DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into between Client ("Controller") and Dapper Rhinos B.V. ("Processor"), Individually referred to as "Party" and jointly referred to as the "Parties", as an addendum to the main agreement for the provision of services ("Services") to the Controller by the Processor (the "Agreement"), and sets out the terms under which Processor will process Personal Data on behalf of the Controller in the context of the Services.

This DPA is intended to ensure compliance with all applicable laws and regulations relating to the Processing and protection of personal data, including but not limited to the GDPR and the General Data Protection Regulation Implementation Act ("Applicable Privacy Legislation") and any applicable local implementation act. Capitalized terms used in this DPA, such as Controller, Processor, Personal Data, Processing, Data Subject, and Supervisory Authority, will have the meaning given to them in the GDPR unless otherwise defined in this DPA.

1. Scope of the DPA

1.1 Unless the Parties have agreed otherwise in writing, the provisions of this DPA governs the Processing of Personal Data by the Processor in connection with the Agreement. Unless otherwise agreed in writing, this DPA will apply to all Processing activities carried out by the Processor under the Agreement, as required by Article 28(3) of the GDPR.

1.2 The subject matter of the Processing is the provision of Services as described in the Agreement. The nature of the Processing includes the collection, storage, analysis, and transmission of Personal Data. The purpose of the Processing is to support the Controller's marketing activities. The Processing will continue for the duration of the Agreement and any post-termination retention period as permitted under this DPA.

1.3 The Personal Data Processed by the Processor on behalf of the Controller may include, but is not limited to: IP addresses, cookie identifiers, device identifiers, location data, online identifiers, contact details (such as names and email addresses), behavioral and engagement data, user preferences, campaign interaction data, and other Personal Data collected or generated in the context of digital marketing, advertising, and analytics activities.

1.4 The Parties acknowledge and agree that the Processor is not intended to Process, and the Controller will not instruct the Processor to Process, any special categories of Personal Data as defined in Article 9 of the GDPR, nor any Personal Data relating to criminal convictions or offences (Article 10 GDPR), unless explicitly agreed otherwise in writing and subject to appropriate safeguards.

1.5 The Processor will Process Personal Data on behalf of the Controller, in accordance with the latter's written instructions and under the latter's responsibility and in the manner laid down in this DPA. The Processor will only Process the Personal Data on the instructions of the Controller, unless otherwise required by law.

1.6 The Controller warrants that the Processing of Personal Data as described in this DPA and the Agreement has a valid legal basis under Applicable Privacy Legislation, and that the Controller has fulfilled all obligations under Applicable Privacy Legislation necessary for lawful Processing by the Processor on its behalf.

2. **General obligations of the Processor**

2.1 The Processor has no control over the purpose of and the means for the Processing of Personal Data and does not make any independent decisions about the use of the Personal Data, the provision to third parties, and the duration of the storage of Personal Data.

2.2 The Processor will immediately notify the Controller in writing if, in the reasonable opinion of the Processor, an instruction constitutes a breach of the Applicable Privacy Legislation.

2.3 The Processor will ensure compliance with the conditions imposed by the Applicable Privacy Legislation on the Processing of Personal Data by processors.

2.4 The Processor will only grant access to the Personal Data to its employees to the extent technically possible and necessary for the performance of the services under the Agreement.

2.5 The Processor will not retain or otherwise Process the Personal Data for longer than necessary for the duration of the Agreement plus 6 months, unless the Controller expressly instructs otherwise in writing or where a longer retention period is required by applicable law.

3. **Provision of Personal Data to Third Parties.**

3.1 The Processor will not disclose or make available any Personal Data to a third party unless (i) this is expressly permitted in the DPA and/or Agreement, (ii) on the basis of an explicit written instruction from the Controller, or (iii) on the order of a judicial or administrative authority, provided that the Processor, in that case, notifies the Controller, to the extent permitted by law, within 48 hours of receiving such an order, in order to enable the Controller to take any legal action available to it.

3.2 If the Processor believes that it is required by law to make Personal Data available to a Supervisory Authority, it will not do so without consulting and obtaining the approval of the Controller. It will inform the Controller in writing as soon as possible of the legal obligation and provide all relevant information that the Controller reasonably needs to take the necessary measures to determine whether disclosure can take place and, if so, under what conditions.

4. **Processing outside the European Economic Area**

4.1 The Processor may transfer and process Personal Data outside the European Economic Area ("EEA"), for example parties such as Google and LinkedIn, in accordance with Chapter V GDPR. Such transfers may take place (i) on the basis of an adequacy decision adopted by the European Commission pursuant to Article 45 GDPR, or (ii) in the absence of such decision, subject to appropriate safeguards within the meaning of Article 46 GDPR, including the Standard Contractual Clauses adopted by the European Commission by Decision (EU) 2021/914 of 4 June 2021, as may be amended or replaced from time to time.

5. **Requests from Data Subjects**

5.1 The Processor will inform the Controller of all requests received directly from Data Subjects regarding the rights of Data Subjects under the Applicable Privacy Legislation, including but not limited to requests for access, rectification, erasure, restriction of processing, or transfer of the Personal Data. The Processor will only comply with such a request if the Controller has instructed the Processor to do so in writing. The Processor will, at Controller's request, provide all reasonable cooperation in fulfilling the Controller's obligation to respond to requests for the exercise of the Data Subjects' rights by means of appropriate technical and organizational measures.

