Moovit – Partner Transit On Demand
Data Processing Agreement
(Independent Controllers)

This Data Processing Agreement (Independent Controllers) (this "**DPA**") forms an integral part of, and is subject to, the Transport on Demand Collaboration Agreement (the "**Partner Agreement**") governing Partner's use of the Moovit Transit on Demand Solution and/or Moovit Transit on Demand Service and entered into by you and the entity you represent (hereinafter referred to as "**Partner**"). **Moovit App Global Ltd.** (hereinafter referred to as "**Moovit**") and Partner are hereinafter jointly referred to as the "**Parties**" and individually as a "**Party**." Capitalized terms not otherwise defined herein shall have the meaning given to them in the Partner Agreement.

This DPA covers the Processing (as defined below) of: (a) Personal Data (as defined below) that the Partner uploads, transfers, or otherwise makes available to Moovit in connection with the Partner Agreement; and (b) Personal Data that Moovit uploads, transfers, or otherwise makes available to Partner in connection with the Partner Agreement.

Collectively, this DPA (including the SCCs, as defined below) and the Partner Agreement are referred to in this DPA as the "**Agreement**."

1. **Definitions**. In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:

    1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

    1.2. "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Controller Personal Data in respect of which Controller is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which the Controller is subject to any other Data Protection Laws.

    1.3. "**Controller Personal Data**" means any Personal Data Processed by Processor on behalf of Controller pursuant to or in connection with the Partner Agreement.

    1.4. "**Controller-to-Controller SCCs**" means the Standard Contractual Clauses (Controller to Controller Transfers - Set II) in the Annex to the European Commission Decision of December 27, 2004 as may be amended or replaced from time to time by the European Commission.

    1.5. "**Controller-to-Processor SCCs**" means the Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of February 5, 2010 as may be amended or replaced from time to time by the European Commission.

    1.6. "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other applicable country as agreed in writing between the Parties, including in the United States and Israel.

    1.7. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

    1.8. "**EU Personal Data**" means Personal Data the sharing of which pursuant to this Agreement is regulated by EU Data Protection Laws.

    1.9. "**GDPR**" means EU General Data Protection Regulation 2016/679.

1.10. "**Moovit Personal Data**" means any Personal Data for which Moovit acts as a Controller.

1.11. "**Partner Personal Data**" means any Personal Data for which Partner acts as a Controller.

1.12. "**Restricted Transfer**" means (a) a transfer of Controller Personal Data from Controller to Processor; or (b) an onward transfer of Controller Personal Data from a Processor to a Sub Processor, or between two establishments of Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of a legal transfer mechanism to be established under this DPA, including without limitation the applicable Standard Contractual Clauses.

1.13. "**Sub Processor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to Process Personal Data on behalf of the Controller in connection with the Agreement.

1.14. "**Standard Contractual Clauses**" or "**SCCs**" means all Controller-to-Processor SCCs and Controller-to-Controller SCCs as defined herein and entered into between the Parties pursuant to this DPA.

1.15. The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

2. **Purpose; Relationship; Scope.**

   2.1. Purpose. The purpose of this DPA is to establish a framework whereby both the Partner and Moovit may, in connection with the Partner Agreement, each be a Controller of Personal Data ("**Controller**") and, in certain cases, transfer or make available that Personal Data to the other Party for that other Party to provide certain services as a Processor ("**Processor**").

   2.2. Relationship of the Parties. The rights, responsibilities, and obligations of the Parties with regard to the terms and conditions of this DPA shall be as follows: (a) for data Processing operations where Moovit Processes Personal Data on Partner's behalf and at Partner's direction, the term "Processor" refers to Moovit, the term "Controller" refers to Partner, and the term "Personal Data" refers to Partner Personal Data; and (b) for data Processing operations where Partner Processes Personal Data on Moovit's behalf and at Moovit's direction, the term "Processor" refers to Partner, the term "Controller" refers to Moovit, and the term "Personal Data" refers to Moovit Personal Data. To the extent applicable to the above-described relationship between the Parties, each Party may then respectfully be referred to hereunder as a Processor or as a Controller, as the context necessitates and as applicable with respect to any given data Processing activity contemplated by this Agreement.

