# Data Protection Addendum

This Data Protection Addendum ("**DPA**") forms part of the Agreement ("**Agreement**") between:

(i) **FinDock**, a company having its registered office at de Bleek 7, 3447 GV Woerden, The Netherlands, **("Vendor") ** acting on its own behalf; and

(ii) the entity referred to as Company in this DPA ("**Company**") acting on its own behalf and as agent for each Company Affiliate.

Party (i) and (ii) above together referred to as “Parties”

The terms used in this DPA shall have the meanings set forth under definitions in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below are the DPA to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

## 1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below shall be construed accordingly:

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

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**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;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted 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).

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Agreement;

1.1.12 "**Subprocessor**" means any person (including any third party, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor to Process Personal Data on behalf of any Company Group Member in connection with the Agreement;

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**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.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

## 2. Processing of Company Personal Data

2.1 Vendor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor shall to the

extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

2.2 Each Company Group Member:

2.2.1 gives Vendor the opportunity to:

2.2.1.1 Process Company Personal Data; and

2.2.1.2 in particular, transfer Company Personal Data within countries where the GDPR is applicable , as reasonably necessary for the provision of the Services and consistent with the Agreement; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 2.2.1 on behalf of each relevant Company Affiliate.

2.3 Annex 1 to this DPA sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments, after consultation with Vendor, to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this DPA.

2.4 Without prejudice to what is set out in this section, the personal data transfer to countries outside the EEA to other data processors that the Vendor has hired within its internal organisation shall be deemed authorized, provided that such disclosure is directly related and auxiliary to the Services and notified to the Company and that all safeguards which are required by the European personal data protection regulations regarding international data transfers to countries outside the EEA are implemented.

## 3. Vendor Personnel

Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## 4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural

persons, Vendor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Vendor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

## 5. Subprocessing

5.1 Each Company Group Member authorizes Vendor to appoint (and permit each Subprocessor appointed in accordance with section 6 of this DPA to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.

5.2 Vendor may continue to use those Subprocessors already engaged by Vendor as at the date of this DPA, subject to Vendor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 14 Calendar days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

Vendor shall not appoint (or disclose any Company Personal Data to) the proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Company Group Member and Company has been provided with a reasonable written explanation of the steps taken.

5.4 With respect to each Subprocessor, Vendor shall:

5.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) Vendor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR;

5.4.3 upon request provide to Company for review such copies of the Contracted Processors agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Company may request from time to time.

5.5 Vendor shall ensure that each Subprocessor performs the obligations under this DPA as they apply to Processing of Company Personal Data

carried out by that Subprocessor, as if it were party to this DPA in place of Vendor.

## 6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Vendor shall assist each Company Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Vendor shall:

6.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

## 7. Personal Data Breach

7.1 Vendor shall notify Company within 72 hours after Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable technical and commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## 8. Data Protection Impact Assessment and Prior Consultation

Vendor shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

## 9. Deletion or return of Company Personal Data

9.1 In case of termination of the Agreement ( the **"Cessation Date"**) and after written notice by Company to Vendor, Vendor shall either erase all Personal Data or return them to Company, as Company decides, and erase all existing copies unless it is obliged to keep these Personal Data on the grounds of EU legislation or Member State legislation.

9.2 Subject to section 9.3, Company may in its absolute discretion by written notice to Vendor require Vendor to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies, if possible, of Company Personal Data Processed by any Contracted Processor. Vendor shall comply with any such written notice within reasonable time of the Cessation Date.

9.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Vendor shall provide written certification to Company that it has fully complied with this section upon request.

## 10. Liability

10.1 Any liability arising from or associated with this Addendum is in keeping with, and is solely governed by, the liability provisions set forth in or otherwise applicable to the Principal Agreement. Therefore, and for the calculation of limits of liability and/or determination of applicability of other limitations of liability, any liability arising by virtue of this Addendum shall be deemed to arise by virtue of the Agreement in question.

10.2 Vendor does not accept any liability for any and all damages which is a result of gross negligence of Company and/or Company affiliate.

10.3 Company and/or Company affiliate holds Vendor harmless for any and all damages as a result of gross negligence on the part of Company and/or Company affiliate.

