DATA PROTECTION AGREEMENT

A. Parties have concluded a Master Service Agreement ("**MSA**"), under which Network, as Vertex Media, provides Services to the Publisher, as the Customer, as specified in the MSA. The execution of the MSA requires the Processing of Personal Data by the Parties. Such Personal Data Processing activities may also include the transfer of Personal Data between Parties.

B. This Data Protection Agreement ("**DPA**") sets out the framework for the provision of Personal Data between the Parties as Controllers in the context of the MSA. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the parties owe to each other and towards Data Subjects.

C. The Parties agree that they are separate Controllers in connection with Personal Data Processed under this Agreement.

D. Each Party shall comply with all the obligations imposed on a Controller under the Data Protection Laws. Publisher acknowledges that certain Data Protection Laws (such as the GDPR) may apply Publisher regardless of the location of the Publisher.

E. Any Processing of Personal Data for any other purpose than stated in this DPA or Main Agreement is strictly forbidden and will be considered a material breach of this DPA and the Agreement.

IT IS AGREED AS FOLLOWS:

1. **Definitions**

Approved Purpose	means the purposes specified in the Master Service Agreement;
Buyer	means other third party that buys and/or attempts to purchase and/or facilitates the purchase of ad inventory through NETWORK or directly from Publisher making use of NETWORK's platform whether or not via third party suppliers for execution;
Contact Point	means the Parties' representatives identified in DPA;
Controller	the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

Data Protection Agreement (DPA)	this Data Protection Agreement – including any and all subsequent amendments thereto- comprising the terms and conditions in the main body of this document, together with the schedules, the annexes and any attachments, and any documents expressly incorporated by reference;
Data Subject	an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Data Protection Laws and Regulations	means all privacy and data protection laws and regulations applicable to the Processing of Personal Data under the Agreement including, where applicable (i) EU Data Protection Laws; (ii) the Children's Online Privacy Protection Act of 1998 and any regulations promulgated thereunder (as amended from time to time, the ("COPPA"); and (iii) the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder (as amended from time to time, the ("CCPA"); (iv) any other similar data protection laws in any other applicable territory, each as amended, replaced, supplemented or superseded.
European Economic Area (EEA)	the economic territory formed by member states of the European Union and countries that are members of the European Free Trade Association (excluding Switzerland);
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC;

Master Services Agreement (MSA)	means the underlying agreement between Parties for the provision of services pursuant to which Parties, in the capacity of Separate Controllers, will carry out certain Processing of Personal Data. For the avoidance of doubt, the actual underlying agreement may be entitled differently than 'Master Services Agreement', and exist in several connected agreements, order forms, and/or general terms and conditions;
Personal Data	any information relating to a Data Subject;
Processing	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. References in this Agreement to 'Process' and 'Processed' shall be construed accordingly;
Standard Contractual Clauses	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;
Supervisory Authority	means (a) an independent public authority which is established by a member state pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of EU Data Protection Laws.

2. Scope of the DPA

1. Each Party shall comply with all the obligations imposed on a Controller under the EU Data Protection Laws. The Parties acknowledge that certain EU Data Protection Laws (such as the GDPR) may apply to the Parties regardless of where the Parties are established.
2. The Personal Data provided by (or on behalf of) the disclosing Party must not be irrelevant or excessive with regard to the Purposes. The Personal Data provided under this Agreement must be limited to the Personal Data outlined in the Appendix 1.

3. Obligation of the Parties

1. NETWORK shall not Process such received Personal Data in a way that is incompatible with the Purposes.

2. Publisher shall ensure that the Personal Data provided by it is accurate and up-to-date at the time of providing such Personal Data. Where either Party becomes aware that the Personal Data provided under this Agreement is no longer accurate or up-to-date, it shall promptly inform the other Party of such inaccuracy and provide the relevant accurate or updated Personal Data to such other Party.

4. Privacy Notices

1. Publisher acknowledges that NETWORK does not have a direct relationship with Data Subjects. Therefore, Publisher undertakes to inform Data Subjects about the involvement of NETWORK, as a Separate Controller, in the Processing of Personal Data, the nature, scope and Approved Purposes of the Processing of Personal Data, identification and contact details of a third party Processor as well as, all the other required information pursuant to Articles 13 and 14 GDPR
   a) if Personal Data will be transferred by Publisher to a third party (including NETWORK), that fact and sufficient information about such transfer and the purpose of such transfer to enable Data Subject to understand the purpose and risks of such transfer; and
   b) if Personal Data will be transferred outside the EEA by NETWORK, that fact and sufficient information about such transfer, the purpose of such transfer and the safeguards put in place to enable Data Subject to understand the purpose and risks of such transfer.

