Argentina Data Protection Law.
- c. Each Party acts as an independent Controller in respect of its Processing of Opt-In Personal Data under Opt-In Applicable Privacy Laws. Neither Party Processes Opt-In Personal Data as a Processor or sub-processor for the other Party under the ID5 ID Agreement and/or this Opt-In DPA.
- d. Each Party shall comply with its respective obligations under the applicable Opt-In Applicable Privacy Laws with respect to its Processing of Opt-In Personal Data.
- e. Company acknowledges that it has reviewed the description of the Nature and Purpose of Processing by ID5 as set forth in Section 3 herein and in the ID5 Privacy Policy. Company agrees that for the purposes of such Processing, ID5 is an independent Controller and not a joint controller with, or Processor for, Company.

3. Details of Processing

- a. **Subject Matter:** The provision and use of any ID5 Service (which may include the ID5 ID Service and/or any Components licensed under an Order Form and/or MSA) by Company involving the collection and exchange of data to enable identity resolution and related services, as further described in the Prime Agreement, to the extent such Processing is subject to Opt-In Applicable Privacy Law.
- b. **Duration:** The Term of the Prime Agreement, subject to any post-termination data retention obligations under the Prime Agreement or applicable Opt-In Applicable Privacy Law.
- c. **Nature and Purpose of Processing:**
 - i. **By ID5:** Processing Collected Signals and Company Signals for the Permitted Purpose, as defined in the Prime Agreement. This includes, as applicable, providing the ID5 ID Service, Component(s), returning encrypted ID5 IDs, identity resolution services, generating ID5 Data, and developing, maintaining, operating, securing, analyzing, and

improving the Site Offering and related ID5 products, services, and technologies, all consistent with the ID5 Privacy Policy and Visitor Choice Signals.

- ii. **By Company:** Implementing the ID5 API on Digital Properties, collecting and transmitting Collected Signals and Company Signals to ID5, receiving and using encrypted ID5 IDs via the ID5 ID Service for the Permitted Purpose, and ensuring appropriate notices and relevant consents scoped to the Permitted Purposes are obtained from Visitors as required by Opt-In Applicable Privacy Laws.

- iii. **Types of Personal Data Processed (Opt-In Personal Data):**

1. **Collected Signals:** As defined in the Prime Agreement, including potentially IP address, user-agent string, page URL, timestamp, and User IDs.
2. **Company Signals:** As defined in the Prime Agreement and subject to the restrictions therein, potentially including hashed email addresses or other User IDs, but excluding Directly Identifiable Data or Sensitive Data.
3. **Categories of Data Subjects:** Visitors to Digital Properties.

4. Obligations of the Parties

- a. **Compliance with Law:** Each Party shall independently comply with its obligations as a Controller under applicable Opt-In Applicable Privacy Laws in respect of the Processing of Opt-In Personal Data.

- b. **Transparency and Lawful Basis (Consent):**

- i. **Company:**

1. Company is solely responsible for providing clear, comprehensive, and accurate notices to Visitors on Digital Properties regarding the Processing of Personal Data by both Company and ID5 (including the use of the ID5 ID Services and ID5 IDs) as contemplated by the Prime Agreement, sufficient to meet the requirements of applicable Opt-In Applicable Privacy Laws, including associated guidelines and supplementary instructions provided by the applicable regulatory and/or data protection authorities of the applicable jurisdiction.
2. Company represents and warrants that it shall obtain and maintain all necessary Visitor Choices, including valid, affirmative consents where required by Opt-In Applicable Privacy Laws, to permit the lawful collection and transmission of Opt-In Personal Data to ID5 and ID5's subsequent Processing thereof for the Permitted Purpose. Company shall ensure Visitor Choice Signals accurately reflecting such choices are collected and transmitted to ID5. ID5 may request proof of consent from time to time. Where available, including the European Economic Area, Company must provide an IAB TCF-compliant consent management platform to collect and transmit TCF strings to ID5 except where expressly agreed by ID5 in writing.
3. Company shall prevent ID5 Services from (A) being executed in any jurisdiction in which there are Opt-In Applicable Privacy Laws; or (B) Opt-In Personal Data is collected and/or communicated to ID5 for Processing; unless Company can fully comply with the provisions of this DPA. ID5 Services should not be used or deployed where Company cannot provide adequate consent mechanisms, including a Consent Management Platform ("CMP") to communicate Visitor Choice Signals to ID5, in compliance with the Service Requirements applicable to the ID5 ID Service and/or the Components, the then-current IAB Europe Transparency and Consent Framework, or other mechanism if approved by ID5 in writing.

