Data Processing Agreement for Road Services

("Data Processing Agreement")

Version August, 2023

BETWEEN

1. The Customer, as defined in the Principal Agreement (hereinafter referred to as "the Controller")
2. Road B.V., whose registered office is at Joan Muyskenweg 37, 1114 AN Amsterdam, The Netherlands, registered in the trade register of the Chamber of Commerce under number 70011346 ("the Processor").

Each referred to as a Party and together as the Parties.

WHEREAS

A. The Controller wishes to appoint the Processor to process Personal Data within the framework of the Road Private Label Agreement ("Principal Agreement"). The Controller shall make available all other data that the Processor might reasonably need, so that the Processor can (a) provide the services as agreed in the Principal Agreement and (b) comply with this Data Processing Agreement, as further detailed in Schedule 1. The Processor has agreed to provide such services on the terms set out in the Principal Agreement. The Processor agrees to process personal data as instructed in this Data Processing Agreement. Any amendment to this agreement must be done in writing and signed by both parties.

IT IS AGREED AS FOLLOWS

1. Definitions

1.1. In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- "Data Processing Agreement" means this data processing agreement;
- "Principal Agreement" has the meaning as described in recital (A);
- "Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject') (an identifiable natural person is one who can be identified, directly or indirectly);
- "Controller Personal Data" means any Personal Data disclosed by the Controller to the Processor and processed by the Processor on behalf and under the instructions of the Controller pursuant to or in connection with the Agreement;
- "Customer" means the legal entity that is a party to the Principal Agreement and defined as the Customer therein;

- “EU Data Protection Laws” means the GDPR and applicable laws implementing or supplementing the GDPR;
- “GDPR” means EU General Data Protection Regulation 2016/679.

1.2. The terms, “Third Country”, “Member State”, "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Controller Personal Data

2.1. The Parties acknowledge that in the performance of the Principal Agreement, the Processor processes Controller Personal Data on behalf of the Controller.

2.2. When Processing such Controller Personal Data, the Processor shall:

i. comply with EU Data Protection Laws; and

ii. not process Controller Personal Data other than on the Controller’s documented instructions, including with regard to transfers of Controller Personal Data to a Third Country or an international organisation, unless required to do so by EU or Member State Law to which the Processor is subject. In such a case the Processor shall inform the Controller of that legal requirement before Processing of that Controller Personal Data, unless that legal requirement prohibits such information on important grounds of public interest.

2.3. Schedule 1 to this Agreement sets out certain information regarding the Processor's Processing of the Controller Personal Data as required by Article 28(3) of the GDPR. The Controller may make reasonable amendments to Schedule 1 by written notice to the Processor from time to time as Controller reasonably considers necessary to meet those requirements.

2.4. The Processor shall immediately inform the Controller if, in its opinion, an instruction (possibly) infringes with EU Data Protection Laws.

3. Processor’s personnel

3.1. The Processor shall ensure that persons authorized to process Controller Personal Data perform such Processing activities in accordance with the instructions given by the Controller and have committed themselves to confidentiality or that these persons are bound to confidentiality by virtue of a legal obligation.

4. Security

4.1. The Processor shall not transfer or make available Controller Personal Data to third parties unless it concerns a third party (‘sub-processor’) as listed in Schedule 3.

4.2. Taking into account the state of the art, the implementation costs as well as the nature, scope, context and purposes of processing and the risks to the rights and freedoms of natural persons that differ in their likelihood and severity, the Processor shall, with respect to the Controller Personal Data, implement appropriate technical and organizational measures to ensure a risk-appropriate security plan, which shall also include, where appropriate, the measures referred to in Article 32(1) of the GDPR.

4.3. The Processor shall prepare a list and description of the security measures (technical, logical and organizational) set out in Schedule 2 of this Agreement and confirm that these measures provide an appropriate level of security, taking into account the state of the art and the security threats that are known or should reasonably have been known. The Processor is authorized to review and adjust the implemented security measures where it deems such to be necessary to ensure an adequate level of security.