2. Notwithstanding the provisions of Clause 4.1, NETWORK guarantees to duly inform Data Subjects about their rights pursuant to Articles 15-22 GDPR. This information needs to be provided in a clear, transparent, and easily accessible manner, in the form of a privacy policy published on NETWORK's website.

5. **Legal Basis of Data Processing**

The Personal Data Processed in the context of the Approved Purposes is at all times covered by a legal basis within the meaning of Article 6 GDPR. In so far the Personal Data is Processed for the Approved Purposes relating to advertising indicated in MSA, the only applicable legal ground is Data Subject's consent pursuant to Article 6(1)(a) GDPR. Publisher is fully responsible for obtaining Data Subject's valid consent for the Processing of the Personal Data for the Approved Purposes relating to advertising. The provisions of Article 6.1. are fully applicable to this end.

NETWORK shall comply with the consent string that it receives from Publisher's consent management platform. NETWORK shall respect end user's choice, which shall be laid out in the consent string.

6. **CCPA and COPPA Compliance**

1. For purposes of the CCPA, the Parties agree that SPP is a service provider (as defined in the CCPA) for purposes of the Agreement; SPP shall not (1) retain, use, or disclose Personal Data for any purpose other than for the specific purposes of performing the Services, including retaining, using, or disclosing Personal Data for a commercial purpose (as defined in the CCPA) other than providing the Services; (2) sell (as defined in the CCPA) Personal Data; or (3) retain, use, or disclose Personal Data outside of the direct business relationship between Parties.

2. Publisher hereby undertakes that it processes data in compliance with COPPA and shall share personal data with COPPA flag with the NETWORK without parental consent, and NETWORK undertakes that it will not violate COPPA rules and it will take necessary measures to handle COPPA flagged data appropriately.

7. **Data Subject Rights**

1. The Parties agree to comply with their obligations to respond to Data Subject access requests and to give effect to other rights of Data Subjects in accordance with Data Protection Laws.

2. The Parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under Data Protection Laws within the time limits imposed by Data Protection Laws.

3. Each Party is responsible for maintaining a record of individual requests from Data Subjects, the decisions made and any information that was provided. Records must include copies of the Data Subject's request, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

8. Technical and Organizational Security Measures

1. Parties shall implement and maintain the technical and organizational measures required pursuant to Article 32 GDPR including all organizational and technical security measures necessary to protect Personal Data against unauthorized or accidental access, loss, alteration, disclosure, or destruction of Personal Data, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

2. Parties shall document the technical and organizational security measures. The documentation shall be made available to each Party upon request in case of a Supervisory Authority request for investigation.

3. Each Party shall ensure that its staff members are appropriately trained to handle, and Process the Personal Data provided (or to be provided) under this Agreement in accordance with the required technical and organizational security measures together with applicable Data Protection Laws.

9. Reporting and Notification Obligations

1. If one of the Parties becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed in the course of the Processing activities ("Data Breach"), that Party shall inform the contact point of the other Party in writing in detail without undue delay upon becoming aware of the Data Breach. This shall also apply in the event that a Data Breach, which can lead to a risk for the rights and freedoms of Data Subjects, is only suspected.

2. Each Party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) Data Subjects under Data Protection Laws and

shall each inform the other Party of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or Data Subject(s).

10. Data Protection Impact Assessment

10.1 Each Party shall carry out any data protection impact assessment required under Article 35 GDPR on its own responsibility for the Personal Data Processed for the Approved Purposes determined under this DPA.

10.2 The Parties agree to provide reasonable assistance to each other in the context of any data protection impact assessment (DPIA) or official inquiry, investigation, or proceeding by a Supervisory Authority that involves both Parties and relates to the Approved Purposes or any shared Processing of Personal Data. This includes, but is not limited to, the provision of relevant documentation, timely notifications, and coordinated responses, to the extent permitted under applicable Data Protection Laws.

11. **Data Transfer to Third Parties**

1. NETWORK is authorized to engage Buyers for carrying out the Processing of Personal Data for the purposes determined under this DPA. Publisher hereby gives its general authorisation to engage such Buyers provided that NETWORK notifies Publisher of Buyers it intends to add or replace prior to the actual engagement. Publisher has the right to object to such an engagement ultimately within 10 working days after it has received NETWORK's notification.

2. NETWORK shall provide list of its subcontractors (including demand partners) that it will share Company's end users' data. Company shall have the right to choose which demand partner its end users' data will be shared. NETWORK hereby agrees that it shall comply with Company's requests.

3. Each Party shall not transfer any Personal Data outside of the EEA unless it has a lawful basis for that transfer, including fulfilling any of the following conditions: (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 GDPR, including entering into Standard Contractual Clauses in the form approved by the EU Commission; or (iii) one of the derogations for specific situations in Article 49 GDPR applies to the transfer.
4. Upon Publisher's request NETWORK shall provide to Company any relevant information documenting its and its third parties (including demand partners) compliance with consent process and mechanisms and supporting records regarding its compliance with consent mechanism.

