# GLOBAL DATA PROCESSING AGREEMENT

This OpenX Global Data Processing Agreement (the "**DPA**") was last updated on, and is effective as of May 1, 2026. It is incorporated by reference into OpenX's Ad Exchange Supply Policy and Ad Exchange Demand Policy (the "**OpenX Policies**"), and forms part of the underlying agreement(s) (the "**Agreement**") between the company listed on the signature page of the Agreement ("**Company**") and the OpenX entity listed on the signature page of the Agreement **("OpenX").** To the extent there is any conflict between this DPA, the OpenX Policies, and/or the Agreement, this DPA will govern unless contradicted by specific privacy terms that have been negotiated between Company and OpenX in the Agreement.

This DPA contains the following sections, which are hyperlinked below. To the extent you have any questions related to this DPA or its applicability to an Agreement, please contact OpenX at legal@openx.com.

---



---

## 1. General Terms Governing All Data Transfers

The following sections govern all data transfers subject to this DPA.

### 1.1 Roles of the Parties

1.1.1 The respective roles of the parties (e.g., whether each is a controller, processor, or other designation) will be set forth in the Agreement.

1.1.1.1 If for some reason the respective roles of the parties are not set forth in the Agreement, Discloser and Recipient will each be considered separate Controllers, and separate Businesses / Third Parties under the CCPA, in relation to the Personal Data being Processed under this DPA, provided that the context and nature of the Processing at issue aligns with those designations.

1.1.1.2 Nothing in this DPA is intended to create a joint Controller relationship unless expressly stated in the Agreement.

1.1.2 The parties will each comply with their respective obligations under Applicable Data Protection Laws in their Processing of Personal Data, including but not limited to the obligations set forth in the applicable sections of this DPA.

### 1.2 Description of Data Transfers

Unless otherwise specified in the Agreement, the following descriptions apply to data transfers under this DPA.

1.2.1 Categories of Data Subjects whose Personal Data may be transferred under this DPA include: consumers of online content.

1.2.2 Categories of Personal Data that may be transferred under this DPA include:

1.2.2.1 Unique online identifiers. These are persistent identifiers that help identify Data Subjects' online activity and interests across devices and over time, such as their IP addresses, cookie identifiers, mobile advertising identifiers, or connected television identifiers. Certain data partners may also disclose additional unique online identifiers, such as hashed email addresses or hashed phone numbers.

1.2.2.2 Online and offline activity and interests (including inferences). This includes information about Data Subjects' online activity and interests, such as their browsing history and online behavior. Certain data partners may also disclose additional information about Data Subjects' offline activity and interests, such as their purchase history, or information derived or inferred from their online and offline activity and interests, such as their likelihood

to be interested in buying a particular product, using a particular service, or visiting a particular website.

1.2.2.3 Non-precise geolocation information. This typically is information about Data Subjects' or Data Subjects' devices' non-precise location, such as their country, region, metro, zip or postal code, or non-precise (zip-code level) geographic coordinates, typically as inferred from their IP address.

1.2.2.4 Browser, device, and service information. This is information about the devices Data Subjects are using to engage online, such as their browser or device type (e.g., Google Chrome, iPhone), screen dimensions, operating system, and preferred language.

1.2.2.5 Ad reporting and delivery information. This is information about the advertisements Data Subjects have been served and how Data Subjects interacted with them, such as the size and format of advertisements they were served and whether they clicked on them.

1.2.3 Categories of Sensitive or Special Category Personal Data that may be transferred under this DPA include: none; the parties do not anticipate any Sensitive or Special Category Personal Data transfers.

1.2.4 The frequency of Personal Data transfers under this DPA is as often Company uses the OpenX services described in the Agreement, for example by sending data to OpenX or receiving data from OpenX to facilitate online advertising services.

1.2.5 The nature and purpose of the Personal Data Processing under this DPA is Processing to facilitate online advertising services, as specified in greater detail in the Agreement. Unless the Recipient is acting in the capacity of a Processor or Service Provider, the parties understand and agree that this may include Processing, including Sales or Shares of Personal Data, to facilitate Targeted Advertising or Cross-Context Behavioral Advertising.

1.2.6 The duration of the Personal Data Processing under this DPA will be for as long as Discloser transfers Personal Data to Recipient.

1.2.7 The retention period for Personal Data Processed under this DPA will be in accordance with the Recipient's retention policies, provided that such policies are consistent with Applicable Data Protection Laws and the terms of this DPA.

### 1.3 Disclosing Personal Data

Unless otherwise specified in the Agreement, where acting as a Discloser, each party will be responsible for the following under this DPA.