## 11. Audit rights

11.1 Subject to sections [11.2 to 11.5], Vendor shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor reasonable notice of at least 14 days of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

11.4 Any damages incurred by Vendor while performing the audit as referred to in this section 11 will be borne by Company.

11.5 A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

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

11.5.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor that this is the case before attendance outside those hours begins. For the sake of clarity: an emergency as stipulated in this section is defined as a possible data breach; or

11.5.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.5.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's compliance with this DPA, after prior consultation with the Vendor; or

11.5.3.2 A Company Group Member is required or requested 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 Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor of the audit or inspection.

## 12. General Terms

12.1 The general terms and conditions as annexed to the Order Form and as part of the Agreement apply to this DPA.

*Changes in Data Protection Laws, etc.*

12.2 Company may propose any other variations to this DPA if Company reasonably considers this DPA to be in violation of any Data Protection Law.

12.3 If Company gives notice under section 12.2, 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 Company's notice as soon as is reasonably practicable.

12.4 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate to amend this DPA pursuant to this section 12.3 or otherwise.

*Severance*

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

## 13. ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

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

*Subject matter of the Processing of Company Personal Data*

Capture and Processing of Personal Data in order to initiate single or recurring payments for the benefit of Company using one or more payment service providers.

Capture and Processing of Personal Data required to identify and match data subjects to one off or recurring payments made to Company using one or more payment service providers.

Capture and Processing of Personal Data required to identify and match data subjects to one off or recurring payments made to Company using one or more payment service providers.

Capture and Processing of Personal Data required for Gift Aid declaration towards HMRC if so instructed by Company.

Capture and Processing of Personal Data needed in order to inform Company and/or Data subject about the status of a payment, including failed, refunded or reversed payments.

Capture and Processing of Personal Data to select the optimal payment method and timing to initiate payments or retry failed, refunded or reversed payments.

*Duration of the Processing of Company Personal Data*

Company Personal Data will be processed for the duration of the Agreement plus 3 months.

*The nature and purpose of the Processing of Company Personal Data*

Processing data consists of collecting, sorting, transferring to payment service providers, matching/reconciliation data against data received from third parties, enriching, restricting, synchronizing and deletion of data.

The purpose of the Processing is to:

a) Process single or recurring payments and collections from the data subjects;
b) Report to Company the status of or recurring payments and collections from the data subjects;
c) Identify and report new data subjects, or additional data elements from data subjects, to Company based information received from payment service providers or third-party organizations;
d) Offer support to Customer in case of questions or problems related to the Services of Vendor;

*The types of Company Personal Data to be Processed*

- Name (title, first, middle and last);
- Address information (Street, house number, postal code, county/state/province, city and country);5
- Customer ID, order ID, campaign member ID, mandate ID and other unique codes to identify the data subject or transaction;
- Bank account information, including account number, branch code / BIC code / sort code , Account holder name, account status at bank;
- Payment card information, including last 4 digits of credit cards, expiration date, card holder name;
- Payment status and history including open amounts, paid amounts, refunded amounts (including reasons codes);
- E-mail and telephone number;
- Gift Aid declarations (UK taxpayers only).

*The categories of Data Subject to whom the Company Personal Data relates*

- Prospects, customers, supporters, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, supporters, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

*Special categories of Data Subject as defined in Article 9 GDPR to whom the Company Personal Data relates*

Processing of special categories of Data Subjects is not anticipated.

*The obligations and rights of Company and Company Affiliates*

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

## ANNEX 2: SUBPROCESSORS

Company approves that Vendor engages with the following Subprocessors in relation to the performance of the Agreement:

| **subprocessor 1** | | |
|---|---|---|
| Statutory name: | Heroku | |
| Statutory address: | 415 Mission Street, Suite 300, San Fransisco, CA, 94105, United States | |
| Subcontracted tasks and obligations, including location of performance: | Generate and process payment related files, match inbound payment files, host giving pages, gateway for receiving payment service provider notifications. | Frankfurt, Germany |
| | | |

| **subprocessor 2** | | |
|---|---|---|
| Statutory name: | BankAccountChecker operated by aoWare Limited | |
| Statutory address: | 130 Old Street, London, EC1V 9BD, England | |
| Subcontracted tasks and obligations, including location of performance: | Check UK bank account and sort code details. | United Kingdom |
| Note: This Subprocessor is only used if Company installs the “FinDock BACS-for-PaymentHub" package. | | |