

OpenX Data Processor Terms

Effective: March 13, 2025

These OpenX Data Processor Terms (“**Terms**”) apply in the limited circumstances where OpenX Technologies, Inc. (“**OpenX**”) has entered into an agreement with our supply or demand partners (“**You**”) to provide specific services to You as a “service provider” or “processor” (the “**Services**”). These Terms apply solely to such Services, and for such Services these Terms supersede the U.S. State Law Compliance section of OpenX’s Supply Policy and/or Demand Policy as applicable. All other provisions of the Supply Policy and/or Demand Policy continue to apply to You and OpenX except as otherwise explicitly provided in the agreement between You and OpenX.

General Compliance

- You and OpenX will comply with all applicable state data protection and data privacy laws and regulations of the United States, as they may be amended or replaced from time to time, including laws and regulations that are enacted or become effective after January 1, 2023 (together, “**U.S. State Privacy Laws**”). As used in these Terms, the term “personal data” includes “personal information” as each term is defined in U.S. State Privacy Laws, and “process” or “processing” has the same meaning as such term is defined in U.S. State Privacy Laws.
- OpenX will take steps to protect personal data You provide or make available to OpenX for OpenX to provide the Services (“**Your Personal Data**”) as required by U.S. State Privacy Laws. This will include OpenX (i) ensuring that each person processing Your Personal Data is subject to a duty of confidentiality, and (ii) maintaining administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of Your Personal Data. OpenX will comply with the terms of the OpenX Security Addendum appended hereto as Exhibit A, as it may be updated from time to time.
- With respect to Your Personal Data, You are a “business” or “controller” and OpenX is a “service provider” or “processor,” in each case as such terms are defined by U.S. State Privacy Laws. The nature and purpose of OpenX’s processing of Your Personal Data are set forth in the agreement describing the Services, and the duration of the processing will be for the duration of the Services. The types of Your Personal Data subject to the OpenX’s processing include online identifiers, commercial or transactions information, Internet or other network activity information, geolocation information, and other information that is linked to such information.

Processing Restrictions

- You provide or make available Your Personal Data for the limited purposes of OpenX providing the Services. OpenX agrees to process Your Personal Data solely to provide the Services and in accordance with the lawful instructions provided by You, except where otherwise required by law.
- For the avoidance of doubt, OpenX will not (i) collect, retain, use, or otherwise disclose Your Personal Data outside of the direct business relationship with You related to the Services; (ii) collect, retain, use, or otherwise disclose Your Personal Data for any purpose other than performing the processing instructed by You related to the Services or as otherwise permitted by U.S. State Privacy Laws; (iii) sell Your Personal Data or share Your Personal Data for targeted online advertising, except on Your behalf and as instructed by You to provide the Services; or (iv) combine Your Personal Data with personal data received from another person or persons except as permitted for a service provider or processor under U.S. State Privacy Laws. OpenX certifies that it understands the restrictions in this section.

Subprocessors

- You acknowledge and agree that OpenX may engage one or more other entities to process Your Personal Data (each a “**Subprocessor**”), including but not limited to the service providers listed

[here](#), so long as OpenX notifies You in advance of such engagement and provides You with the opportunity to object to the engagement of the Subprocessor. OpenX agrees to engage such Subprocessors pursuant to written contracts that contain restrictions on processing that are consistent with the terms of these Terms and, without limiting the foregoing, require the Subprocessor to meet the obligations of OpenX with respect to Your Personal Data.

Individual Rights Requests

- OpenX agrees to notify You in the event OpenX receives a request from, or on behalf of, any individual to exercise such individual's rights under U.S. State Privacy Laws with respect to Your Personal Data. OpenX will provide such information and assistance as may be commercially reasonable and necessary to allow You to comply with your obligations under U.S. State Privacy Laws to respond to such requests.

Information Sharing and Suspension of Processing

- You may take commercially reasonable and appropriate steps to ensure that OpenX processes Your Personal Data in a manner consistent with your obligations under U.S. State Privacy Laws. If OpenX determines that it can no longer meet its own obligations under U.S. State Privacy Laws as a service provider or processor, OpenX agrees to notify You of such determination. Upon such notice or in the event You otherwise become aware of unauthorized processing of Your Personal Data, You may take steps to stop and remediate the unauthorized processing by directing OpenX to temporarily suspend its processing of Your Personal Data until OpenX can meet its material obligations as a service provider or processor under U.S. State Privacy Laws.
- No more than annually, upon reasonable written request, OpenX will make available to You information necessary (i) to demonstrate OpenX's compliance with U.S. State Privacy Laws as a service provider or processor and these Terms or (ii) for You to conduct data protection assessments required by U.S. State Privacy Laws.