1.3.1 Limiting disclosure for Permitted Purposes. Only disclose Personal Data for one or more defined and lawful purposes that are consistent with the terms of the Agreement (the **"Permitted Purposes"**).

1.3.2 Providing required notices. Where required under Applicable Data Protection Laws, ensure that a notice has been made available and will continue to be accessible to the relevant Data Subject(s) informing them that their Personal Data will be disclosed to the Recipient, or to a category of third party describing the Recipient, for the Permitted Purposes and providing other information, as required by Applicable Data Protection Laws.

1.3.2.1 Where applicable, this notice must inform the relevant Data Subject(s) that their Personal Data may be disclosed via cookie or pixel syncing and related technologies and used for the Permitted Purposes, including being Sold or Shared for purposes of facilitating Targeted or Cross-Context Behavioral Advertising.

1.3.3 Providing required opt-out opportunities. Where required under Applicable Data Protection Laws, ensure that the relevant Data Subject(s) has been provided, prior to disclosing any Personal Data, with an easily accessible opportunity to opt-out of relevant Processing, including Selling or Sharing of their Personal Data for purposes of facilitating Targeted or Cross-Context Behavioral Advertising, including by providing the opportunity for the relevant Data Subject(s) to opt-out via industry standard global privacy controls.

1.3.3.1 When the Discloser is not able to provide required notice and/or an opportunity to opt-out to the relevant Data Subject(s), or when the Data Subject(s) elects to opt-out of such Processing activities, Discloser must either (i) not disclose the relevant Data Subjects' Personal Data to Recipient, or (ii) pass to Recipient an industry standard opt-out signal (i.e., a signal endorsed by the Interactive Advertising Bureau ("**IAB**") and transmitted via the IAB OpenRTB specification to document an opt-out) (an "**Opt-Out Signal**") sufficient to confirm the Data Subjects' opt-out.

1.3.4 Collecting required consents. Where required under Applicable Data Protection Laws, obtain, prior to disclosing any Personal Data, any necessary consents, permissions, or authorizations required to permit the Recipient to freely Process the Personal Data for the Permitted Purposes (the "**Required Consents**"), and pass to Recipient an industry standard consent signal (i.e., a signal endorsed by the IAB and transmitted via the IAB OpenRTB specification to document Required Consents) (a "**Consent Signal**") sufficient to confirm the Required Consents.

1.3.5 Minimizing Personal Data disclosed. Only disclose Personal Data as necessary to facilitate the Permitted Purposes, and prohibit the disclosure of the following:

1.3.5.1 Names, email addresses, national identification numbers, or other information that directly identifies a specific natural person and that has not been hashed, encrypted, or otherwise pseudonymized ("**Directly Identifiable Personal Data**");

1.3.5.2 Personal Data from a Data Subject that has not been provided with the notices described in Section 1.3.2, given the required opt-out opportunities described Section 1.3.3, or provided the Required Consents described in Section 1.3.4;

1.3.5.3 Personal Data related to a Data Subject it knows or should know to be a minor under the age of 18;

1.3.5.4 Geolocation data sufficiently precise to locate a specific individual or device; and

1.3.5.5 Sensitive or Special Categories of Personal Data, or other Personal Data that is created or inferred from Sensitive or Special Categories of Personal Data.

1.3.5.6 Notwithstanding the forgoing, to the extent any of the prohibited categories of Personal Data identified in this Section 1.3.5 are inadvertently disclosed, the Discloser remains solely responsible for the classification of such Personal Data, the legal basis for its Processing, and ensuring that it has collected any Required Consents, and passed any required Consent Signals or other compliance signals, to permit the Recipient to freely Process the Personal Data for the Permitted Purposes prior to disclosing such Personal Data.

## 1.4 Receiving Personal Data

Unless otherwise specified in the Agreement, where acting as a Recipient, each party will be responsible for the following under this DPA.

1.4.1 Limiting Processing for Permitted Purposes. Only Process Personal Data in a manner that is consistent with the Permitted Purposes and the notices described in Section 1.4.2, unless required to comply with a requirement of Applicable Data Protection Laws.

1.4.2 Providing required notices. Where required under Applicable Data Protection Laws, ensure that a notice has been made available and will continue to be accessible to the relevant Data Subject(s) informing them about how their Personal Data will be Processed and providing other information, as required by Applicable Data Protection Laws.

1.4.2.1 Where applicable, this notice must inform the relevant Data Subject(s) that their Personal Data may be Processed via cookie or pixel syncing and related technologies and used for the

Permitted Purposes, including being Sold or Shared for purposes of facilitating Targeted or Cross-Context Behavioral Advertising.

