

Data Processing Agreement

This Data Processing Agreement (the "**Agreement**") is entered into by and between Adscend Media Inc, on behalf of itself and its Affiliates (collectively "**Adscend**") and you, as a customer of Adscend services, on behalf of Company and its Affiliates (collectively "**Company**"), each a "**Party**" and collectively, the "**Parties**". This Agreement supplements and all agreement and/ or insertion order entered into by and between Company and Adscend (the "**Initial Agreement**") for provision of certain services (the "**Services**"). Any undefined terms used herein shall have the meaning set forth in the Initial Agreement signed by the Parties.

Scope

Each of the Parties is or may be a Controller of certain Personal Data that it wishes to share with the other Party in connection with the performance of the Services. This Agreement only applies to the extent that Applicable Data Protection Law applies to the Processing of Personal Data under the Initial Agreement, including if (a) the Processing is in the context of activities of an establishment of either Party in the European Economic Area ("EEA") and/ or; (b) the Personal Data relates to Data Subjects who are in the EEA and the Processing relates to the offering to them of goods or services or the monitoring of their behavior in the EEA. The Parties shall ensure that they will Process such Personal Data solely for the purpose set forth in the Initial Agreement or as otherwise agreed in writing by the Parties. For Avoidance of doubt, this Agreement and the obligations hereunder do not apply to aggregated reporting or statistics a Party may provide to the other Party in connection with the provision of the Services hereunder.

Terms and Conditions

1. Definitions

In this Agreement, the following terms shall have the meanings set forth herein. Any undefined terms used herein shall have the meanings set forth in the Initial Agreement.

1. "Affiliates" means any entity which owns or controls, is owned by or controlled by or is under common control or ownership with one of the Parties.
2. "Applicable Data Protection Law" means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law) as may be amended or superseded from time to time.
3. "Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Process", "Personal Data Breach" and "Special Categories of Personal Data" shall have the meaning given in Applicable Data Protection Law.
4. "Controller Model Clauses" in relation to the Processing of Personal Data pursuant to this Agreement means the model clauses of the transfer of Personal Data to Controllers established in third countries approved by the European Commission from time to time, the approved version of which force at present is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004D0915>.
5. "EU Data Protection Law" means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("GDPR"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended and any legislation replacing its amended directive ("e-Privacy Law"); and (iii) any national data protections laws made under, pursuant to, replacing or succeeding (i) and (ii).
6. "ID" means a unique identifier (i) stored on an end-user's device, (ii) a unique identifier generated on the basis of device information, or (iii) a resettable advertising ID associated with a mobile device or an application.

7. "Initial Agreement" means any agreement and/ or insertion order signed between Adscend and Company where a Party engages in the Processing of Personal Data of Data Subjects.
8. "Relevant Privacy Requirements" means all (i) applicable SRPs, laws, governmental regulations and court or government agency orders and decrees relating in any manner to the collection, use or dissemination of information from or about users, user traffic or otherwise relating to privacy rights or with respect to the sending of marketing and advertising communications; (ii) posted privacy policies; and (iii) for mobile applications, the terms of service for the applicable mobile operating system.
9. "Security Incident" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For avoidance of doubt, any Personal Data Breach will comprise a Security Incident.
10. "Security Measures" means the technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
11. "SRPs" mean the rules and self-regulatory principles of the Network Advertising Initiative ("NAI"), Digital Advertising Alliance ("DAA"), and European Interactive Digital Advertising Alliance ("EDAA").
12. "Sub-Processors" means any entity which provides Processing services to a Party in furtherance of such Party's Processing on behalf of the other Party.

2. Relationship of the Parties

1. The Parties acknowledge that each Party is or may be a separate and independent Controller of the Personal Data which it discloses or receives for the Services under the Agreement. Each of the Parties doesn't and will not Process Personal Data which it discloses or receives under the Initial Agreement as joint controllers. Each Party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under the Applicable Data Protection Law.
2. It is agreed that where either Party receives a request from a Data Subject in respect of Personal Data controlled by the other Party, where relevant, such Party will direct the Data Subject to the other Party, as applicable, in order to enable the other Party to respond directly to the Data Subject's request.

3. Parties Personnel

Each Party will ensure that its access to the Personal Data is limited only to those personnel who require such access to perform the Services. Each Party shall impose contractual obligations upon its personnel engaged in the Processing of Personal Data, including relevant obligations regarding confidentiality, data protection and data security. Each Party shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements.

