Independent Controller Data Processing Agreement

Effective February 2022

1. **ACCEPTANCE.** This Independent Controller Data Processing Agreement ("DPA") forms part of the Publisher Master Service Agreement between ConnectAd and Customer (each, a "Party" and together, the "Parties"). This DPA sets forth the legally binding terms between Customer and ConnectAd that govern the Processing of Personal Data (as defined below) under the Agreement.

2. **DEFINITIONS.** For the purposes of this DPA, the following definitions apply. Capitalized terms that are used but not otherwise defined herein shall have the meanings as outlined in the Agreement.
   a. **"Controller"** means the entity that determines the purposes and means of the processing of Personal Data. For the avoidance of doubt, a Controller is also, where applicable, a "data controller" (as such term is defined under European Data Protection Laws) and a "business" (as such term is defined under the CCPA).
   b. **"Data Subject"** means the individual to which the Personal Data relates.
   c. **"Data Protection Laws and Regulations"** means, with respect to a Party, all privacy and data protection laws applicable to such Party's Processing of Personal Data including, where applicable: (i) European Data Protection Laws; (ii) the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder (as amended from time to time, the "CCPA"); and (iii) any other similar data protection laws in any other applicable territory, each as amended, replaced, supplemented or superseded.
   d. **"Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either ConnectAd or Customer respectively, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
   e. **"EEA"** means the European Economic Area.
   f. **"European Data Protection Laws"** means, in each case to the extent applicable to the relevant Personal Data or Processing thereof under the Agreement, (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), (b) laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in the United Kingdom, including the UK General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland under section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") and the Data Protection Act 2018 (collectively, "UK Data Protection Laws"); (c) the Swiss Federal Act on Data Protection ("Swiss FDPA"); and (d) any other data protection laws of the EEA and its Member States.

g. **“Personal Data”** means any information relating to an identified or identifiable natural person to the extent that such information is protected as “personal data” under applicable Data Protection Laws and Regulations.

h. **“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.

i. **“Processor”** means the entity which Processes Personal Data on behalf of the Controller. For the avoidance of doubt, a Processor is also, where applicable, a “data processor” (as such term is defined under European Data Protection Laws) and a “service provider” (as such term is defined under the CCPA).

j. **“Services”** means the services the Parties are obligated to provide or permitted to receive pursuant to the Agreement for which each Party determines the purposes and means of the Processing of Personal Data.

k. **“Sensitive Data”** means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation, as well as any other type of data that is considered sensitive according to Data Protection Laws and Regulations.

l. **“SCCs”** means “Module One: Transfer controller to controller” of the Standard Contractual Clauses set forth in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, made available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/, as supplemented and/or amended by the selections and addendum set forth in **Annex A** of this DPA.

m. **“Transfer”** means the access by, transfer, or delivery to, or disclosure to a person, entity, or system of Personal Data where such person, entity or system is located in a country or jurisdiction other than the country or jurisdiction from which the Personal Data originated.

3. **ROLE OF THE PARTIES.** In performing their respective obligations under the Agreement, each Party may receive Personal Data which may be subject to Data Protection Laws and Regulations. The Parties acknowledge and agree that each Party is a separate and independent controller in respect of such Personal Data and shall individually determine the purposes and means of its Processing of such Personal Data. The Parties further acknowledge that neither Party is responsible for determining the requirements of Data Protection Laws and Regulations applicable to the other Party.

4. **RESTRICTION ON SENSITIVE DATA.** The Parties acknowledge and agree that neither Party shall provide or make available Sensitive Data to the other Party in connection with the Services. The Parties acknowledge and agree that ConnectAd shall have no responsibility or liability for any Sensitive Data erroneously or inadvertently transferred under this DPA. Nothing in this DPA shall be interpreted to limit any restrictions under the Agreement regarding the types of Personal Data that may be provided by Customer to ConnectAd.