1.4.3 Honoring Opt-Out Signals and Consent Signals. Where required under Applicable Data Protection Laws, ensure that its Processing activities are consistent with the Opt-Out Signals and Consent Signals received from the Discloser, including by:

1.4.3.1 restricting its Processing activities when it receives an Opt-Out Signal by: (i) not engaging in Targeted or Cross-Context Behavioral Advertising; (ii) passing the Opt-Out Signal to any downstream recipients of Personal Data and imposing Processing restrictions substantially similar to those in this Section 1.4.3 on such downstream recipients; (iii) not otherwise Selling Personal Data received with the Opt-Out Signal; and (iv) acting in the capacity of a Processor or Service Provider with respect to the Personal Data received with the Opt-Out Signal, including by complying with the obligations in Section 3.1 of this DPA, to the extent applicable; and

1.4.3.2 restricting its Processing activities when it receives a Consent Signal by: (i) not engaging in any Processing that is not consistent with the Required Consents documented within the Consent Signal; and (ii) passing the Consent Signal to any downstream recipients of Personal Data and imposing Processing restrictions substantially similar to those in this Section 1.4.3 on such downstream recipients.

1.4.4 Prohibiting re-identification. Prohibit any action or attempt by Recipient or any third party to associate pseudonymous Personal Data provided by Discloser with Directly Identifiable Personal Data, or otherwise use such Personal Data to identify a natural person.

1.4.5 Restricting downstream disclosure.

1.4.5.1 Only disclose, transfer, Share, or Sell Personal Data to third parties subject to Processing restrictions substantially similar to those set forth in this Section 1.4 and otherwise consistent with Applicable Data Protection Laws.

1.4.5.2 Not disclose, transfer, Share, or Sell Personal Data to any governmental authority, regulatory body, or law enforcement entity except as required to comply with a valid and binding court order, subpoena, or other lawful request under Applicable Law, in which case disclosure should be limited to that which is necessary to comply with the lawful request.

1.4.6 Limiting retention of Personal Data. Process Personal Data only for as long as is reasonably necessary to carry out the Permitted Purposes, unless required to comply with a requirement of Applicable Data Protection Laws.

1.4.7 Maintaining the security of Personal Data. Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, and risks of varying likelihoods and severity to the rights and freedoms of Data Subjects, have in place appropriate technical, administrative, and organizational security measures to protect the Personal Data against Personal Data Breach, including at minimum the measures described in Section 6.

1.4.8 Permitting Discloser remediations. Allow the Discloser the right, upon prior notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by Recipient, including by requiring Recipient to cease the unauthorized Processing and to implement reasonable remediation measures.

1.4.9 Assisting with Discloser diligence. Allow the Discloser to take reasonable and appropriate steps to help to ensure that the Recipient's Processing of Personal Data is consistent with the Discloser's obligations under Applicable Data Protection Laws, including by (i) promptly responding to Discloser's reasonable diligence requests, (ii) providing reasonable assistance to enable Discloser to conduct data protection or privacy impact assessments and prior consultations with Supervisory Authorities as may be required by Applicable Data Protection Laws, and (iii) notifying Discloser if it makes a determination that it can no longer meet its obligations under this DPA or Applicable Data Protection Laws.

## 1.5 Responding to Personal Data Breaches

Unless otherwise specified in the Agreement, in the event of a Personal Data Breach involving Personal Data the Recipient knows or should know to have been received from the Discloser, each party will be responsible for the following under this DPA.

1.5.1 Reasonable investigation and remediation. Upon becoming aware of a Personal Data Breach, the Recipient will promptly (i) investigate the Personal Data Breach; and (ii) take reasonable steps to remediate and mitigate the effects of the Personal Data Breach.

1.5.2 Notification to Discloser. The Recipient will notify the Discloser without undue delay, and within any statutorily prescribed time periods, of the Personal Data Breach and provide any information about the Personal Data Breach as reasonably requested by the Discloser, provided that Recipient will not be required to provide information that would compromise the security of its systems or other clients or customers.

1.5.3 Notification to Supervisory Authorities or Data Subjects. Each party will cooperate with the other, to the extent reasonably requested, in relation to any notifications to Supervisory Authorities or to Data Subjects that are required following a Personal Data Breach. Neither party will provide any notices that name or implicate the other without prior written notice to the other unless required under Applicable Data Protection Laws.