5. Sub-processing

5.1. The Processor shall not engage (or disclose any Controller Personal Data to) a sub-processor without obtaining the Controller's prior written consent. The Controller has approved the sub-processor(s) listed in Schedule 3.

5.2. The Processor shall ensure that any sub-processor complies with all obligations under this Agreement as they apply to the Processing of Personal Data by the Controller that is carried out by that sub-processor, as if it were a party to this Agreement instead of the Processor. In particular, by providing sufficient safeguard with respect to the use of appropriate technical and organizational measures so that the Processing complies with the provisions of the GDPR. Where such other sub-processor fails to comply with its obligations under the EU Data Protection Laws, the Processor shall remain fully liable to the Controller for compliance with such obligations of the other sub-processor subject to Clause 12 of the Agreement.

5.3. The Processor shall inform the Controller of any intended changes regarding the addition or replacement of such other sub-processors, giving the Controller the possibility to object to such changes. The Controller shall not unreasonably object to such addition or replacement. In the event of an objection, the Parties shall cooperate together in good faith to find a suitable alternative. If no such alternative is found or acceptable to the Controller, the Processor has the right to terminate this Agreement in accordance with Clause 9 of the Agreement.

6. Assistance to the Controller

6.1. Taking into account the nature of the Processing, the Processor shall assist the Controller in complying with its obligations to respond to requests under EU Data Protection Laws, including in any case requests of Data Subjects.

6.2. The Processor shall:

6.2.1. Without undue delay , but ultimately within 48 hours after receipt, notify Controller if it receives:

a. a request from a Data Subject to exercise their rights in accordance with any EU data protection legislation relating to personal data, in respect of Controller Personal Data;

b. a (information) request from a competent authority relating to the (Processing of the) Controller Personal Data; or

c. a third-party complaint or request relating to the obligations of the Processor and/or the Controller under the EU Data Protection Laws; and

6.2.2. ensure that it does not respond to that request except on the documented instructions of the Controller or as required by EU or Member State Law to which it is subject, in which case the Processor shall to the extent permitted by that legal requirement inform Controller of that legal requirement before it responds to the request; and

6.2.3. provide all reasonable assistance to the Controller in order to enable the Controller to meet and respond to requests as described in provision 6.2.1 in a timely manner.

7. Personal Data Breach

7.1. The Processor shall notify the Controller in writing , without undue delay, but ultimately within 48 hours after becoming aware, of a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information to enable the Controller to meet any obligations to report or inform the Dutch Data Protection Authority or any other relevant authority and/or Data Subjects of the Personal Data Breach pursuant to the EU Data Protection Laws.

7.2. Such notification shall as a minimum:

a. describe the nature of the Personal Data Breach, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

b. communicate the name and contact details of the Processor's data protection officer or other relevant contact from whom more information may be obtained;

c. describe the likely consequences of the Personal Data Breach; and

d. describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8. Cooperation obligations of the processor

8.1. The Processor shall, at the request of the Controller, within the specified period, cooperate with and assist the Controller, in order to enable the Controller to meet its obligations pursuant to EU Data Protection Laws, including but not limited to the implementation of data protection impact assessments and prior consultations with Supervisory Authorities or other competent authorities, which the Controller reasonably considers to be required pursuant to Article 35 or 36 of the GDPR, taking into account the nature of the Processing and the information that is available for the Processor.

9. Deletion or return of Controller Personal Data

9.1. Except as provided in clauses 9.2, 9.3 and 9.4 the Processor shall, at the request of the Processor and, in any event, within 6 months after the end of the Principal Agreement (the Termination Date), erase all Controller Personal Data and order the deletion of all copies of such Personal Data.

9.2. Subject to clause 9.3 and 9.4, the Controller may by written notice to the Processor, within 1 month after the Termination Date, require the Processor to: (a) return to Controller a complete copy of all Controller Personal Data; and (b) delete or order deletion of all other copies of Controller Personal Data processed by Processor. The Processor shall comply with such written request within 4 months after the Termination Date.