   2.3. Scope of Processing. In the context of the scenarios described above, each Party agrees in its capacity as a Processor of Personal Data to Process the respective Personal Data only for the purposes set forth in the Partner Agreement and in accordance with the terms below. For the avoidance of doubt, the categories of Personal Data Processed and the categories of Data Subjects subject to this DPA are described in **Annex 1** to this DPA.

3. **Controller Obligations.**

   3.1. The Parties in their respective capacity as a Controller agree to: (a) provide documented reasonable and customary instructions to the Processor (and authorize the Processor to instruct each applicable Sub Processor) and determine the purposes and means of the Processor's Processing of Controller Personal Data in accordance with the Partner Agreement and/or this DPA; (b) transfer Controller Personal Data to any country or territory, all as reasonably necessary for the provision of the applicable service provided by the Processor and consistent with the terms of the Partner Agreement, and in accordance with Applicable Laws; and (c) comply with its protection, security and other obligations with respect to Personal Data prescribed by Applicable Laws for a Controller by: (i) establishing and maintaining a procedure for the exercise of the

rights of the individuals whose Personal Data are Processed on behalf of the Controller; (ii) Processing only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses; and (iii) ensuring compliance with the provisions of this DPA by its personnel or by any third party accessing or using Personal Data on its behalf.

3.2. Furthermore, Controller warrants and represents that it is and will remain duly and effectively authorized to give the instructions as set out in Section 3.1 and any additional instructions as provided pursuant to the Partner Agreement and/or in connection with the performance thereof, on behalf of itself and each relevant Controller Affiliate, at all relevant times and at least for as long as the Partner Agreement is in effect and for any additional period during which Processor is lawfully Processing the Controller Personal Data.

3.3. Controller sets forth the details of the Processing of Controller Personal Data, as required by article 28(3) of the GDPR in **Annex 1** (*Details of Processing of Controller Personal Data*), attached hereto.

3.4. Without derogating from Controller's obligations hereunder, including under any data protection or security clauses of the Partner Agreement, Controller may only provide to Processor, or otherwise have Processor (or anyone on its behalf) Process, such Controller Personal Data types and parameters which are explicitly permitted under Controller's applicable privacy policy or which are otherwise lawfully and validly collected (the "**Permitted Controller Personal Data**"). Solely Controller (and not Processor) shall be liable for any data which is provided or otherwise made available to Processor or anyone on its behalf in excess of the Permitted Controller Personal Data **("Excess Data")**. Processor obligations under the Partner Agreement or this DPA shall not apply to any such Excess Data.

4. **Processor Obligations.**

4.1. The Parties in their respective capacity as a Processor, and in the case of Partner as Processor, also in its capacity as Subprocessor of Subcontractor's Driver Data, agree that: (a) Processor shall not Process Controller Personal Data other than on the Controller's documented reasonable and customary instructions as specified in the Partner Agreement or this DPA that were specifically and explicitly agreed to by Processor, unless such Processing is required by Applicable Laws to which the Processor is subject; and (b) Processor shall Process Controller Personal Data, only for the purpose of providing, supporting and improving the Processor's services as contemplated by the Partner Agreement, using appropriate technical and organizational security measures as further described below.

4.2. The Processor will promptly and without undue delay inform the Controller in writing if: (a) Processor becomes aware of any non-compliance by Processor or its personnel with the terms of this DPA or the applicable Data Protection Laws relating to the protection of Personal Data processed under this DPA; (b) in the Processor's reasonable opinion, an instruction from the Controller violates applicable Data Protection Laws; or (c) Processor cannot comply with the requirements of this DPA, in which case the Controller may terminate the Agreement, and any applicable Partner Agreements, or take any other reasonable action, including suspending data Processing operations.

4.3. Processor Personnel. Processor shall take reasonable steps to ensure that access to the Controller Personal Data is limited on a need to know/access basis, and that all Processor personnel receiving such access are subject to strict confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Controller's Personal Data and otherwise comply with the terms of the Agreement, and applicable Partner Agreements.

