Exhibit X

Opt-In Jurisdiction Data Processing Addendum

This Opt-In Jurisdiction Data Processing Addendum (**"Opt-In DPA"**) forms part of and is incorporated into the ID5 ID Agreement, ID5 MSA, and/or other fully executed contractual agreement between ID5 and Company referencing this Opt-In DPA (as applicable, the **"Prime Agreement"**).

1. Definitions

- Capitalized terms used but not defined in this Opt-In DPA shall have the meanings given to them in the Prime Agreement.
- 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 Data and Company Data to the extent they constitute Personal Data under the relevant Opt-In Applicable Privacy Law.

2. Scope and Applicability

- 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.
- 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.
- 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.
- 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.
- 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

- **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 Appliable Privacy Law.

- **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.
- **Nature and Purpose of Processing:**
  - i) **By ID5:** Processing Collected Data and Company Data 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 Data and Company Data 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 Data:** As defined in the Prime Agreement, including potentially IP address, user-agent string, page URL, timestamp, and User IDs.
    2. **Company Data:** 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**

- **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.
- **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.

- **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.
- **Personnel:** Each Party shall ensure that its personnel authorized to Process Opt-In Personal Data are subject to appropriate confidentiality obligations.
- **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.
- **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.
- **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.
- **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).
- **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**

- 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.

- 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 .
- 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**

- **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.
- **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.
- **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.

v1.1 July 3, 2025