9.3. The Processor may retain the Controller Personal Data if storage of the Personal Data is required by EU or Member State law, only to the extent and for as long as required by such law and if the Processor will ensure the confidentiality of all Controller Personal Data and if the Processor will ensure that such Controller Personal Data is only processed for purposes defined by EU or Member State law requiring the storage and for no other purpose.

9.4. On Processor's request, the Controller shall instruct Processor to anonymize Controller Personal Data (or a part thereof) in order for Processor to process such data after the Termination Date for statistical and analytical purposes.

9.5. The Processor shall confirm in writing to the Controller that it has fully complied with clause 9 within 12 months after the Termination Date.

10. Audits

10.1. The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with the obligations that are set out in Agreement and stem directly from EU Data Protection Laws, and allow for and contribute to audits on an annual basis, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Processor. The Parties agree that in substitute of having the Controller perform an audit, the Processor may also provide audit reports on an annual basis, resulting from audits conducted by an independent and third party auditor, attesting to the Processor's compliance with the EU Data Protection Laws, to comply with its information obligation under this Clause 10.1.

10.2. The costs of an audit are for the account of the Controller.

11. Term and Termination

11.1. This Agreement is entered into for the duration of the Principal Agreement. In case the Principal Agreement ends, this Agreement will automatically end as well, with due observance of clause 11.2 of this Agreement.

11.2. Any obligation arising from this Agreement that by nature has post-contractual effect, including, but without limitation to clause 12 and the Processor's obligations under clause 9 of this Agreement shall continue to be in effect after the termination of this Agreement.

12. Liabilities and penalties

12.1. The liability of the Processor as the result of or otherwise related to a breach of this Agreement by the Processor shall not exceed the maximum of the total Fees (as defined in the Principal Agreement) relating to the relevant data processing activity.

13. Miscellaneous

13.1. Any Party's failure to exercise any of its rights pursuant to or in connection with this Agreement shall not constitute a waiver of such rights or in any other way prejudice such rights.

13.2. The rights and obligations under this Agreement can be assigned or transferred by the Processor to an affiliated company of the Processor, including, without limitation, through the sale or contribution of a division or of a business as a whole, or a merger, spin-off or split-up, without the prior written consent of the other Party.

13.3. If and to the extent that a provision in the Principal Agreement and/or corresponding agreements between the Parties conflicts with any provision in this Agreement, the provisions in this Agreement shall prevail.

13.4. This Agreement may be amended only by written agreement between the Parties, without prejudice to clause 2.3 above.

13.5. If any provision of this Agreement is declared void or unenforceable by any court or tribunal of competent jurisdiction, the other provisions of this Agreement shall remain to be of effect, unless the latter provisions must be deemed to be indissolubly connected with the void or unenforceable provision. In the event that the other provisions remain valid, both Parties shall endeavour to replace the void or unenforceable provision by a valid provision which reflects the Parties' original intent to the greatest possible extent.

13.6. General terms and conditions related to the Principal Agreement shall not apply to this Agreement.

13.7. The costs relating to the execution of this Agreement are included in the prices and fees as agreed in the Principal Agreement.

14. Governing Law

14.1. This Agreement shall be governed by and construed in accordance with the laws of the Netherlands.

14.2. For all disputes arising in connection with this Agreement, the parties hereto submit to the exclusive jurisdiction of the courts of Amsterdam.

SCHEDULE 1 -

DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

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

1. 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 Principal Agreement, as supplemented by this Data Processing Agreement.