4.4. Security. Processor shall, in relation to the Controller Personal Data, implement appropriate technical and organizational measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Personal Data while in transit and at rest) to ensure an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR and to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Personal Data. In assessing the appropriate level of security, Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Sub Processing.**

   5.1. Controller authorizes Processor and each Processor Affiliate to appoint (and permit each Sub Processor appointed in accordance with this Section 5 to appoint) Sub Processors in accordance with this Section 5 and any restrictions in the Partner Agreement.

   5.2. Processor and each Processor Affiliate may continue to use those Sub Processors already engaged by Processor or any Processor Affiliate as of the date of this DPA, including for the purpose of cloud hosting services by reputable Sub Processors, as well as any Sub Processors whom Controller requested Processor to use.

   5.3. Processor may appoint new Sub Processors and shall give notice of the appointment of any new Sub Processor (for instance by e-mail), whether by general or specific reference to such Sub Processor (e.g., by name or type of service), including relevant details of the Processing to be undertaken by the new Sub Processor. If, within seven (7) days of such notice, Controller notifies Processor in writing of any objections (on reasonable grounds) to the proposed appointment, Processor shall not appoint for the processing of Controller Personal Data the proposed Sub Processor until reasonable steps have been taken to address the objections raised by Controller, and Controller has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Controller's reasonable objections then Controller or Processor may, by written notice to the other Party, with immediate effect, terminate the Partner Agreement to the extent that it relates to the Processor services which require the use of the proposed Sub Processor without bearing liability for such termination.

   5.4. With respect to each new Sub Processor, Processor shall:

      5.4.1. remain liable to the Controller for the Sub Processors' acts and omissions with regard to data protection where such Sub Processors act on the Processor's instructions;

      5.4.2. before the Sub Processor first Processes Controller Personal Data, take reasonable steps (for instance by way of reviewing privacy policies, as appropriate) to ensure that the Sub Processor is committed to provide the level of protection for Controller Personal Data required by the Partner Agreement; and

      5.4.3. ensure that the arrangement between the Processor and the Sub Processor is governed by a written contract, including terms which offer materially similar level of data protection and information security for Controller Personal Data as those set out in this DPA that meet the requirements of Applicable Laws, including in connection with Restricted Transfers.

6. **Data Subject Rights**.

   6.1. Controller shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g., for access, rectification, deletion of Controller Personal Data, etc.). Taking into account the nature of the Processing, Processor shall reasonably endeavour to assist Controller insofar as commercially feasible, to fulfil Controller's said obligations with respect to such Data Subject requests, as applicable, at Controller's sole expense.

   6.2. Processor shall:

      6.2.1. promptly notify Controller if it receives notice of or becomes aware of any inquiry, investigation or legally binding request for disclosure of Personal Data by a Supervisory Authority or other law enforcement or government authority, unless the Processor is otherwise forbidden by law to inform the Controller, for example to preserve the confidentiality of an investigation by law enforcement authorities;

6.2.2. promptly notify Controller if it receives any complaint or request (in particular, requests for access to, rectification or blocking of Personal Data) directly from a Data Subject under any Data Protection Laws in respect of Controller Personal Data; and

6.2.3. ensure that it does not respond to a Data Subject request except on the documented instructions of Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by Applicable Laws, inform Controller of that legal requirement before it responds to the request.

7. **Personal Data Breach**.

7.1. Processor shall notify Controller without undue delay upon Processor becoming aware of a Personal Data Breach affecting Controller Personal Data, in connection with the Processing of such Controller Personal Data by the Processor or Processor Affiliates. In such event, Processor shall provide Controller with information (to the extent in Processor's possession) to assist Controller to meet any obligations to inform Data Subjects or Data Protection authorities of the Personal Data Breach under the Data Protection Laws.

7.2. At the written request of the Controller, Processor shall reasonably cooperate with Controller and take such commercially reasonable steps as are agreed by the Parties or necessary under Privacy Protection Laws to assist in the investigation, mitigation and remediation of each such Personal Data Breach, at Controller's sole expense.

8. **Data Protection Impact Assessment and Prior Consultation**.