5.2 The Processor will handle all requests for information from the Controller regarding the Processing of Personal Data promptly and properly. At Controller's request, the Processor will provide all information necessary to demonstrate compliance with the obligations of the Controller as laid down in this DPA and Article 28 of the GDPR.

5.3 The Processor will, upon reasonable requestand within a mutually agreed timeframe, cooperate with the Controller in conducting any data protection impact assessment and, where applicable, any prior consultation with a Supervisory Authority, in accordance with Applicable Privacy Legislation.

6. Engagement of sub-Processors

6.1 The Controller hereby gives general written authorisation for the Processor to engage sub-Processors for the performance of this Agreement.

6.2 The Processor will maintain an up-to-date list of its current sub-Processors via [insert hyperlink].

6.3 The Processor will inform the Controller in advance of any intended changes to this list, including the addition or replacement of a sub-Processor. The Controller may object in writing to a proposed change within 15 days after notification, but only on reasonable data protection grounds. If the Controller does not object within this period, the sub-Processor will be deemed approved.

6.4 The Processor remains fully responsible for its sub-Processors and ensures that they are bound by similar data protection obligations as set out in this DPA.

7. Confidentiality

7.1 The Processor will keep the Personal Data and other information obtained from the Controller strictly confidential, applying at least the same level of care as it applies to the protection of its own information of a highly confidential nature.

7.2 The Processor will not disclose the Personal Data or other information obtained from the Controller to persons other than its employees or contractors who need to have access to the Personal Data or other information obtained from the Controller for purposes of this Agreement. The Processor will also impose these confidentiality obligations on its employees or contractors involved in the Processing.

8. Obligation to report data breaches

8.1 The Processor will notify the Controller as soon as possible and within 48 hours after becoming aware of any breach of security that relates to the Processing of Personal Data ("Data Breach").

8.2 The Processor will in any case provide the Controller with the following information: (i) the nature of the Data Breach, where possible indicating the categories of Data Subjects concerned and, where possible, the approximate number of Data Subjects concerned; (ii) the Personal Data concerned and, where possible, the approximate number of Personal Data concerned; (iii) the established and expected consequences of the Data Breach for the Processing of Personal Data and the persons involved; and (iv) the measures taken and to be taken by the Processor to address the Data Breach, including, where appropriate, measures to mitigate any negative consequences of the Data Breach.

8.3 The notification referred to in Article 8.1 will be addressed by the Processor to a contact person designated by the Controller in clause 1.2. Upon receipt of the notification, the Controller will inform the Processor of the manner in which the Controller will, if necessary, report any Data Breach to the Supervisory Authority.

8.4 The Processor will take any reasonable measures necessary to limit the (potential) damage of the Data Breach and will support the Controller in reporting to Data Subjects and/or Supervisory Authorities.

9. **Technical and organisational measures.**

9.1 The Processor will take all appropriate technical and organizational measures to protect Personal Data against loss or any form of unlawful processing ("Security Measures") in accordance with Article 32 of the GDPR. These Security Measures will guarantee a level of security appropriate to the state of the art, the implementation costs, and the nature, scope, context, and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of the Data Subjects resulting from the Processing of the Personal Data Processed by the Processor, and are as follows:

a. Access control, such as role-based access rights, password protection on devices, tools and platforms; multifactor authentication;
b. Data encryption of personal data;
c. Firewalls, antivirus, intrusion detection and prevention systems;
d. Cyber security incident monitoring and logging;

e. Back-up and disaster recovery procedures;
f. Periodic testing and evaluating existing technical and organizational measures;
g. Security trainings
h. Device security

10. Audit

10.1 The Controller may request to audit the Processor's compliance in connection with the processing activities covered by this DPA ("Audit") The Controller will notify the Processor of such request in advance and consult with the Processor to agree on a reasonable date, scope, and duration for the Audit.

10.2 Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations under this DPA.

10.3 Processor will allow for and contribute to Audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

10.4 The Controller will provide the Processor with a copy of the report of the Audit.

11. Termination DPA

11.1 The DPA is entered into for an indefinite period and will end at the time that the Agreement ends, for whatever reason.

11.2 Unless otherwise specified in writing by the Controller, in the event of termination of the DPA, the Processor will immediately return all Personal Data made available to it to the Controller, destroy all digital copies of Personal Data, and declare to the Controller that it has done so.

11.3 If, in the reasonable opinion of the Processor, a legal obligation of the Processor prohibits or restricts the return or destruction of all or part of the Personal Data by the Processor, it will notify the Controller in writing as soon as possible of the legal obligation and provide relevant information that the Controller reasonably needs to determine whether destruction can take place and, if so, under what conditions.

12. Governing law and disputes.

12.1 This DPA is and will be exclusively governed by Dutch law. In case of any disputes arising out of or in connection with this DPA, the Parties will use reasonable efforts to resolve such disputes amicably and in good faith outside of

court. If no resolution is reached within a reasonable period, the dispute will be submitted exclusively to the competent court in Rotterdam, the Netherlands.