1.5.4 Cooperating on obligations. Each party will cooperate and assist the other to comply with obligations regarding Personal Data Breaches arising under Applicable Data Protection Laws taking into account the nature of processing and the information available to the party.

### 1.6 Responding to Data Subject Requests

Unless otherwise specified in the Agreement, the parties will reasonably cooperate as needed and reasonably requested to respond to Data Subject Requests and any other communications from Data Subjects that relate to any Processing of Personal Data governed by this DPA.

### 1.7 Responding to Inquiries from Supervisory Authorities

Unless otherwise specified in the Agreement, the parties will reasonably cooperate as needed and reasonably requested to respond to any communication from any Supervisory Authority concerning any Processing of Personal Data governed by this DPA or compliance with Applicable Data Protection Laws.

### 1.8 Engaging Sub-Processors

Unless otherwise specified in the Agreement, the Recipient may engage one or more other entities to Process Personal Data on its behalf (each, a "**Subprocessor**"), provided that it engages such Subprocessors pursuant to written contracts that contain restrictions on processing that are substantially similar to the terms of this DPA.

---

## 2. Additional Terms Governing Transfers under EU and UK Data Protection Laws

Unless otherwise specified in the Agreement, the following additional terms govern transfers of EU and UK Personal Data under EU and UK Data Protection Laws. For the avoidance of doubt, the General Terms apply regardless of whether the Personal Data is Subject to EU and UK Data Protection Laws.

### 2.1 TCF compliance

2.1.1 The Discloser will comply with the then-current IAB Standard Terms and Conditions for Internet Advertising, including where applicable the IAB European Transparency & Consent Framework Policies (the "**TCF**") and the IAB's Global Privacy Protocol (the "**GPP**"), and where necessary shall obtain a valid, specific, and informed consent for the processing by the Recipient and any third parties to whom Recipient may disclose the Personal Data. Recipient will make available to Discloser a then-current list of any third parties to whom it may disclose the Personal Data upon request.

2.1.2 Where applicable, the Discloser will provide a valid TCF Consent Signal in connection with all Personal Data transferred to the Recipient. This consent must name Recipient as a party that Processes Personal Data obtained from

Discloser for the purposes for which the Recipient is registered under the TCF from time to time.

**2.2 OpenX as Recipient of EU and UK Personal Data**

2.2.1 The parties agree that, where OpenX is the Recipient of EU and UK Personal Data, OpenX Poland sp. z o.o. ("**OpenX Poland**") is the OpenX entity that is the Controller or Processor (as applicable) of such EU and UK Personal Data.

2.2.2 Because OpenX Poland is established in a Member State of the European Union, transfers of EU and UK Personal Data to OpenX Poland do not constitute Restricted Transfers within the meaning of this DPA.

2.2.3 OpenX Poland is responsible for any onward transfer of EU and UK Personal Data outside of the EEA, Switzerland, or UK. Where OpenX Poland is required to enter into appropriate data transfer terms related to such onward transfers, then OpenX represents that it has ensured that appropriate and adequate data transfer measures are in place, including by participating in the EU-U.S. Data Privacy Framework (or the UK or Swiss equivalent and/or any successor mechanism), entering into Standard Contractual Clauses, or entering into binding corporate rules.

**2.3 Company as Recipient of EU and UK Personal Data**

2.3.1 The parties agree that, where Company is the Recipient of EU and UK Personal Data, Company or an Affiliate designated by Company is the Company entity that is the Controller or Processor (as applicable) of such EU and UK Personal Data (the "**Company Controller**").

2.3.2 The Company Controller is responsible for any onward transfer of EU and UK Personal Data outside of the EEA, Switzerland, or UK. Where the Company Controller is required to enter into appropriate data transfer terms related to such onward transfers, then Company represents that it has ensured that appropriate and adequate data transfer measures are in place.

**2.4 Restricted Transfers**

2.4.1 To the extent that any transfers of EU and UK Personal Data from Discloser to Recipient may constitute a Restricted Transfer under this DPA, the parties agree that the following terms will apply.

2.4.2 This Section of 2.4 has been entered into by the parties for the purposes of complying with EU and UK Data Protection Laws for the transfer of EU and UK Personal Data to Recipients established in third countries which do not ensure an adequate level of data protection.

2.4.3 The Standard Contractual Clauses are incorporated by reference and form part of this DPA with the roles of the parties being identified in the Agreement and the parties' signature and dating of the Agreement being deemed to be the signature and dating of the Standard Contractual Clauses. The applicable Module(s) of the Standard Contractual Clauses shall be

determined as follows: Module One (Controller-Controller) shall apply where both parties act as independent Controllers with respect to the relevant transfer; Module Two (Controller-to-Processor) shall apply were Discloser acts as a Controller and Recipient acts as a Processor with respect to the relevant transfer. If Recipient participates in the EU-U.S. Data Privacy Framework (or UK or Swiss equivalent or any successor mechanism), transfers may alternatively rely on such Framework to the extent applicable.