8.1. At the written request of the Controller, the Processor and each Processor Affiliate shall provide reasonable assistance to Controller, at Controller's expense, with any data protection impact assessments or prior consultations with Supervising Authorities or other competent data privacy authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Controller Personal Data by the Processor.

9. **Deletion or Return of Controller Personal Data**.

9.1. Subject to Section 9.2, Processor shall promptly and in any event within up to sixty (60) days of the date of cessation of any services involving the Processing of Controller Personal Data (the "**Cessation Date**"), delete or pseudonymize all copies of those Controller Personal Data, except such copies as authorized including under the Partner Agreement and this DPA or required to be retained in accordance with applicable law and/or regulation.

9.2. Subject to the Partner Agreement, Processor may retain Controller Personal Data to the extent authorized or required by Applicable Laws, provided that Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that it is only processed for such legal purpose(s).

9.3. Upon Controller's prior written request, Processor shall provide written certification to Controller that it has complied with this Section 9.

10. **Audit Rights**

10.1. Subject to Sections 10.2 and 10.3, Processor shall make available to a reputable auditor mandated by Controller in coordination with Processor, upon prior written request, such information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.

10.2. Provisions of information and audits are and shall be at Controller's sole expense and may only arise under Section 10.1 to the extent that the Partner Agreement does not otherwise give Controller information and audit rights meeting the relevant requirements of the applicable Data Protection Laws. In any event, all audits

or inspections shall be subject to the terms of the Partner Agreement, and to Processor's obligations to third parties, including with respect to confidentiality.

10.3. Controller shall give Processor reasonable prior written notice of any audit or inspection to be conducted under Section 10.1 and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2. if Processor was not given a written notice of such audit or inspection at least 2 weeks in advance;

10.3.3. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controller has given notice to Processor that this is the case before attendance outside those hours begins;

10.3.4. for premises outside the Processor's control (such as data storage farms of Processor's cloud hosting providers);

10.3.5. if more than one (1) audit or inspection, in respect of each Processor, already took place in the same calendar year, except for any additional audits or inspections which:

10.3.5.1. Controller reasonably considers necessary because of genuine concerns as to Processor's compliance with this DPA; or

10.3.5.2. Controller is required to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Controller has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

10.4. If a Supervisory Authority requires an audit of the data processing facilities from which the Processor processes Personal Data in order to ascertain or monitor compliance with Data Protection Laws, the Processor will cooperate with such audit. The Controller will reimburse the Processor for its reasonable expenses incurred to cooperate with the audit, unless such audit reveals the Processor's noncompliance with this DPA.

11. **Data Transfers**

11.1. For transfers of EU Personal Data to a Party for Processing by such Party as a Processor on behalf of the transferring Party as a Controller, in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, or otherwise in connection with a Restricted Transfer, Processor agrees it will provide privacy protection for EU Personal Data (a) using the Controller-to-Processor SCCs, or (b) under another legal framework providing adequate protection as agreed by the Parties in a separate agreement. If data transfers under this Section 11.1 rely on SCCs to enable the lawful transfer of EU Personal Data, as set forth in the preceding sentence, the Parties agree that Data Subjects for whom Processor Processes EU Personal Data are third-party beneficiaries under the SCCs. If Processor is unable or becomes unable to comply with these requirements, then EU Personal Data will be Processed and used exclusively within the territory of a member state of the European Union and any movement of EU Personal Data to a non-EU country requires the prior written consent of Controller with respect to Personal Data. Processor shall promptly notify Controller of any inability by Processor to comply with the provisions of this Section 11.1.

12. **General Terms**

12.1. **Governing Law and Jurisdiction**.

12.1.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Partner Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Partner Agreement.

Order of Precedence. Nothing in this DPA reduces Processor's obligations under the Partner Agreement in relation to the protection of Controller Personal Data or permits Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Partner Agreement. In the event of any conflict or inconsistency between this DPA and the Partner Agreement, this DPA shall prevail solely with respect to the subject matter of this DPA and solely if such conflict or inconsistency originate from the requirements of Article 28 of the GDPR (except where explicitly agreed otherwise in writing, signed on behalf of the Parties). This DPA is not intended to, and does not in any way limit or derogate from Controller's own obligations and liabilities towards the Processor under the Partner Agreement, and/or pursuant to the GDPR or any law applicable to Controller, in connection with the collection, handling and use of Personal Data by Controller or its Affiliates or other processors or their sub-processors, including with respect to the transfer or provision or Personal Data to Processor and/or providing access thereto to Processor.