Assessments

- You may request in writing, no more than once per year, that OpenX assess its compliance with U.S. State Privacy Laws as a service provider or processor and with these Terms. You agree that OpenX may 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 is provided to You upon request.

Personal Data Breach

- OpenX will notify You in the event of a security incident involving Your Personal Data where such notification is required under U.S. State Privacy Laws ("Personal Data Breach"). OpenX will also promptly (i) investigate the Personal Data Breach and provide You with information about the Personal Data Breach; and (ii) take reasonable steps to remediate and mitigate the effects of the Personal Data Breach.

Deletion

- At the end of OpenX's provision of the Services, You agree that OpenX will delete Your Personal Data consistent with OpenX's data retention policies, unless OpenX is required by law to retain Your Personal Data.

Exhibit A

OpenX Data Security Addendum

This Data Security Addendum (the “**Addendum**”) describes OpenX’s information security guidelines for maintaining security controls designed to protect against any accidental, unauthorized or unlawful destruction, loss, alteration, disclosure of data. This Addendum applies in the limited circumstances where OpenX has entered into an agreement with a supply or demand partner (“**Customer**” or “**You**”) to provide specific services to You as a “service provider” or “processor” (the “**OpenX Services**”). Additional security features may be described in the agreement between You and OpenX (“**Agreement**”) or the Terms of Service governing your use of the OpenX Services. Unless otherwise specified herein, the terms of your Agreement with OpenX supersede the terms of this Addendum and will continue to apply to You and OpenX. OpenX’s privacy policies (which apply to personal data collected from business partners, end users, and visitors to our website) are separate from this Addendum and are available for reference via our Privacy Center: <https://www.openx.com/privacy-center/>.

OpenX may update this Addendum from time to time to document changes in security policies for the OpenX Services. OpenX will, upon request, certify to its compliance with this Addendum.

1. Overview of OpenX’s Data Security Program

OpenX has a risk-based data security program (the “**Data Security Program**”) designed to ensure the OpenX Services are delivered in a secure manner and to protect the OpenX Services and related OpenX systems from threats and data loss. This Addendum describes the Data Security Program as of the effective date listed above. OpenX regularly assesses and makes improvements to the Data Security Program based on evolving security threats, regulatory requirements, and industry standards.

OpenX uses commercially reasonable security measures to guard the computer systems and information storage facilities which safeguard against the unauthorized destruction, loss, alteration of or access to Customer data. OpenX encrypts information relating to, or capable of being associated, directly or indirectly, with a particular natural person or household (“**End User Data**”) using a cryptographic algorithm employing a key length of at least 256 bits (or a higher standard of encryption if commercially reasonable) when transmitted over networks outside OpenX or when in storage or being transported outside of OpenX’s systems or facilities, including in any any mobile device or equipment with information storage capabilities. OpenX does not transmit, directly or indirectly, End User Data to any individual or entity in any country to which the export of such information is prohibited by U.S. export laws or regulations.

2. Standards

OpenX follows and continues to implement industry-leading security practices such as ISO 27001. OpenX primarily operates on Google Cloud Platform (GCP) infrastructure and implements robust security controls to protect customer data. To ensure transparency and accountability, OpenX undergoes regular third-party audits to validate compliance with AICPA SOC 2.

For more information about OpenX's approach to privacy and data protection, please visit our [Privacy Center](#).

3. Risk Assessments

OpenX conducts, or retains independent third parties to conduct, information security risk assessments whenever there is a material change in OpenX's business or technology practices that may impact the privacy, confidentiality, security, integrity, or availability of Customer data. The risk assessments include identifying reasonably foreseeable internal and external risks to privacy, confidentiality, security, integrity, or availability; assessing the likelihood of, and potential damage that can be caused by, identified risks; assessing the adequacy of personnel training concerning the Data Security Program; updating the Data Security Program to limit and mitigate identified risks as appropriate and to address material changes in relevant technology, business practices, and personal information practices and regulations; and assessing whether the Data Security Program is operating in a manner reasonably calculated to prevent and mitigate unauthorized access to or disclosures of Customer data.

4. Physical Security and Access Controls

Physical access to locations hosting OpenX systems have limited access points, which are governed by access cards and monitored by surveillance cameras. Access to any physical computing equipment involved with data hosting is physically restricted.