2.4.4 Where the transfer of EU and UK Personal Data to Recipient by Discloser would be a Restricted Transfer, and where the parties are relying on the Standard Contractual Clauses as the transfer mechanism, the parties agree to comply with the obligations set out in the Standard Contractual Clauses as though they were set out in full in this DPA, with Discloser as the 'data exporter' and Recipient as the 'data importer' for the purposes of the Standard Contractual Clauses. Except as otherwise indicated in this Section 2.4, the information in this DPA, together with the information in the Agreement, sets out the details of the parties as required by the Standard Contractual Clauses and the Annexes to the Standard Contractual Clauses.

2.4.5 For the purposes of Clause 9(a) of the Standard Contractual Clauses, option 2 (general written authorisation for sub-processors) shall apply. The parties have agreed to the list of sub-processors specified in Clause 3.5. The time period for notifying the data exporter of any intended changes to the list of sub-processors shall be 60 days.

2.4.6 For the purposes of Clauses 17 and 18 of the Standard Contractual Clauses, the governing law and choice of forum shall be the law and courts of the EU Member State in which the Discloser is established (or, if not established in the EU, Ireland). Where OpenX is the Discloser, the governing law will be the laws of Poland and the choice of forum will be the courts of Poland.

2.4.7 In the event of any conflict or inconsistency between the provisions of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will govern.

---

## 3. Additional Terms Governing Controller to Processor and Business to Service Provider Data Transfers

Unless otherwise specified in the Agreement, the following additional terms govern transfers of Personal Data where the Discloser is a Controller or Business in relation to the Personal Data being disclosed and the Recipient is a Processor or Service Provider. For the avoidance of doubt, the General Terms apply regardless of the status of the Recipient.

### 3.1 Additional Processing Restrictions on Recipient

Unless otherwise specified in the Agreement, where acting as a Recipient, each party will be responsible for the following when acting as a Processor or Service Provider under this DPA.

3.1.1 Cease Processing of, and delete or return to the Discloser, all Personal Data Processed under this DPA upon the earlier of (i) the termination of the Agreement or (ii) the end of the services provided by Recipient, provided that Recipient may retain Personal Data where and to the extent required to fulfill a legal obligation.

3.1.2 Only Process Personal Data in a manner that is consistent with the Permitted Purposes, the notices described in Section 1.4.2, and the written lawful instructions provided by the Discloser, unless required to comply with a requirement of Applicable Data Protection Laws, and notify the Discloser without undue delay if, in its opinion, an instruction provided by the Discloser infringes Applicable Data Protection Laws.

3.1.3 For the avoidance of doubt, the Recipient will not (i) Process the Personal Data outside of the direct business relationship with the Discloser related to the Permitted Purposes; (ii) Process the Personal Data for any purpose other than performing the Processing instructed by Discloser related to the Permitted Purposes or as otherwise permitted by Applicable Data Protection Laws; (iii) Sell the Personal Data or Share the Personal Data for Targeted or Cross-Context Behavioral Advertising; or (iv) combine the Personal Data with Personal Data received from another person or persons except as directed by Discloser and permitted for a Processor or Service Provider under Applicable Data Protection Laws.

3.1.4 The Recipient certifies that it understands the restrictions in this Section 3.1.

### 3.2 Additional Instructions for Responding to Personal Data Breaches

Unless otherwise specified in the Agreement, where acting as a Processor or Service Provider under this DPA, the Recipient will: (i) notify the Discloser of any Personal Data Breach involving Personal Data it knows or should know was received from Discloser within 72 hours; and (ii) not notify Supervisory Authorities or Data Subjects of the Personal Data Breach without the Discloser's prior written authorization, unless required by Applicable Data Protection Laws.

### 3.3 Additional Restrictions on Responding to Data Subject Requests

Unless otherwise specified in the Agreement, where acting as a Processor or Service Provider under this DPA, the Recipient will notify the Discloser in the event it receives a Data Subject Request that involves Personal Data the Recipient knows or should know was provided by the Discloser. The Recipient will provide such information and assistance as may be commercially reasonable and necessary to allow the Discloser to comply with its obligations under Applicable Data Protection Laws to respond to such Data Subject Requests.