12. Liability

The limitations of liability in the MSA apply in all cases.

13. Miscellaneous

1. This DPA will enter into force upon its acceptance thereof by the Parties.

2. This DPA shall expire simultaneously with the MSA.

3. In the event of any inconsistency between the provisions of this DPA and the provisions of the MSA or Terms of Conditions, the provisions of this DPA shall prevail.

4. This DPA is governed by the laws of the Czech Republic. Any disputes arising out of or in connection with this DPA shall be brought exclusively before the competent court located in Czech Republic locally competent according to the registered office of NETWORK. The parties waive any objection to venue or any claim of inconvenient forum.

5. By signing the DPA, Publisher agrees to be bound by this DPA.

14. Contact points

Each Party shall, in accordance with EU Data Protection Law requirements, appoint a single point of contact that can be contacted by the other Party and/or Data Subjects for the handling of questions, notifications, claims, requests or other communication in relation to this DPA. The points of contact for each of the parties are stated in the MSA.

Appendix 1

(All terms not defined herein are as defined in the MSA.)

A. Service:
   Services as defined in the MSA such as automated selling of ad inventory, and managed services by NETWORKs for Publisher's digital properties

B. Subject and duration of Processing:

- Select basic ads
- Measure ad performance
- Personal Data is processed on a daily basis till agreement termination.

- Nature and purposes of Processing:**Ad Reporting and Conversions:** Reporting to advertisers information about when and how users have been exposed to their ads, clicked on their ads, or visited their website, and reporting to publishers information about when and how ads were shown on their properties and were clicked on.
- **Serving ads:** Allowing publishers to offer advertising inventory in their mobile apps and websites, and advertisers to bid on and fill that inventory.
- Interest-Based Advertising: Allowing Vertex Digital s.r.o. and Vertex Digital s.r.o. Customers to infer interests and serve ads to users based on their app and website activity and inferred interests. Vertex Digital s.r.o.'s policies prohibit Vertex Digital s.r.o. Customers from sending or

targeting advertisements based on information that we consider sensitive, such as race, religion, politics, sex life, or health.

- **Geo-Targeting:** Where permitted by the user's device, allowing Vertex Digital s.r.o. and Vertex Digital s.r.o. Customers to serve ads based on a user's location.**Frequency Capping:** Preventing users from seeing the same ad too many times.
- **Providing and Improving Our Services:** Auditing, researching, and analyzing data in order to maintain, protect, and improve our Services and develop new services, and to ensure that our technologies function properly.
- **Fraud Detection and Prevention: I**dentifying invalid clicks (or ad queries) and protecting Vertex Digital s.r.o. and Vertex Digital s.r.o. Customers from fraudulent behavior.

C. Purposes of Processing

- to comply with a law, regulation, legal process, or governmental request
- to protect the safety of any person
- to address fraud, security or technical issues
- to protect the rights or property of Vertex Digital s.r.o., Vertex Digital s.r.o. Customers, users of our website, or end users.

D. Categories of Data Subjects:
End Users of Publisher's digital properties.

E. The Types of Personal Data:

- Advertising ID (cookie ID, not linked to user account)
- IP address
- User ID/ Account name provided by publisher
- User ID/ Account name provided by third-party vendor
- Information about your device, such as
    - the type and model
    - manufacturer
    - operating system (e.g. iOS or Android)
    - carrier name
    - IP address, mobile browser (e.g. Chrome, Safari)
    - applications using the Vertex Digital s.r.o. Services and the version of such applications, and identifiers assigned to your device, such as
        - its iOS Identifier for Advertising (IDFA)
        - Android Advertising ID
        - or unique device identifier (a number uniquely allocated to your device by your device manufacturer).
    - The geo-location of your device (using GPS or other geo-location data), when location services have been enabled for the mobile app or website that uses the Vertex Digital s.r.o. Services.
    - Log information, including
        - the app or website visited
        - session start/stop time
        - time zone
        - network connection type (e.g., WiFi, cellular)

        - cookie information.
    - Information that Vertex Digital s.r.o. Customers and other third parties have collected and share with Vertex Digital s.r.o., such as information about activity in their services. This may include
        - the content you view or searches you made
        - the language you prefer
        - or other non-personally identifying demographic or interest information, to help make the ads served to you more relevant.
    - Information about ads served, viewed, or clicked on, such as the
        - type of ad
        - where the ad was served
            - whether you clicked on it (the ad)
        - whether you visited the advertiser's website or purchased the product or service advertised.