2. The nature and purpose of the Processing of Controller Personal Data

Examples:

- *Storage in the Road Platform*
- *Processing for client administration, invoicing, accounting, debtor administration, compliance with its legal obligations in relation to the prevention of fraud and money laundering and employee management.*

Means of Processing:

- *Software developed by Road*
- *Integrations:*
- *Payt*
- *Postmark*
- *SalesForce*
- *Netsuite*
- *Intercom*
- *Aircall*
- *Checkout*
- *Worldline*
- *Payone*

Purpose of Processing:

- *User management*
- *Provision of Service*
- *Follow-up of sales process*
- *Mail management*
- *Payment processing*

3. The types of Controller Personal Data to be Processed

Examples:

- *Name*
- *First name*
- *Account name*
- *Password*
- *E-mail address*
- *Telephone number (landline/mobile)*

- *Home address*
- *Account number*
- *IBAN*
- *Charge location data*

4. The categories of Data Subjects to whom the Controller Personal Data relate

Examples:

- *Customers*
- *Employees*
- *Business partners*
- *Suppliers*
- *Visitor of platform*

5. The obligations and rights of the Controller

The obligations and rights of the Controller are set out in the Principal Agreement, as supplemented by this Data Processing Agreement.

SCHEDULE 2 -

TECHNICAL AND ORGANIZATIONAL MEASURES

This Schedule 2 describes the technical and organizational measures that Processor maintains to ensure it processes and protects Personal Data in a responsible way and in accordance with clause 4 of this Agreement, considering the state of the art, the costs of implementation, the nature, scope, context, the purpose of processing and the risks involved for data subjects.

Examples:

(Physical) access control to processing infrastructure:

- The web application, communication and database servers of Road are located in secure data centers managed by Google, with whom Road has signed the "Data Processing and Security Terms" in order to comply with the standards and obligations of the General
- Data Regulation.

Access control to systems for the processing of Personal Data:

- Road has taken appropriate measures to prevent non-authorised persons from using its systems for the Processing of Personal Data.
- Measures taken:
    - o Secure access to Road application by means of authorisation
    - o Automatic blocking of the user after repeatedly entering a wrong password.
    - o Automatic monitoring and reporting of issues that may occur on the various platforms
    - o Enforced Wildcard HTTPS and TLS 1.3 for all API and web endpoints
    - o Automatic renewal of SSL certificates
    - o DNS and HTTP protection (DDOS, access control, spam protection)
    - o DKIM & DMARC verification for outgoing mail traffic
    - o Encryption of passwords by BCRYPT

Checking availability:

- Road has implemented appropriate measures to ensure that Personal Data are protected against involuntary destruction or loss.
- Measures taken:
    - o Daily backups of the Main Database
    - o Monitoring including automatic notifications and weekly health reports
    - o Performance monitoring system
    - o Scalable infrastructure
    - o CDN server network for better website performance

SCHEDULE 3 -

LIST OF SUB-PROCESSORS

The Controller has authorized the use of the following sub-processors:

Name	**Processing Activity**	**Address**
Google	Platform Hosting	Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland
SalesForce	CRM	SFDC Ireland Ltd. Level 1, Block A Sandyford Business Park Dublin 18 Ireland
Oracle NetSuite	ERP	Oracle Corporation UK Limited Oracle Parkway Thames Valley Park Reading RG6 1RA United Kingdom
Aircall	Support	Aircall SAS 11-15 Rue Saint-Georges 75009 Paris France
Intercom	Support	Intercom 3rd Floor, Stephens Ct., 18-21 St. Stephen's Green Dublin 2 Ireland
Payt	Accounts Receivable Management	Payt B.V. Ubbo Emmiussingel 21 9711 BB Groningen The Netherlands
Postmark by ActiveCampaign	Email Communication	AC PM, LLC 1 N Dearborn Street, Suite 500 Chicago, IL 60602 United States
Checkout	Digital payment processing	Checkout SAS 20 bis rue La Fayette, 75009 Paris France
Worldline	Physical payment processing	Worldline Financial Services (Europe) S.A. 33 Rue Du Puits Romain Bertrange, L-8070 Luxembourg
Payone	Physical payment processing	Payone GmbH Lyoner Straße 15 60528, Frankfurt am Main Germany