### 3.4 Additional Diligence Assistance

Unless otherwise specified in the Agreement, where the Recipient is acting as a Processor or Service Provider under this DPA, the Discloser may request in writing, no more than once per year, that the Recipient assess its compliance with Applicable Data Protection Laws as a Processor or Service Provider and with this DPA, and the Recipient will make available to Discloser all information reasonably necessary to demonstrate such compliance.

3.4.1 To facilitate compliance with this Section 3.4, the Discloser may arrange, or may ask the Recipient to arrange for a qualified and independent third party to conduct such an assessment so long as (i) the third party uses an appropriate and accepted control standard or framework and assessment procedure; and (ii) the report of such assessment, or a reasonably sufficient summary thereof, is provided to the Discloser upon request.

3.4.2 If any such assessment reveals any material noncompliance with the Recipient's obligations under this DPA or the Agreement, the Recipient will remedy (and demonstrate to the Discloser that it has remedied) such noncompliance within 30 days. The Discloser may cease sending Personal Data to the Recipient until the noncompliance has been remedied, and may terminate the Agreement if a remedy is not possible or is not achieved within 30 days.

### 3.5 Additional Restrictions on Subprocessors

Unless otherwise specified in the Agreement, where acting as a Processor or Service Provider under this DPA, the Recipient will provide the Discloser with advance notice of any use of a Subprocessor(s) and provide the Discloser with an opportunity to object to the engagement of the Subprocessor(s). Where OpenX is the Recipient, the Discloser agrees that it has received advance notice and assents to the engagement of the Subprocessors listed here.

---

## 4. Representations Related to U.S. Data Sharing Rules

To the extent that Personal Data subject to the U.S. Privacy Laws or U.S. Data Sharing Rules will be Processed under this DPA, the Recipient represents to the Discloser that: (i) it is not a "covered person" or a "foreign entity" as defined under the U.S. Data Sharing Rules; (ii) it will not share or otherwise enable access to Personal Data subject to U.S. State Privacy Laws or any other data that is subject to the U.S. Data Sharing Rules with any covered persons or foreign entities as defined under the U.S. Data Sharing Rules; (iii) if it further discloses Personal Data subject to U.S. Privacy Laws or any other data subject to the U.S. Data Sharing Rules to any third party, it will impose written terms requiring that third party to also comply with the U.S. Data Sharing Rules; (iv) it will not otherwise violate the U.S. Data Sharing Rules; and (v) it will promptly inform the Discloser if it can no longer comply with this provision, and will promptly report to the Discloser any known or suspected violations of the U.S. Data Sharing Rules.

## 5. Definitions

**5.1** In this DPA, the following terms will have the meanings set out below:

5.1.1 **"Business**", **"Consumer"**, **"Controller"**, **"Cross-Context Behavioral Advertising"**, **"Data Subject"**, **"Personal Data"**, **"Process/Processing"**, **"Processor"**, **"Sell"**, **"Sensitive Personal Data"**, **"Service Provider"**, **"Share"**, **"Special Categories of Personal Data"**, **"Targeted Advertising"**, **"Third Party"**, and related or equivalent terms will have the same meaning as defined in Applicable Data Protection Laws;

5.1.2 **"Affiliate"** means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership with either OpenX or Company (as the context allows), 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;

5.1.3 **"Applicable Data Protection Laws"** means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including but not limited to, where applicable, (i) EU and UK Data Protection Laws and (ii) U.S. Privacy Laws.

5.1.4 **"CCPA"** means the California Consumer Privacy Act, as amended by the California Privacy Rights Act and as otherwise amended from time to time, including its implementing regulations;

5.1.5 **"Data Subject Request"** means a request from a Data Subject to exercise any right under Applicable Data Protection Laws;

5.1.6 **"Discloser"** means the party or its Affiliate disclosing Personal Data to the other party or its Affiliate under this DPA.

5.1.7 **"EEA"** means the European Economic Area, including but not limited to the European Union ("**EU**");

5.1.8 **"EU and UK Data Protection Laws"** means (i) all EU, Swiss, or UK regulations applicable to the processing of Personal Data including but not limited to the GDPR, the UK GDPR, and the FADP, (ii) the national laws of each EEA member state, Switzerland, and the UK implementing any EU, Swiss, or UK directive applicable to the Processing of Personal Data (such as Directive 2002/58/EC), and (iii) any other legislation and/or regulation implementing or made pursuant to the laws and regulations described in (i) and (ii), 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 EU, Swiss, or UK jurisdiction; in each case, as may be amended, superseded or replaced from time to time;

5.1.9 "**EU or UK Personal Data**" means any Personal Data that Discloser transfers to Recipient, to the extent such Personal Data is related to residents of the EEA, Switzerland, or UK, or the disclosure of such Personal Data is otherwise subject to EU and UK Data Protection Laws;

5.1.10 **"FADP"** means the Swiss Federal Act on Data Protection;

5.1.11 **"GDPR"** means Regulation (EU) 2016/679;

5.1.12 **"Personal Data Breach"** means any known or reasonably believed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data subject to this DPA.