12.2. **Changes in Data Protection Laws**.

12.2.1. Controller may by at least forty-five (45) calendar days' prior written notice to Processor, request in writing any variations to this DPA or to the Standard Contractual Clauses if they are required, as a result of any change in, or decision of a competent authority under any applicable Data Protection Law, to allow Processing of those Controller Personal Data, including with respect to Restricted Transfers, to be made (or continue to be made) without breach of that Data Protection Law; and

12.2.2. If Controller gives notice with respect to its request to modify this DPA under Section 12.3.1:

12.2.2.1. Processor shall make commercially reasonable efforts to accommodate such modification request; and

12.2.2.2. Controller shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor for any further steps and costs associated with the variations made herein.

12.3. If Controller gives notice under Section 12.3.1, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Controller's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days, then Controller or Processor may, by written notice to the other Party, with immediate effect, terminate the Partner Agreement to the extent that it relates to the services which are affected by the proposed variations (or lack thereof).

12.4. **Severance**. Should any provision of this DPA be deemed invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (a) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Partner Agreement with effect from the later date set out below.

NOTWITHSTANDING THE BELOW SIGNATURE BLOCKS REMAINING UNSIGNED, PARTNER'S ACCESS TO OR USE OF THE TOD SOLUTION, TOD SERVICE OR ANY PART THEREOF CONSTITUTES ACTIVE ACCEPTANCE OF THE TERMS OF THE MOOVIT TRANSIT ON DEMAND PLATFORM TERMS OF SERVICE AND THIS DATA PROCESSING AGREEMENT.

Partner

Signature _____

Name _____

Title _____

Date _____

Moovit App Global Ltd.

Signature _____

Name _____

Title _____

Date _____

Annex 1: Details Of Processing Of Controller Personal Data

This **Annex 1** includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data. The subject matter and duration of the Processing of the Controller Personal Data are set out in the Partner Agreement.

The nature and purpose of the Processing of Controller Personal Data: the Processing is intended to enable the relationship of the Parties contemplated by the Partner Agreement, including the rendering of services in the nature of such services as those detailed in the Partner Agreement.

The types of Controller Personal Data to be Processed are as follows:

Where Moovit is a Controller: Moovit business contact information; [Moovit end-user details, end-user geo-location, end-user routing and schedule information, phone number, payment details, name, , location of order, location of pickup and location of drop off, accessibility and number of passengers traveling together, and any other information necessary for the provision of the TOD Service]; solely to the extent that such parameters are deemed as Personal Data under applicable law.

Where Partner is a Controller: Partner business contact information; Partner's Driver Data, including Partner's Driver and Partner's Fleet vehicle location, routing and schedule information, Partner's Driver credentials, and any other information necessary for the provision of the Transport Service.]Subcontractor's business contact information, solely to the extent that such parameters are deemed as Personal Data under applicable law.

Where Partner is a Processor: [Moovit personnel, Moovit end-user details, end-user geo-location, end-user routing and schedule information, phone number, payment details, name, phone number, location of order, location of pickup and location of drop off, accessibility and number of passengers traveling together, and any other information necessary for the provision of the TOD Service; And as Subprocessor for Subcontractor's Driver Data, including Subcontractor's Driver and Subcontractor's Fleet vehicle location, routing and schedule information, Subcontractor's Driver credentials, and any other information necessary for the provision of the Transport Service.]

The categories of Data Subject to whom the Controller Personal Data relates to are as follows:

Where Moovit is a Controller: [Moovit's personnel; Moovit App end-users.]

Where Partner is a Controller: [Partner's personnel, Partner's Driver, and Subcontractor Representatives.]

Where Partner is a Processor: [Moovit personnel, Moovit App end-users and Subcontractor's Drivers]

The obligations and rights of Controller. The obligations and rights of Controller and Controller Affiliates are set out in the Partner Agreement and this DPA.