DATA PROCESSING TERMS

These DATA PROCESSING TERMS (the “**Terms**”) shall apply for all ad serving by Extreme Reach, Inc. or its affiliates ("**Service Provider**" or “**XR**”) on any websites, applications, digital properties, CTV, OTT (collectively, “**Digital Property**”) owned, operated, controlled, or represented by you and/or your affiliates (“**PUBLISHER**”). Service Provider and PUBLISHER are collectively referred to as the “**Parties**” and individually as a “**Party**.”

These Terms shall apply where PUBLISHER sells or otherwise provides digital advertising inventory to certain advertisers (the “**Advertiser**”) for the placement of advertisements on its Digital Properties; and the Advertiser and/or its agencies have engaged Service Provider to serve digital advertisements and collect certain advertising campaign performance data on behalf of the Advertiser (the "**Services**"); and Advertiser places Service Provider’s pixels and/or other code or technology (the “**Pixel(s)**”) on Advertiser’s advertisements being served on the Digital Property to collect campaign performance data.

1. **Geography.** These standard terms are supplemented by the Attachments below for certain geographic regions and jurisdictions, as applicable. For jurisdictions other than the EU, Switzerland, and the UK, where the terms of Attachment 1, or the information therein, are sufficient to comply with such jurisdictions’ applicable data privacy laws, Attachment 1 shall apply. If the terms of an applicable Attachment conflict with the standard terms herein, the terms of the Attachment control for the applicable geographic region.

2. **Data Collection Services and Practices.** Service Provider may engage third-party service providers to assist in the delivery and optimization of advertisements. These third-party service providers may include pixels or other tracking technologies in the advertisements for the sole purpose of delivering, optimizing, and reporting on the performance of such advertisements. Service Provider represents and warrants that in connection with its use of Pixels on the Digital Property:

   a. Service Provider has entered into the necessary agreements with Advertiser or its agenc(ies) and has received the necessary consent and permission from Advertiser or its agencies to place its Pixels on the advertisements served on the Digital Property.
   b. The Pixels will only collect data from advertisements it serves and will not otherwise collect any data from the Digital Property.
   c. Agency, Advertiser, or Service Provider will include the Pixel in the creative for each advertisement provided to PUBLISHER. Prior to changing the scope or functionality of any such Pixels, Service Provider will provide PUBLISHER with information about any such changes.
   d. It will not permit or enable any Pixel to attach or redirect to third party tags, pixels, code or other tracking technologies that have not been placed directly on the Digital Property (“piggybacking”) without express permission from PUBLISHER.
   e. It will not resell or otherwise transfer any data it collects or receives from the Digital Property other than as permitted under these Terms, whether or not such data contains any personally identifiable information or personal information. This prohibition does not apply to any transfer of data to the applicable Advertiser or its agency in carrying out the Services.
   f. Data collected from the Pixel will be used solely to provide reports and other analytics to Advertiser or its agency regarding the performance of an advertisement or campaign. Service Provider will otherwise not use the data collected from the Pixel to serve targeted advertisements to the users of PUBLISHER’s Digital Property.
   g. Service Provider will promptly honor any requests it receives from users of PUBLISHER Digital Property to opt-out of data collection by Service Provider.
   h. It will not grant access to data collected or tracked by means of the Pixel on the Digital Property to any third party, except as directed by Advertiser or (a) on a need to know basis in order to provide specific services to Advertiser; (b) after conducting a reasonable investigation of such third party; and (c) upon entering a written agreement with such third party which contains obligations which are at least as restrictive as the foregoing.
   i. It will not use malicious code of any kind.
   j. It will notify PUBLISHER of any actual or suspected breaches of security or incidents related to PUBLISHER or its users within one (1) week of discovery of such incident (or earlier where legally required).

k. Without limiting any of the foregoing, Service Provider does and will comply with all applicable laws, rules, regulations, legal orders or decrees and similar promulgations.

l. Service Provider will employ commercially reasonable methodologies, technologies, and other means to prevent the introduction of, and will not intentionally introduce any software virus, worm, "back door," "Trojan Horse," or similar harmful, destructive, or disruptive code or device into the Pixels or any other materials or services provided by Service Provider or into the Digital Property.

m. Service Provider will destroy any data collected from the Digital Property no later than (2) years after the termination of Advertiser's contract, except where anonymized and aggregated for long-term benchmarking purposes.

n. Where Service Provider uses subprocessors to assist in providing the services, each subprocessor will be bound by data protection obligations equivalent to those set forth in these Terms. Upon request, Service Provider shall provide a current list of subprocessors engaged in processing the Publisher's data. Service Provider is liable for any acts or omissions of subprocessors that result in a breach of these Terms.