- ii. **ID5:** ID5 shall ensure that the ID5 Privacy Policy provides clear and comprehensive information about its Processing activities as required by applicable Opt-In Applicable Privacy Laws. ID5 shall Process Opt-In Personal Data received from Company only for the Permitted Purpose(s) and in accordance with the Visitor Choice Signals transmitted by Company.

- c. **Data Subject Rights:**

- i. Each Party is independently responsible for responding to Data Subject requests it receives relating to the Personal Data it Processes as a Controller under the relevant Opt-In Applicable Privacy Law.
- ii. The Parties agree to provide reasonable assistance to each other as necessary (at the requesting Party's expense for out-of-pocket costs) to enable the handling of Data Subject requests under applicable Opt-In Applicable Privacy Laws (e.g., access, rectification, erasure, restriction, data portability, objection, withdrawal of consent). Company shall provide mechanisms for Visitors to exercise rights related to Company's Processing, and ID5 provides the ID5 Opt-Out mechanism for rights related to its Processing.
- d. **Personnel:** Each Party shall ensure that its personnel authorized to Process Opt-In Personal Data are subject to appropriate confidentiality obligations.
- e. **Security:** Each Party shall implement and maintain appropriate technical and organizational measures to protect Opt-In Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure, consistent with the Prime Agreement and the requirements of applicable Opt-In Applicable Privacy Laws.
- f. **Personal Data Breaches:**
 - i. In the event of a Personal Data Breach affecting Opt-In Personal Data, the Party experiencing the breach shall notify the other Party without undue delay, where feasible and solely to the extent required by the Opt-In Applicable Privacy Laws, if the breach is likely to materially impact the other Party or the privacy rights of Data Subjects whose Opt-In Personal Data was impacted by the Personal Data Breach.
 - ii. Each Party is independently responsible for complying with its own obligations under the relevant Opt-In Applicable Privacy Law regarding Personal Data Breach notification to supervisory authorities and/or affected Data Subjects. The Parties agree to cooperate reasonably in relation to any Personal Data Breach investigations as required.
- g. **Data Protection Impact Assessments:** Each Party is responsible for undertaking any Data Protection Impact Assessments or similar assessments required under applicable Opt-In Applicable Privacy Laws for its own Processing activities. The Parties shall provide reasonable assistance to each other (at the requesting Party's expense for out-of-pocket costs) if required for such assessments related to the Processing of Opt-In Personal Data under this Opt-In DPA.
- h. **Records of Processing:** Each Party shall maintain records of its Processing activities involving Opt-In Personal Data as required by applicable Opt-In Applicable Privacy Laws (such as Article 30 GDPR where applicable).
- i. **Sub-processors/Third Parties:** This DPA addresses the Controller-to-Controller relationship. Where a Party engages processors or sub-processors for its own Processing activities involving Opt-In Personal Data, that Party remains solely responsible for complying with Controller obligations under the relevant Opt-In Applicable Privacy Law regarding such engagements (such as Article 28 GDPR where applicable).

5. Data Transfers

- a. Any transfer of Opt-In Personal Data from one Party to the other shall be conducted in compliance with the requirements of the applicable Opt-In Applicable Privacy Law governing the data being transferred.
- b. To the extent that the Processing of Opt-In Personal Data involves a transfer subject to Applicable European Data Protection Law outside the European Economic Area, Switzerland, or the UK to a territory not recognized by the relevant authority (e.g., European Commission or UK Information Commissioner's Office) as ensuring an adequate level of data protection, the Parties agree to rely on the applicable Standard Contractual Clauses (SCCs) approved by the European Commission, incorporated herein by reference, supplemented by the UK Addendum. The details of the SCCs module(s) and any specific annexes/appendices applicable are documented in Schedule A to this Exhibit Y at id5.io/legal/agreements/SCCs.
- c. For transfers subject to other Opt-In Applicable Privacy Laws requiring specific cross-border transfer mechanisms, the Parties agree to cooperate in good faith to implement such mechanisms as legally required.

