OpenX Ad Exchange – European Data Transfer Terms

These European Data Transfers Terms (the "**Terms**") are made and entered into between OpenX Poland sp. z.o.o ("**Data Exporter**") and each Demand Side Platform ("**DSP**") or Publisher located outside of the EEA ("**Data Importer**"). It is supplemental to the agreement between Data Importer and an OpenX entity for the provision of the OpenX Ad Exchange (the "**Agreement**") and forms part of the respective Supply Policies or Demand Policies as they apply to the Data Importer (the "**Policies**"). These Terms are effective from the date on which Data Exporter sends personal data to Data Importer (the "**Effective Date**").

1. **Definitions and Interpretation**

1.1. The following definitions and rules of interpretation apply in these Terms:

"**European Data Protection Legislation**" means European Directive 2002/58/EC, the GDPR and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates them and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**European Personal Data**" means the processing of personal data to which data protection legislation of the European Union, or of a Member State of the European Union or European Economic Area, or the United Kingdom or Switzerland was applicable prior to its processing by Data Importer.

"**GDPR**" means Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data;

"Restricted Transfer" means any transfer of personal data which, absent the incorporation into this Terms of the Standard Contractual Clauses, would breach European Data Protection Legislation;

"**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from **Module One Clauses** as indicated in this Addendum, and no other module and not including any clauses marked as optional;

"**controller**", "**personal data**", "**processing**" and "**processor**" shall have the meaning given to them in Article 4 of the GDPR.

1.2. Clause, Schedule and paragraph headings shall not affect the interpretation of these Terms.

1.3. The Schedule forms part of these Terms and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Schedule.

1.4. Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular.

1.5. These Terms shall be binding on, and ensure to the benefit of, the parties to these Terms and their respective personal representatives, successors and permitted assigns, and references to any party shall include that party's personal representatives, successors and permitted assigns.

1.6. A reference to legislation or a legislative provision is a reference to it as amended, extended or re-enacted from time to time.

1.7. Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

1.8. A reference to these Terms or to any other agreement or document is a reference to these Terms or such other agreement or document, in each case as varied from time to time.

2. **Transfers under these Terms**

2.1. These Terms have been entered into by the Parties for the purposes of complying with Data Protection Legislation for the transfer of personal data to controllers established in third countries which do not ensure an adequate level of data protection. In the event of any conflict or inconsistency between:

2.1.1. the provisions of the Agreement or Policies and this Terms, the provisions of these Terms shall prevail; and

2.1.2. the provisions of these Terms and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Save as specifically modified and amended in the Terms, or as set out in the Standard Contractual Clauses, all of the terms, provisions and requirements contained in the Agreement and Policies shall remain in full force and effect and govern these Terms.

2.2. Where the transfer of personal data to Data Importer by Data Exporter would be a Restricted Transfer, the parties agree to comply with the obligations set out in the Standard Contractual Clauses as though they were set out in full in these Terms, with Data Exporter as the 'data exporter' and Data Importer as the 'data importer' for the purposes of the Standard Contractual Clauses. Schedule 1 sets out the details of the details of the parties as required by the Standard Contractual Clauses; the Annexes to the EU Standard Contractual Clauses;

2.3. For the purposes of the Standard Contractual Clauses, the following shall apply: (i) Clause 17 (Governing law) the clauses shall be governed by the laws of Poland; and Clause 18 (Choice of forum and jurisdiction) the courts of Poland shall have jurisdiction.

SCHEDULE 1

Annex I: Module one (controller to controller)

A. List of parties

Data Exporter

Legal Entity and Address	Contact Person and Contact Details	Activities in relation to the data transfer	Signature and Name	Date	Role
OpenX Poland sp. z.o.o	Joshua Metzger Data Protection Officer dpo@openx.com	Makes available personal data to the Data Importer through the OpenX Exchange.	_____	The Effective Date	Controller

Data Importer

Legal Entity and Address	Contact Person and Contact Details	Activities in relation to the data transfer	Signature and Name	Date	Role
The Data Importer, with their Address as set out in the Agreement.	As set out in the Agreement	Receives and processes the data transferred to it from the Data Exporter through the OpenX Exchange	As set out in the Agreement	The Effective Date	Controller

B. Description of transfer

Categories of data subjects whose personal data is transferred: Individuals whose personal data is contained in a bid request (if a Data Importer is a DSP) or individuals whose personal data is contained in bid response, or creative content (if a Data Importer is a Publisher).

Categories of personal data transferred: If a Data Importer is a DSP, data sent by the Data Exporter in a bid request will vary depending on the information included in the ad request, sent by the Publisher to the Data Exporter. This information may include: unique ID of the bid request; IP address and user-agent string; geolocation information (e.g. lat / lon, country code, region code, ZIP code; whilst OpenX may be sent information derived from precise

device location, including GPS data, it predominantly uses location derivable from IP address within the exchange); device information (e.g. device operating system version, device make, device model) and browser information (type of browser, browser language, browser settings); device identifiers (e.g. Mobile Advertising IDs (MAIDs), Apple's Identifier for Advertisers (IDFA) and Google's Advertising ID for Android devices (AAID)); user information (e.g. gender or list of keywords / interests); details about the publisher's website / app (e.g. name, domain, URL of the website where impression will be shown, contextual taxonomy of a website or content language); cookie IDs and other unique identifiers, including those to allow cookie syncing and information about the activity on the website/app (web pages or apps visited, time those web pages or apps were visited or used). If a Data Importer is a Publisher, creative markups encoded by DSPs in bid responses may include user IDs and other unique identifiers or pixels, including those that allow cookie or pixel syncing, and this information may be provided to Data Importer through the OpenX Ad Exchange as part of the delivery of an advertisement.

Sensitive data transferred (if applicable): N/A

The frequency of the transfer: Data is transferred upon each use of OpenX Ad Exchange by the Data Importer (if a Data Importer is a DSP) or data is potentially transferred upon each use of OpenX Ad Exchange by the Data Importer (if a Data Importer is a Publisher).

Nature of the processing: OpenX Poland is required to transfer personal data received from its Publishers to its DSPs, in order to allow DSPs to determine whether they wish to bid on advertising opportunities available on Publishers' assets and place advertising. OpenX Poland may also be required to transfer personal data received from DSPs to its Publishers, in order to allow DSPs to obtain information about the performance of their advertising.

Purpose(s) of the data transfer and further processing: allow DSPs to assess a bid request and determine whether to make a bid response (if a Data Importer is a DSP) or to measure advertising performance (if a Data Importer is a Publisher).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data is retained by the Data Importer in accordance with their retention policies.

C. Competent Supervisory Authority

PUODO (Poland)

Annex II: Technical and organizational measures

A. General Technical and Organisational Measures

Data Importer implements the following security measures with respect to the data transferred by the Data Exporter:

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