3. **PUBLISHER Representations and Warranties**. PUBLISHER represents and warrants:

   a. In carrying out its duties under this Terms and in operating its Digital Properties when any applicable advertising campaign is being run with Service Provider's Pixel(s) it will comply with all applicable laws, rules, regulations, legal orders or decrees and similar promulgations, including but not limited to any data privacy laws.

   b. It will not modify the Pixel, outside of updates required during trafficking, without prior notification to Service Provider and an opportunity for Service Provider to cure any potential defect in the Pixel, except as explicitly allowed herein.

4. **Removal of Pixels.** Publisher shall not remove or delete the Pixel except as allowed in this Section. Upon notice to Service Provider, PUBLISHER may remove from the Digital Property any Pixel or other code or material provided by Service Provider if (1) the advertising campaign for which such Pixel is being used has concluded, (2) at the request of the Advertiser or advertiser's agency, (3) to comply with any Law or to prevent a third party claim or lawsuit, (4) or to prevent any potential or actual damage to PUBLISHER's or any third party property.

5. **Compensation.** For the delivery of advertising content for Advertiser and/or its agencies to PUBLISHER, Service Provider will be compensated solely by the Advertiser or agencies that have retained Service Provider for this purpose, unless explicitly agreed otherwise with PUBLISHER. PUBLISHER will have no obligation to pay Service Provider for the delivery of ads to the Publisher's destination, unless such work is instructed by the Publisher. For any other services provided to or for PUBLISHER charges may apply, as agreed between Service Provider and PUBLISHER.

6. **Limitation of Liability.** IN NO EVENT WILL SERVICE PROVIDER OR PUBLISHER BE LIABLE FOR ANY INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF THESE TERMS (INCLUDING LOSS OF BUSINESS, REVENUE, PROFITS, USE, OR OTHER ECONOMIC ADVANTAGE), HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Disclaimer.** OTHER THAN AS EXPRESSLY STATED HEREIN, SERVICE PROVIDER MAKES NO FURTHER REPRESENTATIONS OR WARRANTIES, IMPLIED OR OTHERWISE.

8. **General Provisions.** These Terms constitute the entire understanding and agreement between Service Provider and Publisher with respect to the subject matter hereof and hereby supersedes all prior or contemporaneous writings or understandings unless there is a fully executed agreement between Service Provider and Publisher that covers data processing, in which case the terms of that agreement shall control. These Terms will be governed by the laws of the State of New York, United States of America, without regard to its choice of law principles, and any disputes arising hereunder will be submitted exclusively to the jurisdiction of a competent court in New York County in the State of New York (to which jurisdiction each Party hereby consents and waives any objections). If any provision of these Terms is determined to be illegal, unenforceable, or otherwise invalid by a court of competent jurisdiction, the remainder of these Terms will be unimpaired and remain in full force and effect.

ATTACHMENT 1 – EUROPEAN STANDARD CONTRACTUAL CLAUSES

*Where required by applicable data protection law, XR shall not Process or transfer any data (nor permit any data to be Processed or transferred) in a territory outside the EEA or UK (collectively, "****Europe****") unless it has taken such measures as are necessary to ensure that the transfer is in accordance with applicable data protection law. In particular, where such data is to be transferred outside of Europe to XR or another recipient who is not located in a territory which has been considered adequate under applicable data protection law, the European Standard Contractual Clauses (2021/914) ("****SCCs****") shall be incorporated into this Agreement as follows:*

1. *The legal entity named on this account shall be the 'data exporter' of such data;*
2. *XR shall be the 'data importer';*
3. *where XR receives and uses such data as a processor acting on behalf of Data Exporter, Module Two of the SCCs ("****C2P SCCs****") shall apply, as follows:*
    a. *Annex I of the C2P SCCs shall be deemed completed with the information set out in the relevant part of Annex 1 of this Attachment 1;*
    b. *Annex II of the C2P SCCs shall be deemed completed with the information set out in Annex 2 of this Attachment 1 ;*
    c. *Annex III of the C2P SCCs shall be deemed completed with the information set out in Annex 3 of this Attachment 1;*
    d. *Clause 7 (Docking Clause) of the C2P SCCs shall be included;*
    e. *Clause 9 of the C2P SCCs shall include OPTION 1 and the time period shall be 10 days;*
    f. *Clause 17 (Governing Law) of the C2P SCCs shall include OPTION 2 and shall refer to the Netherlands as the Member State; and*
    g. *Clause 18(b) of the C2P SCCs shall refer to the courts of the Netherlands;*
    h. *Data Exporter has the authority* to enter into SCCs with XR on Data Exporter Europe's behalf*; and*
    i. *in the event of any conflict between the SCCs and the provisions of this Agreement, the SCCs shall prevail.*
    j. *Annexes to the SCCs*