5.1.13 **"Recipient"** means the party or its Affiliate receiving Personal Data from the other party or its Affiliate under this DPA.

5.1.14 **"Restricted Transfer"** means any transfer of Personal Data which, absent the incorporation into this DPA of the Standard Contractual Clauses, would breach EU and UK Data Protection Laws;

5.1.15 **"Standard Contractual Clauses"** means:

a. With respect to Personal Data subject to the GDPR, 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 modules one and two of such clauses and not including any clauses marked as optional, and annexes to the standard contractual clauses as set out in Section 7 of this DPA ( the "**EU Standard Contractual Clauses**");
b. With respect to Personal Data subject to the FADP, the EU Standard Contractual Clauses, provided that: (i) any references in the clauses to the GDPR shall refer to the FADP; (ii) the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the EU Standard Contractual Clauses; and (iii) the supervisory authority is the Swiss Federal Data Protection and Information Commissioner;
c. With respect to Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 and in force since 21 March 2022 but, as permitted by clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum so that: (i) the details of the parties in table 1 shall be as set out in Section 7 of this DPA (with no requirement for signature); (ii) for the purposes of table 2, the addendum shall be appended to the EU Standard Contractual Clauses (including the selection of modules and disapplication of optional clauses as noted above) and clause 2.4.5 above selects the option and timescales

for clause 9; and (iii) the appendix information listed in table 3 is set out in Section 7 of this DPA.

5.1.16 **"Supervisory Authority"** means, as applicable, (i) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; (ii) any similar regulatory authority responsible for the enforcement of Applicable Data Protection Laws in the UK upon its exit from the EU; (iii) any regulatory authority responsible for the enforcement of U.S. Privacy Laws; and (iv) any regulatory authority responsible for the enforcement of other Applicable Data Protection Laws.

5.1.17 **"U.K. GDPR"** means the GDPR as retained in United Kingdom ("**UK**") law pursuant to the EU (Withdrawal) Act 2018 and as amended from time to time.

5.1.18 **"U.S. Data Sharing Rules"** means, as applicable, (i) the DOJ Rule 28 CFR Part 202 implementing Executive Order 14117 Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern; and (ii) H.R. 7520 Protecting Americans' Data from Foreign Adversaries Act of 2024.

5.1.19 **"U.S. Privacy Laws"** means any United States ("**U.S.**") federal or state law governing or applicable to the Processing of Personal Data (or equivalent terms) of U.S. persons, including without limitation (i) the Federal Trade Commission ("**FTC**") Act; (ii) the Children's Online Privacy Protection Act ("**COPPA**"); (iii) the U.S. Data Sharing Rules; (iv) any state law governing notification to Consumers and Supervisory Authorities following an applicable Personal Data Breach; (v) the CCPA; (vi) analogous federal or state laws that are now or may be entered into force, as applicable to the parties, including but not limited to applicable privacy laws in force in Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, or Virginia; and (vii) the Washington My Health My Data Act or analogous federal or state laws.

---

## 6. Data Security Addendum

Unless otherwise specified in the Agreement, where acting as a Recipient, each party will be responsible for the following data security obligations under this DPA.

### 6.1 General security obligations

Recipient will implement appropriate technical and organizational measures to ensure a level of security appropriate to the Processing and will implement and maintain a written, risk-based information security program designed to protect Personal Data against any Personal Data Breach. Such program shall include administrative, technical, and physical safeguards appropriate to:

6.1.1 the nature of the Personal Data processed;
6.1.2 the volume and sensitivity of such Personal Data;

6.1.3 the state of the art;
6.1.4 the costs of implementation; and
6.1.5 the risks presented by the Processing.

Recipient may update or modify its security measures from time to time, provided that such modifications do not materially reduce the overall level of protection for Personal Data as set forth in this Section 6.

**6.2 Risk assessments**

Recipient will periodically assess reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Personal Data and shall implement safeguards designed to mitigate identified risks appropriate to its size, complexity, and Processing activities.