4. Sharing of Personal Data

1. In performing its obligations under the Initial Agreement, the Parties may provide Personal Data only for (i) the purposes set forth in the Initial Agreement or as (ii) otherwise agreed in writing by the Parties, provided such Processing strictly complies with (i) Applicable Data Protection Law, (ii) Relevant Privacy Requirements and (iii) its obligations under this Agreement (the "Permitted Purposes").
2. Each Party agrees to receive Personal Data from the other Party, provided that the Party providing the Personal Data strictly complies with the (i) Applicable Data Protection Law, (ii) Relevant Privacy Requirements and (iii) its obligations under this Agreement.
3. A Party shall not share any Personal Data with the other Party (i) that allows Data Subjects to be directly identified (for example by reference to their name and e-mail address); (ii) that contains any Special Categories of Personal Data, unless expressly agreed in writing or as

permitted under Applicable data Protection Law and/ or; (iii) that contains Personal Data relating to children under the age of 16 years.

4. Each Party will Process Personal Data that is disclosed to it by the other Party only for the Permitted Purposes in accordance with the provisions of this Agreement, save that may further process Personal Data for secondary purposes that are not incompatible with the Permitted Purposes, or which is otherwise agreed to by the Parties in writing, provided that such further Processing complies with Applicable Data Protection Laws.
5. Neither Party will disclose any Personal Data provided by the respective other Party to any third party without prior written consent of the other Party except: (i) as permitted or required pursuant to the Initial Agreement and this Agreement; or (ii) where required by applicable law.

5. Cross-Border Data Transfers

1. Where EU Data Protection Law applies, neither Party shall transfer any Personal Data received from the other Party (nor permit any Personal Data to be transferred) to a territory outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with the EU Data Protection Law. Such measures may include (without limitation) transferring of the Personal Data to a recipient in a country that the European Commission has decided provides adequate protection to personal data or to the recipient in the United States that has certified compliance with the EU-US Privacy Shield framework.
2. Except with regard to Personal Data transferred from one Party to the other Party in reliance on the transferring Party's Privacy Shield certification or other appropriate transfer mechanism specified in Section 4.1, the Standard Contractual Clauses contained in the Controller Model Clauses (the "Standard Contractual Clauses") shall apply to the receiving party's Processing of Personal Data in countries outside the EEA that do not provide an adequate level of data protection. To the extent that the Parties transfer Personal Data in reliance on the Standard Contractual Clauses, the Standard Contractual Clauses shall be completed and signed contemporaneously with the execution of this Agreement by the Parties.
3. Where and to the extent the Standard Contractual Clauses apply pursuant to this Section 5, if there is any conflict between this Agreement and the Standard Contractual Clauses shall prevail.

6. Privacy Obligations

1. Each Party shall maintain a publicly-accessible privacy policy on its mobile apps and websites that is available via a prominent link that satisfies disclosure requirements of Applicable Data Protection Law.
2. Each Party warrants and represents that it has provided Data Subjects with appropriate transparency regarding data collection and use and all required notices and obtained any and all consents or permissions necessary under e-Privacy Law. Where a Party in the initial Controller and it relies on consent as its legal basis to Process Personal Data (e.g., precise geolocation data), it shall ensure that it obtains a proper affirmative act of consent from Data Subjects in accordance with Data Protection Law and relevant Privacy requirements in order for itself and the other Party to identify the information disclosure requirements and each Party hereby permits the other Party to identify it in the other Party's privacy policy, and to provide a link to the other Party's privacy policy in its privacy policy.

7. Technical and Organizational Measures

Adscend and Company shall implement appropriate technical and organizational security measures to protect the Personal Data. In the event that Adscend or Company suffers a confirmed Security Incident, each Party shall cooperate in good faith to agree and action such measures as may be necessary to mitigate or remedy the effects of the Security Incident.

8. Third Party Processors

Each Party acknowledges that in the provision of some Services, it may transfer Personal Data to and otherwise interact with third party data processors. Each Party agrees that if and to the extent such transfers occur, the transferring Party is responsible for entering into separate contractual arrangement with such third-party data processors, binding them to comply with obligations in accordance with Applicable Data Protection Law. For avoidance of doubt, such third-party data processors are not Sub-Processors.