6. Miscellaneous

- a. **Conflict:** In the event of any conflict or inconsistency between the terms of this Opt-In DPA and the Prime Agreement concerning the Processing of Personal Data subject to Opt-In Applicable Privacy Laws, the terms of this Opt-In DPA shall prevail.
- b. **Governing Law and Jurisdiction:** This Opt-In DPA and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of England and Wales, and subject to the exclusive jurisdiction of the Courts of England, as set out in the Prime Agreement. However, this choice of law and jurisdiction does not prevent a Data Subject from bringing proceedings in the jurisdiction mandated by the applicable Opt-In Applicable Privacy Law where required by that law.
- c. **Updates:** This Opt-In DPA may be updated by ID5 in accordance with Section 8(b) of the ID5 ID Agreement or equivalent provision of any other contractual agreement between ID5 and Company.

Exhibit Y

OPT-OUT JURISDICTION DATA PROCESSING ADDENDUM

This Opt-Out DPA sets out the terms and conditions that apply to the Processing of Personal Data under the Prime Agreement where such Processing is subject to Opt-Out Applicable Privacy Laws. The Parties intend that this Opt-Out DPA addresses the requirements of Opt-Out Applicable Privacy Laws, including Applicable U.S. Privacy Law such as the California Consumer Privacy Act (CCPA) as amended, acknowledging that such laws may evolve and new Opt-Out Applicable Privacy Laws may emerge globally.

1. Definitions

- a. Capitalized terms used but not defined in this Opt-Out DPA shall have the meanings given to them in the Prime Agreement.
- b. In this Opt-Out DPA, the following terms shall have the meanings set out below and, where applicable, shall be interpreted consistently with the definitions provided under the relevant Opt-Out Applicable Privacy Law:
 - i. "**Opt-Out Personal Data**" means Personal Data Processed by either Party pursuant to the Prime Agreement where such Processing is subject to Opt-Out Applicable Privacy Laws.
 - ii. "**Business**," "**Third Party**," "**Sale**," "**Sharing**," "**Consumer**," "**Commercial Purpose**," "**Service Provider**," and similar terms shall have the meanings ascribed to them in the relevant Opt-Out Applicable Privacy Law (e.g., the CCPA), as applicable to the specific Processing activity.
 - iii. "**Component(s)**" means the selected Components as described in the ID5 MSA and/or Order Form(s), as applicable.

2. Scope and Applicability

- a. This Opt-Out DPA applies exclusively to the Processing of Personal Data (including Collected Signals and Company Signals) under the Prime Agreement that is, or in the future becomes, subject to laws other than Opt-In Applicable Privacy Laws (as defined in the Prime Agreement).
- b. The applicability of this Opt-Out DPA may change in the event of a change in Applicable Privacy Laws resulting in the requirement to obtain the data subject's explicit consent prior to the relevant processing ("**Opt-In Applicable Privacy Laws**"), and, instead, the Opt-In DPA (available at id5.io/legal/agreements/dpa/opt-in) will apply from the effective date of the revised Applicable Privacy Law(s) with respect to some or all Processing. As of June 2025, Opt-Out Applicable Privacy Laws include, but are not limited to, the United States and its various state laws such as CCPA/CPRA.
- c. Each Party shall comply with its respective obligations under the Out-Out Applicable Privacy Laws with respect to its Processing of Opt-Out Personal Data.
- d. In the event of any conflict between the terms of this Opt-Out DPA and the Prime Agreement concerning the Processing of Personal Data under Opt-Out Applicable Privacy Laws, the terms of this Opt-Out DPA shall prevail.

3. Details of Processing

- a. **Subject Matter:** The provision and use of any ID5 Service (which may include the ID5 ID Offering and/or any Components licensed under the Prime Agreement) by Company involving the collection and exchange of data to enable identity resolution and related services, as further described in the Prime Agreement, to the extent such Processing is subject to Opt-Out Applicable Privacy Law.
- b. **Duration:** The Term of the Prime Agreement, subject to any post-termination data retention obligations under the Prime Agreement or applicable Opt-Out Applicable Privacy Law.
- c. **Retention:**
 - i. **ID5:** ID5 will delete or otherwise permanently remove Opt-Out Personal Data within 99 days of receipt.
 - ii. **Company:** Company will delete or otherwise permanently remove Opt-Out Personal Data received from ID5, including ID5 IDs (encrypted and decrypted as applicable) and any Component Outputs (as described in an ID5 MSA and/or Order Form, as applicable) within thirty (30) days of receipt.
- d. **Data Processing Description**
 - i. **Categories of Data Subjects:** Visitors to Digital Properties.
 - ii. **Categories of Personal Data:**
 - 1. **Collected Signals:** As defined in the Prime Agreement, including IP address, user-agent string, page URL, timestamp, and User IDs.
 - 2. **Company Signals:** As defined in the Prime Agreement and subject to the restrictions therein, potentially including hashed email addresses or other User IDs, but excluding Directly Identifiable Data or Sensitive Data.
 - iii. **Processing Activities:** Collection and transmission via the ID5 API, receipt of Company Signals, creation and provision of encrypted ID5 IDs, use for identity resolution, analysis, service improvement, reporting, honoring opt-outs, all as part of providing the ID5 ID Service and/or Component(s) and fulfilling the Permitted Purpose.
 - iv. **Purpose of the Processing:** Each Party's exercise of its respective rights and performance of its obligations with respect to the Permitted Purpose as defined in the Prime Agreement.