Access to OpenX systems is limited to authorized OpenX personnel. OpenX further limits access to the GCP environment in which end user data is processed to personnel who require such access in order to perform their essential job functions. Access authorizations for OpenX personnel are reviewed at least annually and are rescinded promptly upon change of roles or separation from OpenX. OpenX maintains access logs to the GCP environment in which end user data is processed including date, time, and user identifier. Access logs are maintained in a secure area for a minimum of ninety (90) days.

Upon a Customer's written request, OpenX will promptly identify in writing all OpenX personnel who have been granted access to customer data as of the date of the request. OpenX may provide Customer with access logs as required to comply with governing law to assist in forensic analysis if there is a reasonable suspicion of inappropriate access.

5. Business Continuity and Disaster Recovery

Any facility housing OpenX Systems is designed to withstand adverse weather and other reasonably predictable natural conditions. All networking components and web and application servers are configured in a redundant configuration. OpenX maintains a business continuity and disaster recovery program. Policies and procedures are in place to provide the OpenX Services with minimal interruptions, including disaster recovery planning and testing capabilities; recovery site management; and standard backup and recovery procedures.

6. Penetration Testing

At least one time each year, OpenX retains an independent third party to conduct a penetration test of our infrastructure designed to detect any material security weaknesses in such infrastructure. OpenX uses a reputable third party that is certified by recognized industry standards as being qualified to perform such penetration testing. To the extent any material weakness is identified, OpenX takes appropriate action to remedy such weakness.

7. Employee Training

All OpenX personnel receive annual education on the importance of security, confidentiality, and privacy of Customer data; OpenX data security policies and practices; and the risks to OpenX and its customers associated with Security Incidents. OpenX implements measures designed to ensure that all personnel are sufficiently trained, qualified, and experienced to fulfill their functions under the Data Security Program and any other functions that might reasonably be expected to be carried out by the personnel responsible for safeguarding Customer data.

8. Change Management

OpenX maintains and continually enhances the OpenX Services. These enhancements may include changes in response to relevant technology and systems, unauthorized access to Customer data, and/or the discovery of material privacy or security vulnerabilities. Security controls, procedures, policies, and features may change or be added but will deliver a level of security protection that is not materially lower than that provided as of the Effective Date of this Addendum.

OpenX maintains a change management process with separation of duties and appropriate approvals required for modification to OpenX Systems, including patch management for the OpenX Services.

9. Incident Management

OpenX maintains an Incident Management Policy covering standard operational procedures and tactics to minimize the impact of incidents involving a compromise of security, potentially leading to accidental or unauthorized access to, or disclosure, alteration, or destruction of OpenX data or assets (“**Security Incidents**”). Security Incidents are classified according to

severity of impact, with high-severity incidents triggering root cause analysis and reviews to identify areas for long-term improvement.

OpenX has a dedicated security team (the “**Security Team**”) responsible for implementing and maintaining the Incident Management Policy. The Security Team is responsible for conducting the initial investigation following the reporting of a potential Security incident. Upon receiving notice of a potential Security incident, the Security Team will investigate the report, collect and preserve any evidence associated with the security issue, and aid in mitigation and remediation efforts to restore operations.

In the event of a Security Incident involving Customer data, OpenX will:

- a. notify Customer of such Security Incident by email or phone within 72 hours after OpenX has become aware of the Security Incident;
- b. start an investigation of the Security Incident;
- c. take all appropriate actions to remediate the effects of the Security Incident and mitigate any risks that may arise from the Security Incident;
- d. provide Customer with timely and ongoing reports on the outcome of its investigation including any risk to Customer data and the corrective action OpenX will take, or has taken, to respond to the Security Incident;
- e. ensure that all risks associated with such Security Incident are ultimately resolved within a timely manner following such Security Incident; and
- f. preserve all records and other evidence relating to the Security Incident.
- g. Customer may disclose the occurrence of a Security Incident involving End User Data in connection with legally required notice to Customer’s clients, employees or vendors; law enforcement agencies; or any other notice required by law (“**Notifications**”).
- h. OpenX shall cooperate in good faith with Customer in Customer’s handling of any Security Incident, including, without limitation any investigation, reporting, the timing and manner of any Notifications, or other obligations required by applicable law or regulation, or as otherwise required by Customer to respond to and mitigate any damages caused by the Security Incident. OpenX agrees to reimburse Customer for reasonable fines, costs and losses incurred in connection with a Security Incident

10. Insurance

OpenX maintains information security liability insurance and errors & omissions insurance covering liability for Security Incidents with coverage and limits commensurate with our size and risk profile.