ANNEX 1: DETAILS OF PROCESSING

A. 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: the legal entity named on this account
Address: address of the Data Exporter listed in this account
Contact person's name, position and contact details: contact listed on this account
Activities relevant to the data transferred under these Clauses: Controller owns, operates, controls or represents various Digital Properties
Date: date of acceptance of these Terms
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: Extreme Reach, Inc.
Address: 66 Hudson Blvd E, Suite 2110, New York, NY 10001.
Contact person's name, position and contact details: Stephen K. Robinson, General Counsel and Chief Privacy Officer, srobinson@extremereach.com

Activities relevant to the data transferred under these Clauses: Serving ads on the Digital Properties and associated analytics and measurement of such advertisements
Date: date of acceptance of these Terms
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:
Consumers to whom advertising impressions are served.

Categories of personal data transferred:
Information related to a consumer's device, such as IP Address, and, where combined or linked to IP address, Device Type, Browser Type and User Agent strings.

Sensitive data transferred (if applicable):
N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Data are transferred on a continuous basis (on advertising creatives including the importer's technology)

Nature and purpose of the Processing

As Processor: The Data Importer acts as Processor in relation to the following activities: The personal data are transferred to enable the importer to deliver advertising to Data Exporter's properties. The data transferred is further processed in order to enable the importer to provide reports on the service to the exporter, its affiliates or its advertisers and agencies.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As Processor: XR shall retain the personal data for as long as it is required to provide the Services to the applicable Advertiser.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

See Annex 3. The duration of processing by sub-processors is concurrent with the importer's duration of processing as described in this Annex 1.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organizational measures implemented by XR (including any relevant certifications) to maintain an appropriate level of security taking into account the nature, scope, context and purposes of the processing, and the risks for the rights and freedoms of natural persons, are as follows:

Type of measure	**Terms**
Measures of pseudonymisation and encryption of personal data	Description of technical measures in place to prevent re-identification: XR has implemented data minimisation and privacy-by-design into its services development process to prevent personal data from being directly linkable to a data subject. If and when directly identifiable information were to be processed in connection with the services for addressability purposes, XR will ensure that industry standard cryptographic techniques are immediately applied to such data, including but not limited to, hashing, to help ensure data cannot be reidentified by unauthorised parties. Notwithstanding the foregoing IP addresses are commonly not hashed or otherwise anonymized. However, IP addresses are not shared with third parties without the explicit approval from the controller of this data. Advertising identifiers used by XR to track devices and deliver ads are not persistent; they are designed to deprecate within a reasonable time frame. When activating/monetizing audiences, sensitive or directly identifiable personal data is not processed, but instead segment codes/deal codes are exchanged by the parties. XR does not process any characteristics about data subjects in connection with the services. The data importer uses, as far as possible, encryption for the transport of personal data.
Measures for ensuring ongoing confidentiality of processing systems and services	Description of measures in place to secure information stored on systems: XR has implemented and maintains a written information security program aligned to industry practices, and has implemented measures to ensure the integrity, availability and security of personal information, including regular vulnerability scans and endpoint protection. XR limits the risk that personal data will be exposed by implementing a data retention schedule to systems that store personal data processed under the agreement.

	Personnel agree to confidentiality terms and must complete security and privacy training
Measures for ensuring ongoing integrity of processing systems and services	XR has implemented and maintains an information security program that contains services administrative, technical and physical safeguards appropriate to protect against anticipated threats to, confidentiality and integrity of, and the unauthorized or accidental destruction, loss, access, acquisition, alteration or use of, personal data, and that meets (i) reasonable security practices applicable to XR's industry; and (ii) any security requirements under the laws applicable to the company under applicable law. These safeguards include software development, change management, system access, physical security, and other policies and processes that protect the integrity of systems and services.
Measures for ensuring ongoing availability and resilience of processing systems and services	XR maintains personal data availability and resilience through a variety of technical, physical, and administrative measures. Examples of these measures include: fault tolerant infrastructure with geographically distinct availability zones for redundant data; secured and monitored operational sites; and, business continuity planning and testing, incident response and review, vendor review, and other related policies and processes.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	See response above. Further measures include regular backups and recovery testing.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	At least once annually, security measures relevant to the processing of personal data are reviewed and tested for alignment with industry best practices. Security compliance has been integrated into XR's product development practices, and XR privacy, security and engineering teams collaborate regularly to ensure those standards are kept up to date. XR engages with independent third parties to assess the effectiveness of security controls.
Measures for user identification and authorization	As part of XR's security program, XR maintains a System Access and Password policy that governs standards for user access, including user provisioning and authorization.