**6.3 Physical security and access controls**

Recipient will implement reasonable physical and logical access controls designed to:

6.3.1 limit access to Personal Data to authorized personnel who require such access for legitimate business purposes;
6.3.2 restrict physical access to facilities where Personal Data is processed or stored; and
6.3.3 maintain authentication and access management procedures appropriate to the nature of the Processing.

Access rights shall be reviewed periodically and revoked promptly when no longer required.

**6.4 Encryption and data transmission**

Recipient shall implement encryption or equivalent protective measures for Personal Data in transit over public networks and, where appropriate, at rest, taking into account industry standards and the sensitivity of the data.

**6.5 Business continuity and disaster recovery**

Recipient will maintain reasonable business continuity and disaster recovery measures designed to ensure the availability of Personal Data and restore access in a timely manner following a physical or technical incident.

**6.6 Security testing and monitoring**

Recipient will maintain a program designed to monitor the effectiveness of its security controls, which may include vulnerability assessments, security testing, or third-party audits, as appropriate to its size and risk profile.

Nothing in this Section requires Recipient to provide penetration test results or other confidential security documentation except as required by Applicable Data Protection Laws or as reasonably requested by Discloser in the event of a Personal Data Breach in accordance with Section 1.5 of this DPA.

### 6.7 Personnel security and training

Recipient will ensure that personnel with access to Personal Data are (i) subject to appropriate confidentiality obligations and (ii) provided with periodic training on information security and privacy responsibilities appropriate to their roles.

### 6.8 Change management

Recipient will maintain reasonable change management procedures designed to ensure that material modifications to systems affecting the security of Personal Data are appropriately reviewed and authorized.

### 6.9 Personal Data Breach management

Recipient will maintain written incident response procedures designed to detect, investigate, and remediate Personal Data Breaches. In the event of a Personal Data Breach, the parties will act in accordance with Section 1.5 of this DPA.

### 6.10 Insurance

Recipient shall maintain commercially reasonable levels of information security liability insurance consistent with industry standards for similarly situated companies and errors and omissions insurance appropriate to its size and risk profile.

---

## 7. Annexes to the EU SCCs and Appendices to the UK SCCs

**Annex I / Appendix 1:**

**A: LIST OF PARTIES**

**Data exporter(s):** *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name: **As set out in the Agreement**

Address: **As set out in the Agreement**

Contact person's name, position and contact details: **As set out in the Agreement**

Activities relevant to the data transferred under these Clauses: **As set out in the Agreement**

Signature and date: **As set out in the Agreement**

Role (controller/processor): **Controller**

**Data importer(s)**: *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: **as set out in the Agreement.**

Address: **as set out in the Agreement.**

Contact person's name, position and contact details: **As set out in the Agreement**

Activities relevant to the data transferred under these Clauses: **As set out in the Agreement**

Signature and date: **As set out in the Agreement**

Role (controller/processor): **Controller (in situations where Module 1 is applicable), Processor (in situations where Module 2 is applicable)**

**B: DESCRIPTION OF TRANSFER**

**MODULE ONE: CONTROLLER TO CONTROLLER**

**MODULE TWO: CONTROLLER TO PROCESSOR**

***Categories of data subjects whose personal data is transferred:***

As set out in Section 1.2.1 of this DPA

***Categories of personal data transferred:***

As set out in Section 1.2.2 of this DPA

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures***

N/A

***Frequency of transfer (e.g. whether on a one-off or continuous basis) (EU standard contractual clauses only):***

As set out in Section 1.2.4 of this DPA

***Nature of the processing/ processing operations:***

As set out in Section 1.2.5 of this DPA

***Purpose(s) of the data transfer and further processing (EU standard contractual clauses only):***

As set out in Section 1.2.5 of this DPA

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period (EU standard contractual clauses only):***

As set out in Sections 1.2.6 and 1.6.7 of this DPA

***For transfers to (sub-) processors, the subject matter, nature and duration of the processing (EU standard contractual clauses only):***

As set out in the in accordance with Section 3.5 of this DPA

**C: <u>COMPETENT SUPERVISORY AUTHORITY (EU standard contractual clauses only)</u>**

PUODO (Poland)

**Annex II/ Appendix 2: technical and organisational measures**

As set out in Section 6 (Data Security Addendum) of this DPA

---

## 8. Version History and Summary of Changes

| Version Date | Summary of Changes |
|---|---|
| May 1, 2026 | N/A - initial draft. Please note that this Global Data Processing Agreement has replaced the OpenX Data Processing Terms as of the Version Date. If you would like to review the OpenX Data Processing Terms, or have other questions about the applicability of this DPA to an Agreement, please contact legal@openx.com. |

---