5. **OBLIGATIONS OF THE PARTIES.**
    a. **Lawfulness of Processing.** Each Party acknowledges and confirms that: (a) it will comply with applicable Data Protection Laws and Regulations and this DPA in connection with its Processing of Personal Data; (b) it will only give lawful instructions to any Processors and/or Sub-Processors; (c) it will be responsible for determining the legal basis(es) of its own Processing activities; and (d) it will provide the other Party with reasonable assistance, information and cooperation as such Party may reasonably request to ensure compliance with the Parties' respective obligations under Data Protection Laws and Regulations.
    b. **Consent for Processing.** Where applicable, each Party agrees that it has obtained, or has taken commercially reasonable efforts to cause to be obtained, valid Data Subject consent (including renewal of consent) as required by Data Protection Laws and Regulations for each Processing purpose for all Personal Data made available for use in connection with the Services, and, as between the Parties, remains solely responsible for obtaining such valid consent and communicating all relevant withdrawals or revocations of consent to the other Party. Each Party shall (a) notify the other Party of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Personal Data that it provides to such Party (the "Data Receiving Party") under the Agreement that would impact the Data Receiving Party's ability to comply with the Agreement, this DPA or applicable Data Protection Laws and Regulations, and (b) where applicable, accept and abide by instructions and/or any consent signals transmitted by the other Party for Processing of Personal Data (including, for example, in the format consistent with the OpenRTB guidelines and/or relevant IAB framework signals). For the avoidance of doubt, nothing in this Section 4(b) shall limit Customer's notice and/or consent obligations under the Agreement or under Section 9 of this DPA.
    c. **Privacy Notices.** In addition to any privacy policy or notice requirements under the Agreement, each Party agrees to provide all notices and disclosures to Data Subjects required to be provided by such Party under Data Protection Laws and Regulations regarding the Processing of Personal Data contemplated under this DPA and the Agreement including, where applicable, all disclosures regarding a Data Subject's right to opt-out of Personal Data sales (as such term is defined under the CCPA).

6. **NO OWNERSHIP OR LICENSE.** Nothing in this DPA shall be construed to convey any ownership interest or license in the Personal Data that is contrary to the ownership interests and licenses set forth in the Agreement.

7. **DATA SUBJECTS' RIGHTS.** Each Party hereby authorizes the other Party to release all Personal Data in its possession directly pertaining to a verified Data Subject request for data portability to the Data Subject or his/her authorized representative, without regard to whether such Personal Data are owned/licensed by ConnectAd or Customer.

8. **REGULATORS.** Each Party agrees to: (a) promptly notify the other Party in writing of any question, complaint, investigation, inquiry, warrant, subpoena or proceedings from or brought by any public, governmental, and/or judicial agency or authority (each, a "Regulatory Request"), that relates to such other Party's (i) Processing of Personal Data in relation to the Services, or (ii) potential failure to comply with Data Protection Laws and Regulations; and (b) comply with any written litigation hold, document preservation notice, or similar legal hold requested by the other Party in connection with any Regulatory Request, lawsuit, or other claim, except to the extent required by applicable law.

9. **DATA TRANSFERS.**
    a. **Transfer Authorization.** Subject to this Section 9, the Parties acknowledge and agree that each Party is authorized to Process and Transfer Personal Data in any jurisdiction provided that such Processing complies with Data Protection Laws and Regulations. Each Party shall ensure that any Transfer it initiates will, where applicable, be subject to a lawful data transfer mechanism and/or appropriate onward transfer agreements that require that any further Transfers be conducted under a lawful data transfer mechanism.
    b. **Onward Transfers by ConnectAd.** Customer acknowledges and agrees that ConnectAd may (i) store and Process Personal Data in the United States or anywhere ConnectAd or its Processors maintain facilities, and (ii) disclose and/or Transfer Personal Data to third-party Controllers located in the United States and other countries as contemplated under the Agreement.
    c. **Transfers of Personal Data From the EEA, Switzerland or the United Kingdom.** With respect to any Transfer of Personal Data originating from the EEA, Switzerland, or the United Kingdom to a Party in a country whose laws have not been deemed by the European Commission to provide an adequate level of protection for Personal Data, and such Transfer is not subject to an alternative adequate transfer mechanism or otherwise exempt from Transfer restrictions under European Data Protection Laws, the Parties agree that the SCCs will be incorporated herein by reference and will apply to the relevant Transfer governed thereby. In furtherance of the foregoing, the Parties agree to the selections and addendum set forth in **Annex A** of this DPA. The SCCs shall automatically terminate with respect to a given Transfer once the Transfer governed thereby becomes lawful under European Data Protection Laws in the absence of such SCCs on any other basis.

10. **CONFIDENTIALITY.** The Parties agree to take steps to ensure that any person acting under their authority who has access to the Personal Data is subject to an appropriate confidentiality obligation.

11. **LIMITATION OF LIABILITY.** Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to any limitation of liability as set forth in the Agreement and any reference to such limitation of liability of a Party means the aggregate liability of the Party under the Agreement and this DPA together. Additionally, each Party shall be independently liable for its own Processing of Personal Data to the extent such Processing does not comply with Data Protection Laws and Regulations.

12. **APPLICABLE LAW AND JURISDICTION.** This DPA is and remains governed by and shall be construed in accordance with the law designated as applicable in the Agreement, except to the extent required otherwise under the SCCs.

13. **ORDER OF PRECEDENCE.** Except as specifically set forth in this DPA, the terms and provisions of the underlying Agreement shall remain unmodified and in full force and effect. In the event of a conflict between the terms of the Agreement and the terms of this DPA, the terms and provisions of this DPA shall prevail with regard to data protection matters.

14. **TERMINATION AND SURVIVAL.** The Parties agree that this DPA is terminated upon the termination of the Master Service Agreement.