	XR has in place procedures that comply with applicable law to authenticate requests from data subjects who have submitted rights requests. XR has operational and technical controls in place to ensure access to systems that process personal data is only granted to authorized employees with a "need to know". XR has in place industry standard policies to ensure that unauthorized current and former personnel cannot improperly access systems that process personal data.
Measures for the protection of Data during storage	XR does not process any sensitive personal information related to the services, and personal data processing is limited in scope, pseudonymized (i.e., cookie ID, user agent information, etc.) and cannot be directly identified with a natural person by XR. Personal data is only stored for as long as necessary for Advertiser's legitimate business purposes and is subject to a data retention schedule. Personal data minimization procedures are in place with regard to personal data stored on XR's systems.
Measures for ensuring physical security of locations at which personal data are processed	Facilities involved in the processing of personal data are accessible only by authorized personnel. Technical controls are in place to secure processing facilities including access controls, two-factor authentication, firewalls, and anti-malware. Personal data can only be accessed by personnel who have a need-to-know and whose access to such information is required in order to deliver advertising services under the Agreement. XR provides personnel who access personal data with appropriate information security and data protection training. XR maintains appropriate physical security measures at each facility where personal data is processed, including authentication of all personnel who access data centers, IT equipment having physical barriers designed to prevent access by unauthorized individuals, and manned reception areas or logging of visitor entry/exit dates and times.
Measures for certification/assurance of processes and products	XR participates in industry certification and self-regulatory programs such as IAB TCF 2.0, and the IAB CCPA Compliance Framework. XR is accredited by the MRC for CTV, Desktop, Mobile, and App Impressions.
Measures for ensuring data minimisation	Procedures are embedded in the system development process to minimize personal data collected and processed by XR where legally required (e.g., truncation

	of IP address, stripping of personal data when an impression will be monetized using contextual ad-targeting, no data collection from unconsented or improperly consented impressions). XR has a dedicated technical privacy specialist whose role focus is at least partly dedicated to reviewing the implementation of data minimization across the organization.
Measures for ensuring accountability	XR performs a data mapping exercise that complies with Article 30 of GDPR and has created a record of processing activity to ascertain the scope of personal data processing activities performed by the organization. XR has implemented a privacy program that is appropriate to the scope and nature of personal data processed that includes a personal data breach policy, data protection and legitimate interest assessments (where appropriate), appointment of a data protection officer (DPO), and data protection controls such as privacy by design. The foregoing measures are regularly reviewed (at least once annually) and updated to ensure alignment with applicable law and industry standards.
Measures for allowing data portability and ensuring erasure	XR has implemented and maintains procedures to ensure data portability and erasure that comply with data protection laws. XR has designated a data protection leader who is responsible for ensuring all requests from data subjects are reviewed and documented, including requests for erasure and copies of personal data, and that data subject requests are carried out timely and in accordance with law.

General Principles

- XR shall implement and maintain an adequate and appropriate Security Incident management program.
- XR shall encrypt all Sensitive data, and any other data that is required to be encrypted under applicable laws or regulations, when transmitted electronically.
- XR shall ensure that all individuals that will have access to data undergo and successfully complete adequate and appropriate privacy and data security training prior to having access to data. Such training must be provided to all such individuals on at least an annual basis and comply with applicable laws, regulations and best industry practices.
- XR shall implement and maintain policies documenting the consequences for violations of XR's privacy and data security policies and escalation procedures for non-compliance with such policies.

ANNEX 3
SUB-PROCESSOR LIST

Sub-processors include, but are not limited to the following:

Name of Sub-Processor	Address of Sub-Processor	Contact person's name, position and contact details	Description of Processing by the Sub-Processor
AWS	**410 Terry Ave. N Seattle, WA 98109**		**Storage/hosting**