4. Roles and Responsibilities of the Parties

- a. **Roles; Compliance with Law:** The Parties acknowledge that under Opt-Out Applicable Privacy Laws, their specific roles may vary (e.g., Controller/Controller, Business/Third Party). Both Parties act as independent controllers (or the equivalent concept under the relevant Opt-Out Applicable Privacy Law) regarding their respective Processing activities, except where expressly stated otherwise for a specific jurisdiction herein.
- b. **CCPA/CPRA Specific Roles:**
 - i. Where the CCPA/CPRA applies: a. Company is a "Business" and ID5 is a "Third Party" with respect to the Personal Data Processed under this Opt-Out DPA, unless ID5 is acting solely as a "Service Provider" for a specific, limited processing activity explicitly agreed upon separately in writing.
 - ii. Company represents and warrants it is providing Personal Data to ID5, or permitting ID5 to collect Personal Data, in compliance with the CCPA/CPRA, including providing necessary notices and opt-out rights related to any "Sale" or "Sharing" (as defined by CCPA/CPRA) that may occur through the use of the ID5 ID Offering and/or Component(s).
 - iii. ID5, as a Third Party, shall comply with the applicable obligations under the CCPA/CPRA, including processing the Personal Data for the Permitted Purpose consistent with the notices provided by Company to the Consumer and honoring opt-out signals passed by Company.

c. **Other Opt-Out Jurisdictions:** In jurisdictions governed by other Opt-Out Applicable Privacy Laws, the Parties shall comply with their respective obligations applicable to their roles under such laws, consistent with the principles of notice, opt-out, and independent processing for the Permitted Purpose(s) as outlined herein.

5. Obligations of Company

a. **Lawful Basis and Transfer:** Company is solely responsible for ensuring it has a valid legal basis for the collection, Processing, and transfer of Personal Data to ID5, and permitting ID5's collection and Processing of Personal Data via the ID5 API, under all applicable Opt-Out Applicable Privacy Laws.

b. **Notice to Visitors:** Company shall ensure that each Digital Property provides clear, comprehensive, accurate, easily accessible and legally compliant notices to Visitors that comply with all Opt-Out Applicable Privacy Laws. Such notices must include, at a minimum:

- i. A description of the categories of Personal Data collected (including via cookies and similar technologies like the ID5 API) and the purposes for which it is collected and Processed by Company and by third parties like ID5.
- ii. Disclosure that Personal Data may be provided to or collected by third parties, such as ID5, who may Process the data for their own commercial purposes, including the provision and improvement of identity resolution and related advertising technology services, consistent with the Permitted Purpose under the Prime Agreement.
- iii. Information about how Visitors can exercise their rights under Opt-Out Applicable Privacy Laws, including the right to opt-out of the "Sale" or "Sharing" of Personal Data, Profiling, Targeted Advertising, cross-context behavioral advertising, or other relevant processing activities, as applicable.
- iv. Where required by Opt-Out Applicable Privacy Laws, specific information about ID5's processing activities and a link to the ID5 Privacy Policy and ID5 Opt-Out mechanism.

c. **Visitor Choices and Opt-Outs:** Company shall:

- i. Provide Visitors with the necessary mechanisms to exercise their choices including but not limited to opt-out rights as required by Opt-Out Applicable Privacy Laws.
- ii. Accurately collect and respect Visitor Choices, including Opt-Out Requests.
- iii. Transmit Visitor Choice Signals, including Opt-Out Requests applicable to ID5's Processing, accurately, completely, and promptly to ID5 via the mechanisms specified in the ID5 ID Requirements.

d. **Data Accuracy and Minimization:** Company shall use reasonable efforts to ensure that any Company Signals provided to ID5 is accurate and limited to what is necessary for the Permitted Purpose.

e. **Data Protection Impact Assessments:** Each Party is responsible for undertaking any Data Protection Impact Assessments or similar assessments required under applicable Opt-Out Applicable Privacy Laws for its own Processing activities. The Parties shall provide reasonable assistance to each other (at the requesting Party's expense for out-of-pocket costs) if required for such assessments related to the Processing of Opt-In Personal Data under this Opt-Out DPA.