15. **INVALIDITY AND SEVERABILITY.** If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

16. **COUNTERPARTS.** This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

Annex A

Standard Contractual Clause Selections and Addendum

The following selections and addendum shall supplement and/or amend the SCCs rated into the Independent Controller Data Processing Addendum.

SCCs Section Reference	**Concept**		**Selection by the Parties**
Section IV, Clause 17	Governing law		The laws of the Republic of Austria.
Section IV, Clause 18 (b)	Choice of forum and jurisdiction		The courts of the Republic of Austria.
Annex I.A	List of Parties – Data exporter(s)	Name:	Customer
		Address:	As set forth in the Agreement
		Contact:	As set forth in the Agreement
		Activities relevant to the data transferred under these Clauses:	Receipt of the Services from ConnectAd under the Agreement.
		Signature and Date:	The Parties agree that execution of the DPA by each Party shall constitute execution of the SCCs by both Parties as of the effective date of the DPA.
		Role (controller/processor):	controller
Annex I.A	List of Parties – Data importer(s)	Name:	ConnectAd Demand GmbH
		Address:	Niederhofstrasse 37/4.1 A-1120 Vienna, Austria
		Contact:	DPO, contactable at privacy@connectad.io

SCCs Section Reference		Concept	Selection by the Parties
		Activities relevant to the data transferred under these Clauses:	The provision of the Services to Customer under the Agreement.
		Signature and Date:	The Parties agree that execution of the DPA by each Party shall constitute execution of the SCCs by both Parties as of the effective date of the DPA.
		Role (controller/processor):	controller
Annex I.B	Description of the Transfer	*Categories of data subjects whose personal data is transferred*	End users of Customer's digital properties.
		Categories of personal data transferred	Categories of Personal Data transferred will depend upon the Services selected by the Customer and may include: (i) Cookies (session, persistent, LSO, other) or other unique IDs; (ii) Interest activity, behavioral targeting, or other profiling data; (iii) IP address; (iv) hashed email; and (v) User agent string/OS/chipset/screen.
		Sensitive data transferred (if applicable) and applied restrictions or safeguards	N/A
		The frequency of the transfer	Continuous basis for the term of the Agreement.
		Nature of the processing	As set forth in the Agreement.
		Purpose(s) of the data transfer and further processing	To allow ConnectAd to provide the Services under the Agreement.
		The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Data is retained only for as long as needed to fulfil obligations defined in the Agreement, or as long as needed to support a business purpose.
		For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As above.

SCCs Section Reference	Concept	Selection by the Parties
Annex I.C	Competent Supervisory Authority	The competent supervisory authority, in accordance with Clause 13 of the EU SCCs will be, for Data protected by the EU GDPR, the EU supervisory authority determined to be appropriate in the event that a relevant situation arises, and for Data protected by the Swiss DPA, the Federal Data Protection and Information Commissioner ("FDPIC"). With respect to UK Data, the competent supervisory authority is the Information Commissioners Office (the "ICO").
Annex II	Technical and Organisational Measures	As below.

TECHNICAL AND ORGANIZATIONAL MEASURES

ConnectAd strongly believes in privacy and data protection and is, therefore, a strong supporter of any privacy-regulation framework. We live data minimization and privacy-by-design in all our processes.

A. GENERAL TECHNICAL AND ORGANISATIONAL MEASURES

1. **ACCESS CONTROL OF PROCESSING AREAS.** Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely phones, database and application servers and related hardware) where the data are processed or used, to include:

   a. establishing security areas;
   b. protection and restriction of access paths;
   c. securing the data processing equipment and personal computers;
   d. establishing access authorization for employees and third parties, including respective authorization;
   e. limiting access to personnel who require it for their job function;
   f. all access to the data centers where data are hosted is logged, monitored, and tracked; and
   g. data centers where data are stored are secured by a security alarm system, or other appropriate security measures.

2. **ACCESS CONTROL TO DATA PROCESSING SYSTEMS.** Processes to prevent data processing systems from being used by unauthorized persons, to include:

   a. identification of the terminal and/or the terminal user to the data processor systems;
   b. automatic time-out of user terminal if left idle, identification and password required to reopen;
   c. regular examination of security risks by internal personnel and qualified third-parties;
   d. issuing and safeguarding of identification codes;
   e. password complexity requirements (minimum length, required character classes, etc.);

f. enforcing the use of multifactor authentication; and
g. protection against external access by means of firewall and network access controls.

3. **ACCESS CONTROL TO USE SPECIFIC AREAS OF DATA PROCESSING SYSTEMS.** Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that data cannot be read, copied or modified or removed without authorization, to include by:

   a. implementing binding employee policies and providing training in respect of each employee’s access rights to the data;
   b. assignment of unique user identifiers with permissions appropriate to the role;
   c. effective and measured disciplinary action against individuals who access Personal Data without authorization;
   d. release of data to only authorized persons; and
   e. policies controlling the retention of back-up copies.

