OPTIMIZELY DPA EXHIBIT 4
SUPPLEMENTARY MEASURES

Optimizely further commits to implementing supplementary measures based on guidance provided by EU supervisory authorities in order to enhance the protection of Customer Personal Data in relation to the processing in a third country, as described in this Schedule.

1. Additional Technical Measures (Encryption)

1.1. The personal data is transmitted (between the Parties and by Optimizely between data centers as well as with a Sub-processor) using strong encryption.

1.2. The personal data at rest is stored by Optimizely using strong encryption.

2. Additional Organizational Measures (Governance)

2.1. Internal policies for governance of transfers especially with groups of enterprises -

2.1.1 Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal requests from public authorities to access the data.

2.1.2 Development of specific training procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

2.2. Organizational methods and data minimization measures. Development and implementation of commercially reasonable practices by both Parties to appropriately and promptly inform respective data protection officers, if existent, and their legal and internal auditing services on matters related to international transfers of personal data transfers.

2.3. Others. Adoption and regular review by Optimizely of internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions, when necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

3. Additional Contractual Measures

3.1. Transparency obligations -

3.1.1 Optimizely declares that (a) it has not and will not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (b) it has not and will not purposefully create or change its business processes in a manner that facilitates access to personal data or systems, and (c) that national law or government policy does not require Optimizely to create or maintain back doors or to facilitate access to personal data or systems or for Optimizely to be in possession or to hand over the encryption key.

3.1.2 Optimizely will verify the validity of the information provided for the TIA questionnaire on request and provide notice to Customer in case of any material changes without delay. Clause 14(e) of the SCCs shall remain unaffected.

3.2. Obligations to take specific actions. In case of any order to disclose or to grant access to the personal data, Optimizely commits to inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for Optimizely.

3.3. Empowering data subjects to exercise their rights -

3.3.1 Optimizely commits to fairly compensate the data subject for any material and non-material damage suffered because of the disclosure of his/her personal data transferred under the chosen transfer tool in violation of the commitments it contains.

3.3.2 Notwithstanding the foregoing, Optimizely shall have no obligation to indemnify the data subject to the extent the data subject has already received compensation for the same damage.

3.3.2. Compensation is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Optimizely infringement of the GDPR.

4. Additional obligations in case of requests or access by public authorities

4.1. Optimizely shall promptly inform Customer -

4.1.1 Of any legally binding requests from a law enforcement or other government authority ("Public Authority") to disclose the personal data shared by Customer ("Transferred Personal Data"); such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided. Such notification shall occur prior to the disclosure of any personal data in response to such requests.

4.1.2 If it becomes aware of any direct access by public authorities to transfer personal data in accordance with the laws of the country of destination, such notification shall include all information available to Optimizely.

4.1.3. If Optimizely is prohibited from notifying Customer and/or the data subject, Optimizely agrees to use commercially reasonable efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. Optimizely will document those efforts, and will share them with the data exporter upon request.

4.2. Optimizely agrees to review, under the laws of the country of destination, the legality of the public authority's request, notably whether it remains within the powers granted to the requesting public authority and exhaust all available remedies to challenge the request if, after a careful assessment, Optimizely concludes that there are grounds under the laws of the country of destination to do so. This includes requests under section 702 of the United States Foreign Intelligence Surveillance Court or Executive Order 12333. When challenging a request, Optimizely shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. Optimizely shall not disclose or provide access to the personal data requested until required to do so under the applicable procedural rules and, at such time, shall provide only the minimum amount of information required to comply with the request, based on a reasonable interpretation of the request.

4.3. Optimizely agrees to preserve the information required to comply with this Exhibit 4 for the duration of the Agreement and, unless prohibited by applicable law, make it available to the competent supervisory authority upon request and when required by applicable law.