9. Audit Rights

Each Party shall allow for and contribute to limited audits of the Security Measures in accordance with the following procedures:

1. Upon Party's written request, the other Party will provide the requesting Party or its appointed auditor with the most recent certifications and/or summary audit report(s), which it has procured to regularly test, assess and evaluate the effectiveness of the Security Measures.
2. The Parties will reasonably cooperate by providing available additional information concerning the Security Measures to help each other better understand such Security Measures.
3. Each Party shall promptly notify the other Party with information regarding any non-compliance discovered during the course of an audit.
4. Each party will bear its own costs in respect of this section 9.

10. Liability, Payment of Compensation & Insurance

1. Notwithstanding anything to the contrary in the Initial Agreement, where pursuant to Article 82(4) of the GDPR, in order to ensure effective compensation of one or more individuals, the Parties agree that their respective liability shall be apportioned according to each Party's respective responsibility for the harm (if any) caused. In the event either Party is found to be liable for entire damage, or disproportionately large portion of damages, arising from a breach or breaches of the GDPR relating to activities under this Agreement then the other Party shall indemnify that Party for that portion of compensation attributable to any breaches of GDPR giving rise to the compensation for which it is responsible.
2. If a Data Subject asserts its rights against either Party pursuant to Article 26(4) of the GDPR and such assertion includes a claim for money, such Party will notify the other Party to give an opportunity to participate in the defense at such other Party's own expense.
3. Each Party shall take out and maintain insurance policies to the value sufficient to meet their respective liabilities under or in connection with this Agreement. Upon a Party's request, the other Party will provide evidence that such insurance is in place.

11. Concluding Provisions

This Agreement shall survive termination or expiry of the Initial Agreement. Upon termination or expiry of the Initial Agreement, each Party may continue to Process Personal Data provided that such Processing complies with the requirements of this Agreement and Applicable Data Protection Law.

12. Miscellaneous

This Agreement and any underlying Initial Agreement shall constitute the entire agreement between the Parties with respect to the subject matter hereof, and this Agreement supersedes all prior agreements or representations, oral or written, regarding such subject matter. This Agreement shall be interpreted, construed and enforced in accordance with the laws of Israel. Each Party irrevocably consents to the exclusive jurisdiction of the courts situated in Tel-Aviv district, Israel over all claims and all actions to enforce such claims or to recover damages or other relief in connection with such claims except to the extent that the Applicable Data Protection Law require otherwise. Adscend may assign this Agreement to any Affiliate entity. In case Adscend assigns the Initial Agreement to one of its Affiliates, this Agreement will be assigned to such Affiliate together with the Initial Agreement. The Parties may execute this Agreement in counterparts, including facsimile, PDF, via electronic signature systems (i.e. DocuSign, EchoSign, etc.) and other electronic copies. Which taken together will constitute one instrument.

The Parties acknowledge that they have read and understood the terms of this Agreement and agree to be legally bound by them.

Schedule A

Processing/ Transfer Activities

Data Subjects

The Personal Data transferred concern the following category of Data Subjects:
Individuals about home Personal Data is provided via the Services.

Categories of Data

The Personal Data transferred concern the following category of data:
Data relating to individuals provided via the Services.

Special Categories of Data

N/A

Purpose of the Transfer

The transfer is intended to enable the data exporter to determine the purpose and means of Processing of Personal Data obtained through data exporter's products to support the sales, recruiting, marketing, educational, or other business practices of the data importer to facilitate advertising to Data Subjects.

Recipients

The Personal Data may be disclosed only to the following recipients or categories of recipients:

- Third parties that have, or may have, a commercial relationship with the data exporter (e.g., buyers, sellers, advertisers, customers, corporate contractors); who have a legitimate business purpose for the Processing of such Personal Data and who have been bound to comply with Data Privacy Requirements, Applicable Data Protection Laws and other data protection obligations at least as restrict as those found in this Agreement.
- Third party service providers (such as IT systems and hosting service providers) who have been bound to comply with Data Privacy Requirements, Applicable Data Protection Laws and other data protection obligations at least as restrict as those found in this Agreement, including all technical security, data integrity and audit obligations relevant to the system involved.
- Law enforcement or government authorities where necessary to comply with applicable law, to address criminal acts that have been or are committed, or to respond to lawful process or discovery requests provided that the recipient of such request shall, to the extent legally permissible, promptly advise the other Party of the request.
- Those recipients as necessary to respond to an emergency that poses a threat of harm to safety of a user or other individuals, or otherwise as necessary to protect the rights or property of Adscend and Company, its data subjects and the importer provided however, that such discloser shall be terminated immediately after the emergency has passed; and
- Legal counsel or other advisors subject to appropriate non-disclosure agreements or obligations.