4. **TRANSMISSION CONTROL.** Procedures to prevent data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which parties the transfer of data by means of data transmission facilities is envisaged, to include:

   a. use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
   b. implementation of encryption for the transport and storage of personal data (transport encryption and data-at-rest encryption);
   c. constant monitoring of infrastructure, including performance of the penetration tests of systems and patching systems against known vulnerabilities; and
   d. monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. **INPUT CONTROL.** Measures to ensure that it is possible to check and establish whether and by whom data has been input into data processing systems or removed, to include:
   a. authentication of the authorized personnel;
   b. protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
   c. segregation and protection of stored data via database schemas and logical access controls;
   d. utilization of user codes (passwords); and
   e. maintaining audit logs or trails that capture what personnel accessed data, when that data was accessed, and the type of access (read only, write or edit access).

6. **AVAILABILITY CONTROL.** Measures to ensure that data are protected from accidental destruction or loss, to include:
   a. automatic failover between sites;
   b. infrastructure redundancy; and

c. regular backups performed on database servers.

7. **SEGREGATION OF PROCESSING.** Procedures to ensure that data collected for different purposes can be processed separately, to include:
    a. separating data through application security for the appropriate users;
    b. storing data, at the database level, in different tables, separated by the module or function they support; and
    c. designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately.

B. TECHNICAL AND ORGANISATIONAL MEASURES FOR SENSITIVE DATA

N/A

ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

Both Parties (as defined in the DPA) agree that the SCCs shall be modified and/or supplemented as follows:

1. **TRANSFERS FROM SWITZERLAND.** If the SCCs apply to the Processing of Personal Data originating from Switzerland, the SCCs shall be modified as follows:
    a. the term “member state” shall not be interpreted in such a way as to exclude data subjects in Switzerland from suing for their rights in their place of habitual residence in accordance with Clause 18(c);
    b. the SCCs shall also protect the data of legal entities until the entry into force of the revised FDPA on or about 1 January 2023;
    c. references to the GDPR or other governing law contained in the SCCs shall also be interpreted to include the FDPA;
    d. the parties agree that the supervisory authority as indicated in Annex I.C shall be the Swiss Federal Data Protection and Information Commissioner.
2. **TRANSFERS FROM THE UNITED KINGDOM.** If the SCCs apply to the Processing of Personal Data originating from the United Kingdom, the parties acknowledge and agree that that the SCCs shall be read and interpreted in light of the provisions of UK Data Protection Laws. Accordingly, the Parties wish to amend them to the extent necessary so they operate in accordance with such laws and to provide appropriate safeguards in accordance with Article 46 of the UK GDPR. In furtherance of the foregoing, the parties agree that, at a minimum, the following modifications shall apply:
    a. Clause 6 is replaced with: “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”
    b. References to “Regulation (EU) 2016/679” or “that Regulation” are replaced by “UK Data Protection Laws” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws.
    c. References to Regulation (EU) 2018/1725 are removed.
    d. References to the “Union”, “EU” and “EU Member State” are all replaced with the “UK.”
    e. Clause 13(a) and Part C of Annex II are not used; the “competent supervisory authority” is the Information Commissioner.
    f. Clause 17 is replaced to state “These Clauses are governed by the laws of England and Wales.”
    g. Clause 18 is replaced to state: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”

3. **SUPPLEMENTAL BUSINESS-RELATED CLAUSES.** In accordance with Clause 2 of the SCCs, the Parties wish to supplement the SCCs with business-related clauses, which shall neither be interpreted nor applied in such a way as to contradict the SCCs (whether directly or indirectly) or to prejudice the fundamental rights and freedoms of Data Subjects. The Parties therefore agree that the applicable terms of the Agreement and this DPA shall apply if, and to the extent that, they are permitted under the SCCs, including without limitation the following:

   a. The information required to be provided to Data Subjects under Clause 8.2(a) shall be provided by Customer using the relevant information provided by ConnectAd in Annex I.

   b. In the event of a data subject request for a copy of the clauses in accordance with Clause 8.2(c), each Party agrees to make all redactions reasonably necessary to protect business secrets or other confidential information of the other Party.

   c. ConnectAd shall be deemed in compliance with Clause 8.7 to the extent such onward transfers occur in accordance with Article 4 of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

   d. The terms of the Agreement governing indemnification and limitation of liability, including Section 11 of the DPA, shall apply to each Party’s liability under Clauses 12(a), 12(c), and 12(d).

   e. The termination provision(s) of the Agreement shall apply to a termination pursuant to Clause 14(f) or Clause 16.

   f. Certification of deletion of Personal Data under Clause 16(d) shall be provided by ConnectAd upon written request of Customer.