6. Obligations of ID5

a. **Purpose Limitation:** ID5 shall Process Personal Data received or collected under this Opt-Out DPA only for the Permitted Purpose as defined in the Prime Agreement, which includes ID5's own commercial purposes related to providing, operating, securing, analyzing, maintaining, and improving the ID5 ID Offering and related ID5 identity resolution products, services, and technologies (including the Component(s)), subject always to:

- i. Compliance with applicable Opt-Out Applicable Privacy Laws.
- ii. Compliance with the terms of the Prime Agreement and this Opt-Out DPA.
- iii. Respecting the valid Visitor Choice Signals transmitted by Company or received directly by ID5.

- b. **Compliance with Opt-Out Requests:** ID5 shall implement and maintain technical and organizational measures to honor Opt-Out Requests communicated via valid Visitor Choice Signals transmitted by Company or received directly via the ID5 Opt-Out mechanism, in accordance with Opt-Out Applicable Privacy Laws and the ID5 ID Offering Requirements.
- c. **Restrictions:** ID5 shall not, to the extent acting as a Third Party under CCPA, "Sell" or "Share" Personal Data received from Company if it has received a valid Opt-Out Request applicable to such data, except as otherwise permitted by the CCPA. More broadly, ID5 shall comply with restrictions on onward processing or transfer as mandated by applicable Opt-Out Applicable Privacy Laws based on received Visitor Choice Signals and choices received directly via the ID5 Opt-Out mechanism.
- d. **Security:** ID5 shall maintain in writing a document outlining its security measures to protect Personal Data Processed under this Opt-Out DPA.
- e. **Confidentiality:** ID5 shall ensure that its personnel authorized to Process Personal Data under this Opt-Out DPA are subject to appropriate confidentiality obligations.
- f. **Sub-processors:** ID5 may engage sub-processors consistent with the terms of the Prime Agreement. Such sub-processors shall operate as Service Providers/Processors as applicable, and their Processing shall be governed by a written agreement between ID5 and such sub-processor.

7. Data Subject Rights

- a. Recognizing that both Parties may receive requests directly from Visitors exercising their rights under Opt-Out Applicable Privacy Laws (e.g., access, deletion, correction, opt-out):
 - i. If Company receives a request relating to Personal Data Processed by ID5 under this Opt-Out DPA, Company shall, where necessary and appropriate, inform ID5 and provide necessary information to assist ID5, or direct the Visitor to ID5 as appropriate.
 - ii. If ID5 receives a request that also pertains to Personal Data held solely by Company, ID5 shall inform Company or direct the Visitor to Company as appropriate.
 - iii. Each Party shall provide reasonable assistance to the other Party as necessary to enable the handling of data subject rights requests in accordance with Opt-Out Applicable Privacy Laws.

8. Security Incidents.

In the event of a security incident affecting Personal Data Processed under this Opt-Out DPA, the Parties shall comply with their respective notification obligations as set out in the Prime Agreement and Opt-Out Applicable Privacy Law.

9. Miscellaneous

- a. **Compliance and Audit.** Each Party is responsible for its own compliance with Opt-Out Applicable Privacy Laws except to the extent ID5 is reliant on Company's performance of its obligations hereunder for ID5's compliance. Company acknowledges ID5's right to verify Company's compliance with its obligations hereunder. The Parties each agrees to notify the other Party promptly in the event it is, or may be, unable to comply with the requirements of Opt-Out Applicable Privacy Laws.
- b. **Governing Law.** This Opt-Out DPA shall be governed by and construed in accordance with the laws of England and Wales, without prejudice to any mandatory requirements under applicable Opt-Out Applicable Privacy Laws.
- c. **Required Amendments.** Amendments to this Opt-Out DPA shall be made in accordance with Section 8(b) of the Prime Agreement.